Doc ID: 6554247

COPY

HISTORY OF THE SIGNAL SECURITY AGENCY

THE GENERAL CRYPTANALYTIC PROBLEM

VOLUME TWO

ARMY SECURITY AGENCY
WASHINGTON, D C.
1946

Declassified and Approved for Release by NSA on
01-12-2017 pursuant to E.O. 13526, MDR Case # 84693

Doc ID: 6554247

DISTRIBUTION OF

HISTORY OF SSA

VOLUME TWO

Copy 1 AS 14

Copy 2 AS-14

Copy 3 AS-70

Copy 4 AS-80

Copy 5 AS-90

Copy 6 AS-95

Doc ID: 6554247

TOP SECRET CREAM

Do NOT Destroy, Return to the
NSA Technical Library when no longer needed
1-145 Copy No. 2

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

~~TOP SECRET CREAM~~

ARMY SECURITY AGENCY

WASHINGTON, D. C.

HISTORY OF THE SIGNAL SECURITY AGENCY

VOLUME TWO

THE GENERAL CRYPTANALYTIC PROBLEMS

Do NOT Destroy Return to the NSA Technical Library when no longer needed
L-145
Copy No

Prepared under the Direction of the

CHIEF, ARMY SECURITY AGENCY

15 January 1947

WDGAS-13

~~TOP SECRET CREAM~~

TOP SECRET CREAM

Doc ID: 6554247

HISTORICAL NOTE

The original draft of this history of the General Cryptanalytic Branch was prepared in the Recorder's Office under the direction of Dr. Albert Howard Carter. Responsibility for work on the various chapters was assigned as follows:

Dr. Albert Howard Carter: chapters XVII (The Hagelin Section); XX, sections B (The Recorders Group) and D (Documents Section).

Captain George E. McCracken: chapters V (Italian Systems); VI (The French Systems); VII (The Swiss Systems); VIII (The Spanish and Spanish-American Systems); IX (The Portuguese and Brazilian Systems); X (The Systems of the Near and Middle Eastern Governments); XI (The Far Eastern and Central European Systems); XII (Miscellaneous Systems); XIII (The Solution of Meteorological Systems), XIV (The Special Examination Unit); XV (Traffic in Commercial Codes; XX, section E (The Decryptographing Unit); XXI (Assistance from Espionage).

Dr. Carter and Captain McCracken: chapter I (The General Cryptanalytic Branch.

Miss Gertrude Ullman: chapter III (The Japanese Military Attaché Systems).

Miss Ullman and Captain McCracken: chapters II (Japanese Diplomatic Systems); IV (German Diplomatic Systems).

Miss Ullman and Dr. Carter: chapter XX, section A (The Research Section).

Mrs. Marjory Max-Muller: chapter XVI (The Machine Cipher Section); XVIII (The Yellow Project).

Mrs. Max-Muller and Miss Ullman: chapter XIX (The RAM Section).

Miss Dale Wallace and Dr. Carter: chapter XX, section C (The Planning and Priorities Unit).

Rough drafts of the chapters were submitted to the heads of the respective sections for approval before being incorporated into the history; they were then edited in the Historical Unit to conform with the general plan of the History; and finally, the completed volume was reviewed by Mr. Frank Rowlett and revised by Miss Ullman in collaboration with the Historian, AS-13.

For data regarding the total production of B-III, attention is invited to Tabs 15 and 16. Detailed information as to the production of various units of the organization will be found throughout the text.

Historian, AS-13

Doc ID: 6554247

TOP SECRET CREAM

HISTORY OF THE SIGNAL SECURITY AGENCY

VOLUME TWO: THE GENERAL CRYPTANALYTIC PROBLEMS

Contents

Chapter		Page
I.	The General Cryptanalytic Branch	1
	A. Organization and Reorganization	1
	B. Cryptanalytic Liaison with the British	11
	C. Cooperation with OP-20-G	23
II.	Japanese Diplomatic Systems	24
	A. Early Work	24
	B. The Red Machine	29
	C. The Purple Machine	30
	D. Transposition	52
	E. Organization of the Japanese Diplomatic Section	54
	F. The Work of the Section	54
	G. Commercial Systems	57
	H. Liaison	58
	I. Training	60
III.	The Japanese Military Attaché Systems	62
	A. Early Work	62
	B. The Principal System (JAS)	64
	C. The Cryptanalytic Attack	69
	D. Production Methods	71
	E. Other JMA Systems	77
	F. Liaison	78
	G. Personnel and Training	79
IV.	German Diplomatic Systems	82
	A. Early Work	82
	B. The Solution of GEC	83
	C. The GEE System	88
	D. Miscellaneous Systems	95
V.	The Italian Systems	98
	A. Early Work	98

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Chapter		Page
VI.	The French Systems	112
	A. The Early Period (April 1941 to June 1942)	112
	B. The Period of Division (June 1942 to September 1943)	115
	C. The French Cipher Unit	117
	D. The Additive Recovery Unit	119
	E. The Code Recovery Unit	123
	F. The French Translation Unit	126
	G. The French Decode Unit	128
	H. The French Transposed Cipher Unit	129
	I. September 1943 to the Present	130
VII.	The Swiss Systems	139
VIII.	The Spanish and Spanish-American Systems	147
	A. The Code Recovery Unit (B-II-a-5)	151
	B. The Cipher Solution Unit	154
	C. The Translation Unit	155
	D. The Spanish Additive Unit	157
IX.	The Portuguese and Brazilian Systems	160
X.	The Systems of the Near and Middle Eastern Governments	170
XI.	Far Eastern and Central European Systems	180
	A. Chinese Systems	180
	B. The Thai Systems	189
	C. The Middle European Systems	190
XII.	Miscellaneous Systems	197
	A. The Belgian Systems	197
	B. Haitian Systems	198
	C. Luxembourg Systems	199
	D. Irish Systems	199
	E. Hungarian Systems	200
	F. Rumanian Systems	201
	G. Liberian Systems	203

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Chapter		Page
XIII.	The Solution of Meteorological Systems	204
	A. The Problem	204
	B. The Organization	206
	C. Training	208
	D. Coverage and Traffic Handling	209
	E. Solutions	210
XIV.	The Special Examination Unit	220
XV.	Traffic in Commercial Codes	229
XVI.	The Machine Cipher Section	234
XVII.	The Hagelin Section	247
XVIII.	The Yellow Project	257
XIX.	The RAM Section	271
XX.	The Technical Staffs and Service Units	280
	A. The Research Section	280
	B. The Recorder's Group	285
	C. The Planning and Priorities Unit	288
	D. Documents Section	292
	E. The Decryptographing Unit	292
XXI.	Assistance from Espionage	295
	Index	304

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

APPENDICES

	TAB
Evolution of the General Cryptanalytic Branch	1
Plan of Organization, Signal Intelligence Service 1 March 1942	2
Work Schedule 18 May--30 May 1942	3
Plan of Organization, General Cryptanalytic Section, B-3 January 1943	4
Memorandum to Mr. Friedman from Lt. Col. Harold Doud	5
Plan of Organization, Cryptanalytic Branch, Arlington Hall Station, 1 July 1943	6
Plan of Organization, General Cryptanalytic Branch, B-III September 1943	7
Proposed T/O for B Branch, 25 September 1943	8
T/O for Cryptanalytic Branch, 17 April 1944	9
Plan of Organization, B Branch, 30 June 1944	10
Memorandum to Lt. Colonel Rowlett from Colonel Harold G. Hayes, 19 August 1944	11
Organization of General Cryptanalytic Branch, 21 August 1944	12
Plan of Organization, Japanese Diplomatic Section Spring 1944	13
Evolution of the Romance Language Section 1941--1944	14
Production of B-III throughout the Year 1944	15
Processing of Diplomatic Traffic, September 1944	16
First Translation of a B-Machine Message	17
The JBA Process from Intercept to Translation	18
The JBC Process from Intercept to Translation	19
A Sample JAS Work Sheet and Translation	20
FMC Work Sheets, French Transposition Problem	21
Persian Enciphered Code Processing	22
Turkish Enciphered Code Processing	23
Arabic Code and Cipher Processing	24
A Typical Problem Routed to the Special Examination Unit	25
Analogue of the Purple Machine	26
Enigma Replica	27
The "003"	28
The Arlington Dudbuster	29
The Autoscritcher Viewed from the Rear	30
The Autoscritcher Viewed from the Front	31
The 5202 Camera, Target, and Generator	32
The 5202 Comparator and Counter	33

TOP SECRET CREAM

Doc ID: 6554247

HISTORY OF THE SIGNAL SECURITY AGENCY

VOLUME TWO: THE GENERAL CRYPTANALYTIC PROBLEMS

CHAPTER I. THE GENERAL CRYPTANALYTIC BRANCH[1]

A. Organization and Reorganization

When, in 1930, the Signal Intelligence Service was established under the Chief Signal Officer, with the Assistant Chief of Staff, G-2 exercizing staff supervision, the directive under which the new Service was to operate emphasized, so far as solution of foreign cryptographic systems was concerned, training for an emergency rather than solution of current systems for the production of intelligence.[2]

Fulfillment of the training program, however, necessitated attempts to intercept sufficient raw traffic to provide material for instructional purposes, and though establishment of adequate intercept facilities was difficult, a certain amount of traffic was intercepted and solved. This was at first chiefly Japanese traffic. When success was achieved in the solution of a given Japanese system, translations were, on occasion, forwarded to G-2, more as an indication of what could be and had been done than because G-2 was expected to make use of the specific contents of the messages thus made readable.

As time passed, interest began to grow in solution of current

---

1. The present volume will contain the story of all cryptanalytic projects undertaken by the Signal Security Agency during World War II except only those of the Japanese Army systems which, because of their magnitude and importance, require separate treatment. See volumes Three (B-II) and Five (B-IV).

2. See Historical Background of the Signal Security Agency, volume Three, chapter V.

Doc ID: 6554247

TOP SECRET CREAM

traffic on an operational basis, rather than as merely incidental to training, and by the outbreak of the War in Europe, on 1 September 1939, there were in the Signal Intelligence Service four cryptanalytic units, under the technical direction of Mr. William F. Friedman. They were designated as follows:

J Section	Japanese Diplomatic, activated about 1935 under Mr. Frank B. Rowlett
G Section	German Diplomatic, activated about 1938 under Dr. Solomon Kullback
I Section	Italian Diplomatic, activated about 1938 under Dr. Abraham Sinkov
M Section	Mexican Diplomatic, activated about 1938 under Mr. H. F. Bearce

These four units were at work, under directives from G-2, on the current solution of diplomatic traffic sent out by the governments concerned. Organization was not rigid, however, since there was a good deal of collaboration between the four units. Successes reached in this early period will be discussed individually in subsequent chapters.

No further cryptanalytic units were established before the attack on Pearl Harbor, but soon after the M Section began its existence it expanded its scope to include a few other Spanish-American countries (chiefly Colombia and Venezuela), and early in 1941 it also commenced attempts at solution of the systems of Vichy France, Spain, Portugal, Brazil, and still other Spanish-American governments. It was thus the forerunner of all units which during the War attacked the systems based

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

on Romance languages except only those in Italian, which, as we have seen, were studied in a special section established at an early date.

Some time in the winter of 1941--whether before 7 December 1941 or as an immediate result of the momentous events of that day--the Signal Intelligence Service as a whole was reorganized into four sections (Tab 1):

A Section	Administrative
A-1	Personnel
A-2	Tabulating Machinery
B Section	Cryptanalytic
B-1	Japanese
B-2	German
B-3	Italian
B-4	Mexican, etc.
B-5	Stenographic
B-6	Traffic
C Section	Cryptographic
D Section	Secret Ink and Photographic Laboratory

The duties of subsections B-1, B-2, B-3, and B-4 continued to be the same as before: B-5 was a group of typists who prepared finished copies of the translated messages, and B-6 was a small unit responsible for giving directives to the intercept stations--the officer in charge was also commanding officer of the Second Signal Service Company--and caring for the routing of traffic within the Cryptanalytic Section. In addition to these two service units, there was another, Tabulating Machinery (A-2), the work of which was largely in support of the Cryptanalytic Section, but since it contributed to some extent to the activities of the Cryptographic Section, the Tabulating Machinery Unit was attached to the Administrative Section.

Between the beginning of the War in December 1941 and the move

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

to Arlington Hall Station in the summer of 1942 certain changes were made. (Tab 2) The old M Section was almost at once divided, B-4 being the designation of the new unit assigned to French traffic and B-7 that of the unit assigned to solution of traffic in the Spanish and Portuguese languages. The former Tabulating Machinery Unit (A-2) was, at about the same time, transferred from the Administrative Section and set up as B-8, though of course it continued as before to work also for the Cryptographic Section. In May 1942 a beginning was made in an organized effort to provide information services for the cryptanalysts, and this new unit was designated B-9. Finally, a new unit (B-10) was set up in the same month to study weather reports transmitted in enciphered forms of the International Meteorological Code. The Cryptanalytic Section was thus organized as follows:

Cryptanalytic Section, OIC Lieutenant Colonel Harold Doud
- B-1 Japanese, OIC Major E. H. F. Svensson
- B-2 German, OIC Captain S. Kullback
- B-3 Italian, OIC Major A. Sinkov
- B-4 French, OIC Lieutenant H. F. Bearce
- B-5 Stenographic, CIC Miss M. Louise Prather
- B-6 Traffic, OIC Major R. E. Schukraft
- B-7 South American, OIC Lieutenant L. M. Glodell
- B-8 Tabulating Machinery, OIC Lieutenant R. H. Adams
- B-9 Information, NCOIC Corporal Ivan Bash
- B-10 Weather, OIC Captain U. S. Lyons

Five of these units were engaged in solution of the varied types of cryptography met with in the systems of a single government or group of governments. In Tab 3 is shown a work schedule for the period 18 - 30 May 1942. Operations involved not only cryptanalysis but decoding and deciphering, and finally, translation of the messages. Another

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

unit (B-10) was engaged in applying cryptanalytic techniques to a special type of traffic sent out by a number of governments. The remaining four units provided services of one sort or another to all the others.

The first result of the great expansion which the Signal Intelligence Service experienced in the first six months of 1942 was the removal of the Traffic Unit (B-6) from the Cryptanalytic Section and its establishment on an autonomous basis as E Section in May 1942. Henceforth, the Cryptanalytic Section was no longer responsible for interception and related functions. But the reorganization went much further than that; the nine remaining units were regrouped, and in some cases dissolved to reform on a new principle of organization, namely, similarity as regards cryptographic type of system involved.

This departure from what had previously been the norm was probably motivated by experience in the solution of ciphers. In this instance a knowledge of the basic language underlying the system is less urgently needed than in the case of code reconstruction. Moreover, the solution of one cipher has more in common with the solution of another in a different language than with the solution of a code in the same language. It was felt therefore that if solution of all codes were made the function of one subdivision, solution of all ciphers the function of another, and possibly also code encipherments were separated from both, progress would be greatly facilitated.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

To put such a policy into operation, the Cryptanalytic Section was reorganized at the time of the move to Arlington Hall Station (June to August 1942), and the final result was as follows:

Cryptanalytic Section, OIC Lieutenant Colonel Harold Doud
- B-1 Miscellaneous service units, OIC Captain Verner C. Aurell
  - Translation
  - Decryptographing
  - Traffic
  - Bulletin
  - Information
- B-2 Code and additive encipherment solution, OIC Captain S. Kullback
  - Code reconstruction
  - Additive encipherment solution
- B-3 Cipher solution and solution of code encipherments other than additive encipherments, OIC Lieutenant Frank B. Rowlett
- B-4 Tabulating machinery, OIC, Captain Perry Molstad

It will be seen that except for Tabulating Machinery, all service units were gathered together in a miscellaneous subsection (B-1), but while this subsection was responsible for Japanese translation and for some of the translation in French and Spanish, it did not prepare translations in other languages, or, indeed, all of those in French and Spanish. Moreover, its decryptographing work was limited to solved systems only, and its traffic function was restricted to sorting and routing traffic after it had reached B Section: it was not responsible for issuing directives to the intercept stations, which was then a function of E Section.

B-2 maintained (1) a subsection which carried on code reconstruction in four units devoted to the French, Italian, Portuguese, and Spanish languages--code reconstruction was not needed in German, owing

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

to compromised code books—; (2) another subsection devoted to solution of additive encipherments (German, Spanish, and weather systems); and (3) also small units devoted to the study of new systems used by the Japanese diplomatic, military attaché, and army communications. See Tabs 5 and 6.

It was in B-2 that the disadvantages of the new arrangement were first keenly felt. In the Italian Unit, for example, which had previously been successful by combining cryptanalytic and linguistic operations in solving the same traffic, the division of solution of encipherment from code reconstruction had a hampering effect upon operations, particularly since the additive encipherment unit was located at a distance from the code reconstruction unit. Each of these two units had more in common with each other than either had with other units practicing the same techniques upon different traffic. Even before the reorganization of 1943 eliminated this disadvantage, attempts had been made to overcome the difficulty by assigning the units to contiguous quarters; then they were joined operationally though separated administratively; and finally, when the reorganization came at last, they were once more amalgamated.

The same disadvantage was felt also in the French units, of which there were actually four instead of two: French Code Reconstruction, French Additive Solution, French Decoding, and French Translation, but here the emergency solution was the establishment of a coordinating committee, which did much to bring about amalgamation of all French

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

units. It must be admitted that this division of functions did not have a bad effect upon solution of systems using Spanish and Portuguese, since only the Spanish Government used additive encipherment and in that case the codes used had been compromised and no reconstruction was necessary. The Portuguese and Brazilian systems were also almost wholly code reconstruction problems. Moreover, in the field of ciphers, that is, in B-3, the new arrangement worked remarkably well.

The Fiscal Year 1943, the first at Arlington Hall Station, was passed with the four-fold organization just described, but it was becoming obvious that a number of factors would soon demand a thorough-going revision. The chief factor which brought this revision about was the cryptanalytic success reached in late spring by the small unit studying the Japanese Army problems. Exploitation of this success was at once necessary, and since this would involve tremendous expansion, the Japanese Army problems were set up, 1 September 1943; as one of the major sections (B-2) of the Cryptanalytic Branch, which the old Cryptanalytic Section had now become. The remainder of B-2 was then amalgamated with B-3, and a new internal organization was effected whereby a return was made to the older form of organization by language units, with a number of units devoted to cipher problems remaining independent (Tab 7). The new B-3 Section also assumed certain of the functions formerly belonging to B-1, which now retained control only of matters pertaining to the Japanese language (translation, code reconstruction, and training) but gave up everything else. The Bulletin, Information, and Liaison Units of B-1,

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

were for a temporary period administered by Headquarters Branch, Signal Security Agency. See Tab 8. The new arrangement of the Cryptanalytic Branch was therefore as follows:

Cryptanalytic Branch, OIC Lieutenant Colonel Earle F. Cook
- B-1 Japanese Language, OIC Major Verner C. Aurell
- B-2 Japanese Military Cryptanalysis, OIC Lieutenant Colonel S. Kullback
- B-3 General Cryptanalysis, OIC Major Frank B. Rowlett
- B-4 Tabulating Machinery, OIC Major Perry Molstad

Some idea of the extent of the expansion in personnel strength of the Branch is afforded by a Proposed Supplemental Table of Organization dated 1 July 1943, revised 17 August 1943, which shows the Cryptanalytic Branch at its actual strength and the increase which was asked for, as follows:

SUMMARY BY CLASSIFICATIONS

Classification	Actual	Proposed
Officers	157	240
Enlisted	240	240
Civilians	1713	4784
Total	2110	5264

SUMMARY BY SECTIONS OF THE BRANCH

Administrative	17	17
Section I	566	1289
Section II	544	2606
Section III	337	312
Section IV	646	1040
Total	2110	5264

The great increase in the needs of Section I (Japanese Language), Section II (Japanese Military Cryptanalysis), and Section IV (Tabulating Machinery), coupled with the slight decline in the requirements for Section III (General Cryptanalysis) reflects the success in solving

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the Japanese Army systems which had recently been achieved.

Not long after this reorganization of September 1943, B-4 (Tabulating Machinery) was given an autonomous relation as G Branch, and in its place were transferred from E Branch those units engaged in Traffic Analysis, which, as was now recognized, were performing operations more closely akin to the intelligence functions of the Cryptanalytic Branch than to the communications functions of E Branch. Later, in 1944, still other E Branch units concerned with Traffic Control were also transferred to B-4.

From February to August 1944 a project set up at Vint Hill Farms Station which utilized Nisei enlisted personnel for translation and a limited amount of cryptanalysis was given the designation of B-5 (Tabs 9 and 10), but this section was later subordinated to B-1 and designated B-I-5. This produced the following organization:

Cryptanalytic Branch, OIC Colonel Harold G. Hayes
- B-1 Japanese Language, OIC Lieutenant Colonel Verner C. Aurell
- B-2 Japanese Military Cryptanalysis, OIC Lieutenant Colonel S. Kullback
- B-3 General Cryptanalysis, OIC Lieutenant Colonel F. B. Rowlett
- B-4 Traffic Analysis and Control, OIC Captain Ralph J. McCartney
- [B-5] Vint Hill Translation Section (temporarily), OIC Major Gordon T. Fish

Finally, those units of the old Cryptanalytic Section which had gone to Headquarters Branch were, on 1 March 1944, set up as the Information and Liaison Branch under Captain James H. Frier, Jr., who was relieved as Officer in Charge on 12 January 1945 by Captain John H. Connor.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

While each of these components of the Cryptanalytic Branch underwent further internal reorganizations from time to time, no other changes in their essential relationships one to another were made throughout the War. In August 1944, however, an Agency-wide reorganization resulted in the redesignation of the Cryptanalytic Branch as the Intelligence Division and the consequent elevation of its component sections to the status of branches. (See Tab 11.) While this change had many advantages of an administrative nature, it did not affect in any was the organization of the five component branches of the Intelligence Division: Language, Military Cryptanalytic, General Cryptanalytic (Tab 12), Traffic Analysis and Control, Information and Liaison.

B. Cryptanalytic Liaison with the British[2]

In the summer of 1940 the War Department had made, as we have seen,[3] a decision to exchange military information with the British, but so far as the Signal Intelligence Service was concerned, this decision was not implemented by actual interchanges until early in 1941. A mission was then sent to England consisting of Captain Abraham Sinkov and First Lieutenant Leo Rosen, who spent February and March 1941 in

---

2. The plan of this History limits the scope of the present volume to cryptanalytic attack upon all foreign systems of communications except those of the Japanese Army, which are discussed in volume Three, but much that is said here is equally applicable to the work on the Japanese Army problem. Indeed, the Sinkov-Rosen mission, as will shortly appear, first made arrangements for an exchange on these problems also.

3. In volume One, chapter IV, section B.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the study of information which the British possessed and in visiting the British cryptanalytic units, then located, except for the compilation unit at Oxford, at Bletchley Park, Bletchley, where they had been moved from London to provide a somewhat greater degree of safety during the Battle of Britain.[4]

According to their report of 11 April 1941, addressed to the Assistant Chief of Staff, G-2, "the primary mission related to German, Japanese, Italian and Russian secret systems." In addition, they received information regarding minor European powers and Latin America.[5] Neither this report, however, nor the longer account[6] which they submitted to the Chief, SIS mentioned what was probably the most significant evidence of the willingness of the British to cooperate:[7]

---

4. Originally it had been intended that Mr. William F. Friedman would participate in the mission and, indeed, the state of his health was one of the factors in postponing the departure. Mr. Friedman was then, however, a Reserve Officer on active duty, and, in spite of the fact that orders had been written, he did not go. Later, the Surgeon General declared him to be permanently incapacitated for active duty because of physical disability, and he therefore reverted to the status of civilian employee, which he had previously held since 1 January 1921. This did not prevent him from making two later missions (1943 and 1945) to England, as will shortly be described.

5. Memorandum to Assistant Chief of Staff, G-2 "Report of Technical mission to England," signed by Captain A. Sinkov and Lieutenant Leo Rosen, 11 April 1941, filed in MID.

6. This is now filed in the Army Security Agency as IL 413.

7. They omitted this fact, of course, for security reasons, as will shortly be seen.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the British, after obtaining special pledges of absolute secrecy,[8] revealed to these American officers the existence of their "E" operations (a successful attack upon traffic enciphered by the German high-security cryptographic machine known as the Enigma and used throughout the War by the German Army, Navy, Air Force, and Railway Service for secret communications). "It is significant to observe (and with some measure of chagrin) that this pledge was publicly violated by the Pearl Harbor investigation."[9]

The report cited, evaluating the fruits of the Sinkov-Rosen mission, was the first of a long series of reports which pointed out that "the material which was furnished . . . will result in a saving of several years of labor on the part of a fairly large staff." In return, these first liaison officers supplied the British with the greatest treasure of the Signal Intelligence Service: the solution of the Japanese high-security diplomatic machine and system, designated by the Signal Intelligence Service as the "Purple." In addition GCCS was given one analogue of this machine, together with all the technical information necessary for its operation in deciphering messages. GCCS was also supplied with the results of American work on the Italian diplomatic problems with which Captain Sinkov had been

8. They were required to take a special oath to reveal what they had learned of the Enigma solution only to three persons: the Assistant Chief of Staff, G-2; the Chief, SIS; and Mr. William F. Friedman.

9. Colonel Abraham Sinkov, interview of 24 May 1946 with Historian, ASA.

TOP SECRET CREAM

Doc ID: 6554247

closely associated. For their part GCCS "suggested definite plans for . . . cooperation including the possibility of a division of effort to avoid duplication." Especially interested in cooperating on Far Eastern problems, GCCS was willing to supply the technical data elaborated by its "cipher section in Singapore,[10] which is getting fairly good results" if the United States would supply competent Japanese translators to make up a deficiency in that field.[11]

In addition to information concerning the results of British study, the two American officers brought back in complete form a Mexican twenty-alphabet cipher and keys, a Brazilian code, several German Air Force code books, as well as partial reconstructions of an Argentine and a Chilean code.

At this point it will be well to digress for a moment to pay some attention to the question as to which side gained most from the Anglo-American collaboration. Persons whose high technical capacities had confined their experience to but one or at most a few fields of operation, particularly when it was in those fields that the British had been able to make very significant contributions to the progress of the Signal Security Agency, have often informally discussed the question, but because they were not in a position to assess the entire history of the liaison and match a British contribution here with an

---

10. Ibid.

11. The sequel to this move will be discussed in volume Three, especially chapter II.

Doc ID: 6554247

TOP SECRET CREAM

American contribution there, no conclusion could generally be reached. Indeed, in a question of this kind, when imponderables are involved, it is advisable to refrain from expressing conclusions hastily arrived at.

Yet some definite conclusions can be stated: the British made their largest contribution in providing a vast supply of information concerning the results of their cryptanalytic studies of past and current systems. Cryptanalytic continuity had begun for the British in 1914, whereas for the Signal Intelligence Service it was broken in 1930 when MI-8 was dissolved. In only one field (Japanese diplomatic systems) had the Signal Intelligence Service been able by 1941 to amass enough data to be able to say that cryptanalytic information was once more continuous, and, significantly enough, it was in this very field that the Signal Security Agency was able to give the British at the outset its most valuable contribution (the "Purple").

On the other hand, the Americans were, all through the War, able to exploit to a much fuller extent than the British the vast possibilities for cryptanalytic purposes inherent in the use of the newer mechanical, electrical, and electronic techniques. Perhaps the best indication that the Anglo-American collaboration was mutually helpful was the fact that it was continued throughout the War and is planned also for the postwar period.

After the return of the Sinkov-Rosen mission, the next event in the history of Anglo-American liaison on cryptanalytic attacks was a

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

visit by Mr. (Commander) A. G. Denniston, then head of GCCS, who discussed with the several SIS sections "matters of general interest in connection with joint cryptanalytic activities."[12] At this time he arranged for Captain (later Major) Geoffrey G. Stevens to come to Washington as an observer of Japanese cryptanalysis.[13] Captain Stevens was to report to and be under the jurisdiction of Captain Edward Hastings, British Liaison Officer for GCCS in Washington.

The first record of a routine exchange of cryptanalytic material is dated just after the Pearl Harbor attack. On 14 December 1941 the Signal Intelligence Service agreed to the proposal made by GCCS that "frequent exchange of material [was] desirable" concerning the principal diplomatic system (GEC).[14] Shortly thereafter the Signal Intelligence Service sent a complete list of recovered daily keys for 1930 and 1940[15] to GCCS, which, indeed, had earlier given Captain Sinkov the results of their work on this system.

In May and June of the following year (1942) Captain Solomon Kullback was assigned to temporary duty at GCCS, where he studied

---

12. "Minutes of Conference," 16 August 1941, Room 3341, Munitions Building, attended by Lieutenant Colonel R. W. Minckler, then Chief, SIS; Captain Harold G. Hayes, then Executive Officer, SIS; Captain Earle F. Cook; Captain A. Sinkov; Lieutenant Leo Rosen; Mr. William F. Friedman; Mr. Frank B. Rowlett; and Dr. S. Kullback. Document on file in the Office of the Director of Communications Research.

13. Recollection of Colonel Harold G. Hayes, 28 May 1945.

14. Telegram dated 14 December 1941, copy in IL 414. See chapter IV.

15. Contained in Document No. IL 414.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

German, Japanese, French, Spanish, Italian, Middle Eastern, Near Eastern, Chinese, South American, and Swedish diplomatic systems, German military systems, and other systems. The material which he brought back was perhaps the largest single shipment received from GCCS: it included GEC keys, work sheets, and a technical description of that system; French keys and instructions concerning encipherment; a number of reconstructions of codes, among which were French, Spanish and Japanese codes; and, finally, the facts then known concerning the solution of German military traffic. Captain Kullback had "found the British most helpful and cooperative and was permitted access to every section [of GCCS] at Bletchley[16] and London.[17] They were completely frank, open and aboveboard with me and kept [back] no detail of their operation, procedures, technique, or results."[18]

In the month of July 1942 the President reviewed the situation[19]

---

16. Bletchley Park, Bletchley.

17. Berkeley Street.

18. Major Kullback's report, dated 1 August 1942, is filed in IL 412. When the Sinkov-Rosen mission went to England, all the sections of GCCS were located at Bletchley Park, Bletchley, about 50 miles northwest of London. By the spring of 1942, when the Battle of Britain had been won, and it was deemed sufficiently safe to move some sections back to London, the diplomatic sections, under Commander Denniston were moved to Nos. 8-9, Berkeley Street, London, and that part of GCCS was thereafter generally referred to as "Berkeley Street." The part remaining in Bletchley was often referred to as "the Park" or "BP".

19. Memorandum for General Marshall, 9 July 1942, signed "F.D.R." A copy of this memorandum and of Major General Strong's reply to General Marshall of the same date are now filed in the Office of the Director of Communications Research. General Marshall's own memorandum, dated 11 July 1942, is filed in MID.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

and was assured by the Chief of Staff that "an interchange of cryptanalytic information had been in progress for over a year and appears to be satisfactory to both services." Indeed, the examples of the uninterrupted flow of materials between the two centers cited throughout this volume show that this cooperation was not only satisfactory but essential to the success of the two organizations.

Meanwhile, the exchange of material with the Examination Unit at Ottawa had begun. The Canadian organization had been founded in 1941; but since Mr. Herbert O. Yardley, who had been head of MI-8 from 1917 to 1929,[20] was employed there, the Signal Intelligence Service and GCCS refused to cooperate with EU until Mr. Yardley was dismissed.[21]

Mr. Oliver Strachey, one of the most experienced members of the GCCS staff, was the first head of EU sent to Ottawa after Yardley's dismissal. He remained for one year and was succeeded by Mr. F. A. Kendrick, who paid several visits to the Signal Intelligence Service during 1942 and thereafter until he returned to England in 1945. The first recorded instance of cooperation between the Signal Intelligence Service and EU involved the receipt from the Canadians of a copy of one of the French codes captured in January 1942 at Miquelon. Cooperation

---

20. On his work see Historical Backgrounds of the Signal Security Agency, prepared by the Historical Unit, Army Security Agency, especially volumes Two, (chapters I-VI) and Three (chapters II-IV). The reason for the attitude of GCCS and the SIS toward Yardley is discussed in volume Two (chapter IV).

21. This was one of the results of the discussions with Commander Denniston.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

with EU has been as cordial and profitable as that with GCCS in every sphere in which EU operates, but it should be pointed out that EU did not carry on a program of cryptanalytic study of any systems except those of the French and Japanese.

In 1943 Mr. William F. Friedman visited GCCS, and between 25 April and 13 July he studied all their operations except those relating to German naval traffic.[22] This visit provided the data on which work in the Signal Security Agency on German military systems was later to be based. Mr. Friedman was not only permitted to view these operations without restriction but he was allowed to prepare a voluminous series of reports on the organization and technique of the British units engaged on this work, something that had never hitherto been permitted even a member of the British staffs![23] About the same time Captain Roy D. Johnson returned from a tour of several months temporary duty at GCCS with a great body of technical knowledge and experience to be applied to the German military problem.

---

22. It should be pointed out that GCCS is an intra-service organization and carries on work in diplomatic, military, and naval systems, whereas in the United States responsibility for attack on different categories of traffic is divided between the Army, the Navy, and the FBI.

23. See "Preliminary Report of Trip to England", 8 July 1943; a fuller account is to be found in "Report on E Operations of the GC & CS at Bletchley Park," 12 August 1943, 113 pages; "Report on 'ISSOS' and 'ISK' Sections," 25 November 1943; "Report on 'E' Operations of the GC & CS," 7 January 1944 (by Lieutenant Clarence S. Barasch); "Report on IBM Operations," 4 October 1943; and "Report on Visit to the Intercept Station at Cheadle and War Office Y Group," 28 August 1943.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Cooperation with the two GCCS centers (Bletchley Park and Berkeley Street) was also carried on by representatives of the Military Intelligence Service. Colonel Alfred McCormack and Lieutenant Colonel Telford Taylor were in England at the same time as Mr. Friedman, and it was agreed between the Assistant Chief of Staff, G-2 and GCCS to appoint an MIS liaison officer at GCCS. Colonel Taylor, who was designated as the first MIS liaison officer, was given space and set up his office in Berkeley Street. For some months Colonel Taylor divided his time between Bletchley Park and Berkeley Street, but later in the summer Mr. Roger S. Randolph of MIS was assigned to assist Colonel Taylor, who was then able to spend more time at Bletchley Park, devoting his attention to the military operations there, leaving the diplomatic to Mr. Randolph. To these men goes much of the credit for the cordial relations between the two centers and for the rapid interchange of information. When, in August 1943, a regular liaison officer was appointed from the Signal Security Agency, these men enabled him to keep informed regarding GCCS operations at both places; the SSA liaison officer made his headquarters at "the Park," and the MIS liaison officer at Berkeley Street assisted in keeping him abreast of the work at that center. Naturally, there was a reciprocal exchange of pertinent information.

In August 1943, when Colonel W. Preston Corderman visited GCCS, Captain John N. Seaman was designated as the first SSA liaison officer, to serve at GCCS as the counterpart of Major Stevens, the GCCS liaison

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

officer at Arlington Hall.[24] While there, Captain Seaman wrote some 50 reports. He was accompanied by Mr. Robert O. Ferner, who studied machine ciphers and worked on other problems at Bletchley Park and in November returned to Arlington Hall. In the autumn of the same year, Mr. Randolph wrote his Personnel Study of Berkeley Street Prepared for Arlington Hall.

In December Captain E. B. C. Thornett, head of Japanese diplomatic work at GCCS, and Captain P. W. Filby, head of the German code work, spent two weeks at Arlington Hall. Liaison between the British and American sections progressed thereafter without interruption, and regular interchange of information made possible the great advances in the cryptanalysis of Japanese and German diplomatic systems which proved to be important factors in the winning of the War.

In March 1944 Captain Walter J. Fried relieved Captain Seaman as SSA liaison officer at GCCS. Upon his return Captain Seaman set up an office to coordinate and expedite the flow of information from Arlington Hall to GCCS and to keep Captain Fried informed of the needs here. He initiated the monthly information letter to the SSA liaison officer abroad as a vehicle for keeping him informed of developments at home. Captain Fried, for his part, between 2 March and 29 November 1944, wrote 123 reports and sent almost 9,000 pages and 32 microfilms of

24. Major Stevens also served as GCCS liaison officer to OP-20-G, while Captain Seaman had no equivalent duty at the Naval Section of GCCS, since OP-20-G had its own liaison officer there.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

technical information to the Signal Security Agency--this in addition to the daily exchange of telegrams and the transmission of documents regularly established between sections which, because of their routine nature, did not require the personal attention of the liaison officer.

In the summer of the same year, from May to August, Lieutenant Colonel Frank B. Rowlett, Chief of the General Cryptanalytic Branch, worked in GCCS, and in the autumn Captain Herbert H. Maass and Sergeant Walter Jacobs went there for study. Mr. Samuel S. Snyder, head of the Japanese diplomatic and military attaché work at Arlington Hall, visited EU in the autumn of 1944 to perfect the exchange of information on Japanese diplomatic systems; in December Dr. Calvin S. Brown was there for the same purpose with respect to French systems.

On 19 October 1944 Mr. Albert W. Small arrived in GCCS and took over the duties of Captain Fried, who remained until the end of November. Mr. Small, in turn, stayed until May 1945 when Major Seaman was given a second tour of duty as liaison officer.

At the beginning of the new year the value of a great body of miscellaneous traffic sent on the Japanese domestic net was recognized, and some agreement was necessary for the allocation of responsibility for this traffic. Accordingly, in March 1945 representatives of the three cooperating centers (GCCS, EU, and the Signal Security Agency) met in Washington and arrived at an agreement which increased in scope their cooperative effort.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

C. Cooperation with OP-20-G

Mention should be made of still another aspect of cooperation, established long before the attack on Pearl Harbor--that between the Signal Security Agency and OP-20-G. Throughout this volume references to such cooperation show that, as the War progressed, the cooperation between the two services increased in scope. When, in 1942, OP-20-G abandoned the study of diplomatic systems,[25] the cooperation between the two services involved largely joint work on the weather systems and technical consultation on machine ciphers. OP-20-G was especially generous in making cryptanalytic-machine time available to the Signal Security Agency.

25. See volume One, chapter IV, section D.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER II. JAPANESE DIPLOMATIC SYSTEMS[1]

A. Early Work

Japanese diplomatic systems were among the first to receive the attention of the original nucleus of cryptanalysts in the Signal Intelligence Service,[2] who had the advantage of possessing a considerable body of Japanese material from the files of MI-8. Between 1919 and 1929 MI-8 had recognized a total of 31 different Japanese systems, of which 18 were diplomatic, 5 military attaché, and five naval attaché systems.[3] The personnel of MI-8 had also prepared a number of reports, the most important being a description of the method of attack used in the case of the so-called "U-Type" codes (JU and its relatives), which were in use between April 1924 and March 1925. Most, but not all of these systems, were made readable in MI-8. For the most part they were the type of codes known as a syllabary; that is, plain-text digraphs

---

1. Sources for this chapter include documents on file in the Japanese Diplomatic Section, General Cryptanalytic Branch: progress reports, historical accounts, descriptions of systems, diaries, publications of the Recorder's Group; RIP-37, publication of OP-20-G; historical files of MI-8; a "Special Historical Report on the Solution of the 'B' Machine," prepared by William F. Friedman on 14 October 1940; interviews with Captain Robert F. Packard, Messrs William F. Friedman, Samuel S. Snyder, Gustavus F. Swift, Dale Underwood, and Miss Elizabeth Stephens; and a lecture by Lieutenant Colonel Frank B. Rowlett.

2. See Historical Background of the Signal Security Agency, volume Three, chapters II-IV, and Japanese Codes and Ciphers 1919-1929, both publications of the Historical Unit, Army Security Agency.

3. The remaining three (JD, JF and JH) are not represented by any material in the files. It should be pointed out that MI-8 referred to the attaché systems as "Army Codes" and "Navy Codes," but the evidence is clear that these systems were in use for the communications of military and naval attachés only.

Doc ID: 6554247

TOP SECRET CREAM

were represented by two-letter code groups, which in some cases stood for a frequently-used word. An innovation first observed in the code JG, introduced in June 1921, consisted of adding to the two-letter syllabary a small number of four-letter code groups all beginning with the same initial letter, in this case "B". The only other point of interest was that codes JL and JW were in English and not Japanese.[4]

Not until 1933 were the cryptanalysts of the Signal Intelligence Service able to turn their attention to Japanese problems. In that year Dr. Solomon Kullback and Mr. John B. Hurt were assigned some Japanese messages which they found to be encoded in a system of the same two-letter and four-letter type known to MI-8.[5] Although these messages and others contained no information of real value as intelligence, they did provide a basis for a study of the type of vocabulary, the grammatical forms, frequencies, and cryptographic habits to be expected in other Japanese traffic. Typical of the solution activities of this period is that of J-6, a system using three-letter and four-letter code groups.[6]

Between 1933 and 1935 five Japanese diplomatic systems were used in rotation at intervals of three months. These systems, solved and

---

4. The attaché systems were distinctly more mature than the diplomatic, showing clear evidence of independent compilation.

5. Mr. Hurt stated on 22 October 1945 that solution and translations were accomplished in a few hours.

6. The description of the attack and the reconstruction are reported in IR 5010-5012 (5 March 1934).

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

read, were all of the familiar two-letter and four-letter type of code with syllabary and vocabulary. By 1938 nine Japanese diplomatic systems had been read by the Signal Intelligence Service. The appearance of new systems and the increasing complexity observed in them during the 1930's may have been the result of the publication in 1931 of The American Black Chamber by Herbert O. Yardley, who had been the Chief of MI-8. If this book had not been published, Japanese diplomatic cryptography probably would not have experienced the variation and improvement that marked its course after 1931. Though for a time the older, very insecure type of syllabary continued in use, the Japanese at least as early as 1932, whether to reduce expenses or to increase the security of their communications, were employing a machine cipher designated by them as the "A" Machine and by the Signal Intelligence Service as the "Red" Machine.[7]

Japanese systems known to the Signal Intelligence Service during the 10 years prior to World War II include the following:

Digraphic substitution:

code		
AW	effective	July 1932 to December 1934
CA	"	November 1936
YO	"	September 1938

7. This is described in section B of this chapter. According to an unsigned typed report based on deciphered messages (on file in the Recorder's Office, B-III), on 1 December 1938 a modification of the Red Machine was contemplated by the Japanese for the purpose of enciphering certain messages of a particularly secret nature.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Polygraphic substitution:

code		
XA	effective	(1931-32?)
XB	"	
DA	"	October 1932 to 15 October 1935
EG	"	January 1933 to 15 October 1935
WI	"	April 1933 to 15 October 1935
IK	"	December 1933 to October 1934
J-6	"	15 October 1935 to 28 February 1938
J-7	"	1 January 1936 to 26 February 1936 Revived March 1940
J-8	"	27 February 1936 to 30 June 1938
J-9	"	1 July 1936 to 31 October 1938
J-10	"	1 November 1938 to 9 April 1939
K-1	"	1 November 1938
J-11	"	10 April 1939 to 1 January 1940
KO	"	April 1939
J-12	"	2 January 1940 to 31 May 1940
J-13	"	1 June 1940 to 15 July 1940
J-14	"	15 July 1940
J-15	"	15 July 1940
P-1	"	15 July 1940
J-16	"	15 August 1940 to 30 November 1940
K-1	"	19 January 1939 to 1 July 1940
K-2	"	19 January 1939
K-3	"	1 July 1940
K-4	"	15 July 1940 to 15 November 1940
K-5	"	15 August 1940 to 30 November 1940
K-6	"	1 December 1940 to 28 February 1940
K-7	"	
K-8	"	1 March 1941
K-9	"	11 March to 25 April 1941
K-10	"	23 June 1941 to 15 August 1943

Spelling Tables:

JE English Spelling
English Spelling and Vocabulary
French Spelling and Vocabulary
"HE" Code
"EX" Code
"OG" Code
"UJ" Code
"CH" Code
"B" Table
PA English Spelling
CA English Spelling

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Transposition, used in conjunction with the earlier systems, became more and more frequent and more and more complicated in the later systems. Characteristic of all Japanese diplomatic systems, and especially of the transposition systems, was the tendency of introducing an innovation in a simple form and following it with a series of complicating changes.[8] Solution of such systems would have been very difficult had analysis been limited to the final stages of these systems. Solution of cryptographic problems is frequently facilitated however by the reading of cryptographic-instruction messages, that is, messages, prepared in a current system or key, giving the users instructions relative to impending changes in the system or indicating new keys and the like. Hence, although cryptographic continuity is always profitable, it was exceptionally so in the analysis and exploitation of Japanese diplomatic systems. Japanese diplomatic traffic supplied the first translation for the Bulletin, submitted 28 January 1935, and the first transmittal of a message from the Signal Corps to G-2 in April 1936. As solutions were made and translations became possible, they were not always forwarded to G-2. At the time of the establishment of the Signal Intelligence Service in 1930, G-2 had expressed the opinion that the fundamental task of the Signal Intelligence Service should be training for a future emergency, not the production of intelligence from current material. As a result, transla-

8. As is now known, such a procedure is not confined to the Japanese.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

tions were forwarded at first more in the interest of showing what Signal Intelligence Service could do than for the purpose of providing intelligence.[9]

B. The Red Machine

Though the personnel of the Signal Intelligence Service had studied cipher machines at an early date, the first machine of this type which they encountered in actual intercepts was that known to the Japanese as the "A" Machine, a designation which was not then known to SIS personnel, who called it the Japanese "Red" Machine.[10] Originally the Red Machine contained, as it was later learned, two cryptographic mechanisms hereinafter called for convenience "cipher wheels" although they were not wheels at all in the ordinary sense. One "wheel" enciphered the 6 vowels and the other the 20 consonants. Thus, the resulting cipher text was composed of vowels enciphered only by vowels and consonants enciphered only by consonants--an attempt to reduce telegraphic expense by producing artificial words in the cipher text. Later the "six" wheel was used for any six letters.

---

9. The personnel engaged in this early solution work, under the direction of Mr. William F. Friedman, were Messrs Frank B. Rowlett, Solomon Kullback, Abraham Sinkov, and, later Messrs Robert O. Ferner, Samuel S. Snyder, Lawrence Clark, and Herrick F. Bearce. Mr. John B. Hurt served as translator. By 1938 Mr. Rowlett had the general supervision of Japanese solution; he and Mr. Ferner were concentrating in particular on the Japanese Red Machine.

10. The use of colors as cover names was adopted about this time, though not universally.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

A third mechanism, called for convenience a "control wheel", controlled the motion of the cipher wheels. In addition to the daily cipher sequence, 240 indicators for the three wheel settings had to be solved. The system, put into use before 1932, was undertaken for study in about 1935 and was solved by 1936. When work on the solution of the "Red" diplomatic machine had already been begun in the Signal Intelligence Service, Mr. Friedman, through a chance conversation with Commander J. N. Wenger of the Navy Code and Signal Section, learned certain details concerning the information which the Navy then had regarding a Japanese Navy cipher machine which the Navy was investigating. Acting on the assumption that the diplomatic machine might prove to be of similar type, the cryptanalysts of the Signal Intelligence Service attempted to determine the number of wheels in use in the machine, and this line of attack proved successful. As revealed in the report cited in footnote 7, page 26, a modification of the machine was on 1 December 1938 contemplated by the Japanese for the purpose of increasing its security. The last message received in this system was dated 21 August 1941, the system being superseded by the more secure "Purple" Machine, which had already been in use for several months and was employed concurrently with the "Red" Machine during those months by a few correspondents.

C. The Purple Machine

The most outstanding achievement in the cryptanalysis of Japanese diplomatic systems, indeed of any diplomatic systems, was the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

solution of the machine known to the Japanese as the "B" Machine and to the Signal Intelligence Service as the "Purple" Machine. It was the solution of this extremely secure system which was referred to in testimony given to the Joint Congressional Investigation into the Pearl Harbor Disaster as "the breaking of the Japanese Code."

Fortunately, the earlier and less elaborate "Red" Machine had already been successfully analyzed by the Signal Intelligence Service, and the traffic in that system was readable, but it was in a special secret Japanese cipher that messages appeared in the latter part of 1938 giving the authorization for travel for a "Communications Expert" named Okamoto, in order that he might put into service certain cryptographic paraphernalia termed by the Japanese diplomatic offices as the Type "B" Cipher Machine. This machine was to replace the then currently used Type "A" Machine for highly secret communications among the important Japanese embassies[11] throughout the world and the Foreign Office in Tokyo. On 19 February 1939 a message, bearing the date of origin as 18 February 1939 and sent in superenciphered code (K-1 transposed and enciphered by special "A" Machine procedure), was intercepted and found to give the effective date of the initiation of the "B" Machine as 20 February 1939. The "A" Machine was still to be used by all holders for certain classes of communications.

Among the first messages received after the effective date of

11. At Washington, Berlin, London, Paris, Moscow, Rome, Geneva, Brussels, Ankara, Shanghai, and Peking.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the "B" Machine were three messages, originating in Warsaw, which had a new type of indicator instead of the normal "A" type indicator. Since examination showed that these messages had not been produced by the "A" Machine, it was assumed that they had been prepared by the "B" Machine; but since 6 of the 26 letters were more or less of abnormally high frequency (as was also the case with the "A" Machine messages) it was also assumed that the "B" Machine used some of the basic principles of the "A" Machine. Further intercepts tended to corroborate this theory. The "A" Machine was continued in regular use at Hsinking and Shanghai and very occasionally (apparently when the "B" Machine was out of commission) the "A" Machine continued to be employed at the places which had been provided with "B" Machines.

After a brief study it was confirmed that the division of the letters into two categories (one group of 6 letters and another group of 20 letters), which was the basis of the cryptographic treatment in the "A" Machine, was retained in the "B" Machine but with a very important change: whereas in the "A" Machine the six letters comprising the "6's", as well as the twenty comprising the "20's", were enciphered by means of what had been deduced as being a rotating commutator, the stepping of which was controlled by a break wheel of 47 positions with certain skips in the cycle (the commutator could advance 1, 2, or 3 steps at a time), in the "B" Machine the "6's" were enciphered by means of a series of 25 heterogeneous and differently mixed alphabets, which were merely a carefully selected set of 25 of the possible

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

720 permutations or transpositions of six elements taken six at a time.

A deciphering chart or "development" was constructed to correspond with these 25 permutations. This chart was revised and corrected from day to day until it became certain that all its elements were absolutely correct. This having been accomplished (by 10 April 1939), it became possible, as a result of cryptanalytic techniques elaborated for the purpose, to decipher the "6's" in practically every message of any considerable length in the "B" Machine. It was found that, so far as the "6's" between two messages with unlike indicators were concerned, the only difference between one indicator and another was the starting point in the cycle of 25 alphabets. There were 120 different indicators but only 25 different starting points, so that four (in certain cases, five) different indicators represented the same starting point.

When the "6's" in a given message were deciphered, the plaintext values of cipher letters scattered here and there throughout the text became available, so that the skeletons of words and phrases offered themselves for completion by the ingenuity and the imagination of the cryptanalyst. For example, suppose that on a given day the six letters forming the "6's" were E, Q, A, D, R, and H, and the following text was at hand:

Cipher: B R A X E F Q C E V Q O O X H E C F D L N H Q R V Q P P L C E R P . . .
Plain: _ H E _ A _ A _ E _ E _ _ _ E R _ _ E _ _ R E Q _ E _ _ _ _ H A _ . . .

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

It is not difficult to imagine that the missing letters are those shown below:

Cipher: B R A X E F Q C E V Q O O X H E C F D L N H Q R V Q P P L C E R P . . .
Plain: T H E J A P A N E S E G O V E R N M E N T R E Q U E S T S T H A T . . .

In this process of filling in the plain-text values of the "20's" the cryptanalyst could be guided only by two things: (1) the positions and identities of the deciphered "6's" and (2) the context. For it speedily became apparent that any cryptographic relationship between the plain-text and the constantly-shifting cipher-text values in the case of the letters constituting the group of "20's" had been most carefully eliminated, disguised, or suppressed. This fact corroborated the conclusion drawn from all statistical and analytical tests made on the cipher texts of the various messages studied.

The process of filling in the plain-text values of the "20's" was therefore, as a rule, a very difficult matter, depending usually upon the particular assortment of letters constituting the "6's". If the text was in Japanese, there was, in addition to the difficulty inherent in the language itself, the added perturbation occasioned by the fact that the Japanese Foreign Office had, on 1 May 1939, instituted a species of "Phillips Code" in connection with their use of the "B" Machine, with a long series of arbitrary letters and abbreviations standing for numbers, punctuation signs, and frequently used combinations of letters, syllables, words, and sometimes complete phrases. For instance, the combination C F C represented period;

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

C C F represented paragraph; the single letter L (not normally used in Japanese) represented the diphthong ai; P represented ni; V represented long U; Q T Q represented Arita (shi) itashi tashi; B K W represented Beikoku (= United States); T K W represented Teikokuseifu (= Japanese Government); S N W represented Sukunakarazu, etc. The difficulties introduced by this code writing alone were quite staggering as well as exasperating, for often the "text", even when finally reconstructed, appeared more like code or a random assortment of letters than plain text. The following sequence, usually found at the beginning of messages, is a combination of Japanese plain text and the code groups already alluded to:

XFCGJ WFOVD DNOBB FYXFO CFYLC CFMSG TSJVR KHIFI CGURV FELBK WTLSI . . .

When separated into the proper lengths and decoded and translated, it stood for "Number 15 (part 1 of 2 parts) Secret, to be kept within the Department paragraph On March 16th the American Ambassador Grew," etc.

For the reconstruction of such text, the services of the Japanese experts were absolutely essential, and the work went very slowly, not only because of its difficulty, but also because the services of these translators were available for this problem only a small part of the time, when the traffic for the daily Bulletin permitted, and this was very seldom. It was found occasionally, however, after the "6's" in a given message had been deciphered, that these letters and their distribution throughout the message gave good indications of

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the presence, in whole or in part, of normal English text. In such cases, the "guessing" process was likely to be considerably easier because of the absence of abbreviations (except for punctuation signs, in which case these were a help), both because of the cryptanalyst's greater familiarity with the language, and because a larger number of workers was available. It happened that in several cases, after a few words had thus been obtained by pure "guessing," a clue was afforded as to the general nature of the message, and this led to a frantic search for a complete document which might be available either in our own files or in the files of other Government agencies. One case was found in which the "B" Machine message contained a paraphrased version of a message which had been transmitted in K-1 code. Advantage was, of course, immediately taken of this circumstance, but the entire text of the "B" Machine message could never be reconstructed from the paraphrased K-1 version, possibly because of the excellence of the paraphrasing, possibly because of the presence of abbreviations, or both.

At this point mention should be made of a favorable circumstance without which the Signal Intelligence Service probably could never have solved the "Purple" Machine. At this very period the United States Government was conducting negotiations with the Japanese Government looking towards an extension of the commercial treaty which had been in effect for a number of years but which was about to expire. As a result, a number of messages in English text had

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

been transmitted between Washington and Tokyo, and a small percentage of the intercepted traffic therefore happened to be in English. This fact greatly lessened the task of "guessing" words, phrases, and sentences in these specific messages, once the distribution and identities of the "6's" had indicated that the text of a message was in English. Now certain of these English-text messages could be fairly readily reconstructed, some of them to the extent of 90 to 95 per cent, because they consisted of quotations from documents and the documents in question were fortunately located and obtained, most often through the cooperation and good offices of G-2.[12] Had it been necessary to reconstruct the plain text of messages from Japanese text alone, the project would doubtless have failed, as did the British attempt being made at the same time, as was afterwards learned. The British, moreover, were handicapped by the fact that they were not in a position to obtain the texts of documents quoted in their original English form in messages enciphered on the machine, as in the case of the Signal Intelligence Service, which had access, through G-2, to the State Department records. However, even the Signal Intelligence Service found on some occasions that to obtain a document

12. The Signal Intelligence Service was forbidden to make any contact of this kind with any other Governmental agency, but every request had to go through G-2, with attendant delays.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

from the State Department required a comparatively long time.[13]

In all, the plain text for parts of some 15 fairly lengthy messages were obtained by the methods indicated, and these were subjected to most intensive and exhaustive cryptanalytic studies. To the consternation of the cryptanalysts, it was found that not only was there a complete and absolute absence of any causal repetitions within any single message, no matter how long, or between two messages with different indicators on the same day, but also that when repetitions of three, or occasionally four, cipher letters were found, these never represented the same plain text. In fact, a statistical calculation gave the astonishing result that the number of repetitions actually present in these cryptograms was less than the number to be expected had the letters comprising them been drawn at random out of a hat! Apparently, the machine had been brilliantly constructed to suppress all plain-text repetition. Nevertheless, the cryptanalysts had a feeling that this very circumstance would, in the final analysis, prove to be the undoing of the system and mechanism, and so it turned out.

In all the foregoing studies, several factors stood out. First,

---

13. In that early period the techniques of obtaining information of this kind had not yet been developed. In one important case, after G-2 had reiterated that a certain document did not exist in the State Department files, Mr. Friedman, by direct contact with the chief of the files of that department, obtained the document in question.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the basic law underlying the "B" Machine was of such character that the ciphering mechanisms seemed to start from certain initial settings and to progress absolutely methodically without cyclic repetition of any sort straight through to the end of the messages, the longest of which for which plain text had been recovered comprising over 1,500 letters. Secondly, two identical plain-text letters in sequence could never be represented by two identical cipher-text letters; nor could two identical plain-text letters 26 letters apart be identically enciphered. This phenomenon which was termed "suppression of duplicate encipherments at the 1st and 26th intervals" formed the subject of long and arduous study, fruitless experimentation, and much discussion. Thirdly, two messages with identical indicators on the same day appeared to be identically enciphered, and on direct superimposition (and written in a cycle of 26) showed themselves to be monoalphabetic within columns, but with the monoalphabets constantly, irregularly and unpredictably shifting from column to column. Fourthly, two messages with identical indicators on different days (with different plugboard arrangements into the machine) were absolutely different. Fifthly, two messages with different indicators on the same day (same plugboard arrangement) were absolutely different and showed no cryptographic similarities whatsoever, Sixthly, in each line of 26 letters two identical letters could be identically enciphered except at the first interval, that is, identical encipherments

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

could, and often did, occur within a line of 26 letters at all intervals, except at the first interval, although this phenomenon was rare at the second, third, fourth, and fifth intervals.

At the same time as the foregoing phenomena were being studied, intensive research was continued in an endeavor to establish primary or basic cipher sequences of the nature of those usually found in cryptographs with rotating commutators, rotors, and the like, such as the Hebern[14] and Enigma[15] cryptographs and our own M-134,[16] etc. For it was inconceivable that the machine employed a nonrepeating key of length corresponding to the total lengths of the messages. Moreover, theoretical considerations eliminated the possibility that an infinite nonrepeating key was being used. Somewhere, somehow, the existence of cyclically-repeating keys or sequences must be uncovered before solution could be effected. But all efforts to disclose the presence of cyclically-repeating sequences were fruitless. In one, and only one, case was there found even the slightest hint

---

14. On machines invented by Hebern, see Historical Background of the Signal Security Agency, volume Three, chapter VI.

15. On the Enigma as used by the Germans, see below chapters XVI and XVII. On a modification of the Enigma used by the United States Army (the Converter M-325, SIGFOY), see History of the Signal Security Agency, volume Eight, chapter II.

16. On the M-134, see Historical Background of the Signal Security Agency, volume Three, chapter VI; History of the Signal Security Agency, volume Eight, chapter II.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

of such sequences as were being sought. In a certain English-text message the letter E was found to be represented by Q, 26 letters away another E was found to be represented by Y, and again 26 letters away another E was found to be represented by V, making the sequence QYV; in the very same message the same trigraph QYV was found to represent three E's similarly spaced. Attempts to add to this QYV sequence were absolutely unavailing. In this long, exhaustive and tedious search for repeated sequences or partially repeated sequences much labor and energy was expended but it was realized that the difficulty was probably due to the paucity of the text, despite the number and length of the individual messages available for study and for which the plain text had been reconstructed. It became apparent that what would be necessary was to obtain, by some manner or other, several messages in the same indicator and on the same day, or else to convert several messages with the same indicator but on different days to the same base, before even the existence of such cyclic sequences could be detected.

In all the thousand or more messages on hand there were but a mere baker's half dozen or so cases in which there were two messages on the same day and in the same indicator. More than two had never been found and this was to be expected in a system with 120 different indicators available for each day. In one case of this rare phenomenon the plain text for one of the two messages was available, but very

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

little could be done even then as regards the solution of the other. For such a method of attack at least 20 to 25 messages, all in the same indicator and on the same day, would be necessary, and this was, of course, recognized as a perfectly hopeless expectation. There remained the possibility of converting several messages with the same indicator but on different days to the same base, and while this method of attack looked extremely difficult, it did not appear hopeless.

A method for this conversion to the same base was developed and termed the "identification of homologs." That is, an attempt was to be made to establish that a given letter on a certain day and another letter on a different day were treated in an absolutely identical or, more accurately speaking, homologous manner by the machine when set to the same indicator. This conversion process is too involved to explain here; it is sufficient to point out that, difficult though it is, it was successful in two cases. One of these yielded a set of six messages, all in indicator 59173, which could all be reduced to the same base. These formed the crucial set of messages from the study of which success in solution of the machine was finally achieved. (Tab 17)

Distribution tables of the letters constituting the text of these six messages were made. It should be stated that in four of these six crucial messages only fragments of plain text had been reconstructed, here and there; the complete or nearly complete plain texts of

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

only two of these six messages had been reconstructed. However, enough data were accumulated from these two completely reconstructed, and the other partially reconstructed, messages to yield distribution tables, which, on careful examination disclosed here and there the presence of repeated sequences. This, coming on 20 September 1940 at about 1400 hours, was the very first indication that a successful attack might be possible. There was excitement at this first glimmer of light upon a subject that had for so many months been shrouded in complete darkness and regarded at times with some discouragement. The nature of the distribution tables referred to is also too involved to explain here, but it should suffice to indicate that they exhibited certain relationships between the successive cipher equivalents of a given plain-text letter and the successive appearances of that plain-text letter in the cryptographic text.

As soon as the existence of cyclic or symmetric sequences became clear, attempts were made to uncover complete basic sequences of the type theoretically predicted. But many conflicts and inconsistencies soon developed, owing to the fact that the cryptographic laws underlying the shifting from sequence to sequence were still unknown. Concurrently with the work connected with straightening out and removing inconsistencies in these reconstructed basic sequences ran the work of uncovering the cryptographic laws referred to, and very soon the general nature of the latter became quite clear. All efforts were

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

concentrated upon the development of the specific laws and specific basic sequences applicable to the indicator under study, viz. 59173, with a view to uncovering all the cryptographic phenomena in this case and then searching for analogous phenomena in the case of other indicators. Certain qualified personnel from other sections were brought in to assist, and a considerable amount of night work was found desirable in order to push this study to completion at the earliest possible moment.

By 27 September 1940, just one week later, the work had progressed to a point where it became possible to hand in two translations representing the very first "solution" to the "B" Machine. Two messages of recent dates, both in the 59173 indicator, were available and were solved by applying the principles of solution by homologs, guided by the aid of the reconstructed basic sequences. It was all the more gratifying that this could be done on the very day that announcement was made of the signing of the Tripartite Agreement among Germany, Italy, and Japan.

Much work remained to be done, however, since only the data applicable to but one out of the whole set of 120 indicators were at hand. To solve the remaining 119 indicators appeared still to present a large problem. These solutions consisted of finding the initial settings of three 20-level rotary electrical cryptographic elements of 25 points each and finding the order in which these three elements

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

were brought into play within each indicator system. With but little slackening of the pace set by the personnel themselves, work progressed with vigor, and by 14 October 1940, when the first written report on the "Purple" Machine was prepared--a report, incidentally, which has been closely followed in the foregoing paragraphs—solutions were available for over one-third of the 120 indicators.

As to the mechanics of the "B" Machine, naturally the basic principles of its construction and operation were deduced from the cryptographic phenomena observable in the messages, and immediately plans were initiated for the construction of an equivalent machine for our own purposes. Orders for the material for two fully automatic machines were placed and expedited. While awaiting the arrival of this material, personnel of the Section designed and constructed a hand-operated machine, which was put into operation in the daily decipherment of current Japanese traffic. The cost of the parts in one "Purple" analogue amounted to $290.97, that for one keyboard typewriter unit $393.68. At the same time, a "Red" cryptograph was reconstructed on the basis of the new knowledge presented by the solution of the "Purple," at a cost of $174.17 for the necessary parts.

It cannot be too strongly emphasized that the construction of these analogues, as they are termed in the literature of cryptology, was based entirely on observation of the effect of the unknown and unseen Japanese cryptographic machines upon the plain text of the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

messages sent in diplomatic correspondence. How closely the American analogues resemble their Japanese counterparts is unknown, since no American cryptanalyst has even at this late date (June 1946) ever seen one of the Japanese "B" Machines. It is clear, however, that the analogues could and did perfectly reproduce the action of the "B" Machines. It would serve no useful purpose to give in detail at this point an elaborate description of the machine as reconstructed,[17] but it should be pointed out that a significant advance had been made by the use of switches of the type employed in automatic telephony. Tab 26.

The solution of the "Purple" Machine was the culmination of 18 months of intensive study, but there still remained the additional problem of the day-to-day solution of the keys themselves, the establishment, that is, of the daily plugboard arrangement or the order and identity of the wires leading from the keyboard into the cryptograph and thence out of the cryptograph into the printing unit. Eventually it was possible to predict what sequences were to be repeated when new ones were no longer being issued to the holders of this system. Machine-enciphered traffic continued to produce valuable intelligence and, with the changes in keys (as with the fall of Germany) and special methods of use and superencipherment (JAA-1,

17. For details concerning these early analogues see the report of 14 October 1940, by William F. Friedman, filed in the Office of the Director of Communications Research.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

JAB, JAD, etc.), new cryptanalytic problems had to be solved. But, in general, the processing of this traffic was speeded up to the point where only a few minutes sufficed to decipher a message for translation. Top priority was early placed on the handling of the traffic in this system used for the most secret and important diplomatic matters, and this continued until the capitulation of Japan in August 1945 caused the traffic to cease.

The story of the solution of the Japanese "B" Machine has been given in much greater detail than it will be possible to reach in the description of other solutions which will appear in subsequent chapters, partly because of the tremendous importance both to the production of valuable intelligence and to the development of the science of cryptanalysis, but also because from this one example the reader may derive a fair notion of the sort of development involved in all.

That solution was at all possible was due in very large measure to two facts. The first of these, the fortunate circumstance which made it possible for the cryptanalysts to have a considerable body of English text at their disposal, has already been treated sufficiently. The other factor which contributed to the success was the harmonious, well-coordinated, and cooperative teamwork of a group of cryptanalysts working for more than a year and a half on the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

problem.[18]

Before leaving the topic, some attention should be given to the fact that it was solution of the "Purple" Machine which made possible (as was brought out in 1945 and 1946 by the Joint Congressional Investigation of the Pearl Harbor Disaster) the reading of a considerable body of Japanese diplomatic traffic which was of great value in revealing the intentions of the Japanese in the months preceding the attack of 7 December 1941. This traffic did not, of course, reveal the exact time and place of the attack, but it did make clear that war was imminent. In this connection the testimony of Major General Sherman Miles, who in December 1941 was Assistant Chief of Staff, G-2, as reported in the Washington Evening Star of 3 December 1945 (p. A-4), is of the greatest interest:

---

18. The report of 14 October 1940, written very soon after success was achieved, mentions the following names of persons who participated in the problem: general supervision: William F. Friedman; specific supervision and coordination: Frank B. Rowlett and Robert O. Ferner; recovery of the "6's": chiefly Genevieve M. Grotjahn, Albert W. Small, and Samuel S. Snyder, assisted at times by Cyrus C. Sturgis, Jr., Kenneth D. Miller, and Glenn S. Laudig; engineering problems: Leo Rosen; assistance on the engineering problems: E. J. Hawkins, Sergeants Oscar Wilder, Jr., and Lawrence B. Roy; tabulations: Ulrich J. Kropfl, Mary Joe Dunning and Hazel Dronenburg; Japanese language: John B. Hurt and Paul S. Cate; clerical work: Frances M. Jerome and Mary Louise Prather; part-time assistance from other sections: Abraham Sinkov, Lawrence Clark, Delia Ann Taylor, Wilma Z. Berryman, and Edward E. Christopher, Jr. Mention is also made of the fact that through Commander L. S. Safford, Office of Naval Communications, the facilities of the Radio Laboratory, Navy Yard, were put at the disposal of the SIS in the construction of the analogues.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Mr. Gesell [counsel for the committee] informed the committee that he will be prepared later to offer a detailed record of the handling of important Japanese messages intercepted during the week before December 7, 1941, but not decoded and translated until a week or more after the attack.

Mr. Gesell said he is gathering data to show the monitor stations that picked up each message, when it was transmitted to Washington, whether by airmail or radio, and when it was received for decoding.

In discussing the delay in decoding these messages today, General Miles told the committee:

"The astonishing thing, gentlemen, is not that these messages were delayed, but that they were able to do it at all. It was a marvelous piece of work."

Among the possible causes for the delay in decoding were these:

a. The necessity for intercepting a considerable volume of traffic all sent in a single key before solution of that key is possible.

b. The creation of a backlog of traffic by a sharp rise in volume of intercepted traffic.

c. The extreme scarcity of competent Japanese translators.[19]

d. The fact that it is impossible to tell from raw traffic which message will be important and which may safely be laid aside until there is time for all. Only when a message has been converted to Japanese plain text can any one, and then only one who knows Japanese, tell which is important and which is not.

In making public earlier reports of investigations of the background of the Pearl Harbor disaster, the Government for security reasons withheld certain passages. As had now been made clear by

---

19. On this point, see volume Four, chapter III, section A, page 23.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the Congressional Investigation, those passages contained references to the success of the Signal Intelligence Service in solving the "Purple" Machine. (The machine was not so called but this is what was meant.) The reasons for concealing this fact were based on two considerations. In the first place, it was imperative that every effort be made to prevent the Japanese from learning that their most secret diplomatic system had been solved, for if they should learn the fact, they would most certainly either abandon the system entirely, in which case the work of the best cryptanalysts for several years would be nullified, or they would change as many elements in the enciphering process as possible under the prevailing conditions of distribution. In either case, the loss to current military intelligence would have been tremendous, as General Marshall eloquently pointed out in his letters to Governor Dewey of 25 and 27 September 1944. With the cessation of hostilities, of course, this consideration lost much of its force, but there was another consideration, in the long run much more vital to the defense of the United States: any success in solving a cryptographic system, if disclosed to the general public, has the immediate effect of stimulating other governments whose messages may now or at a later date be under study to endeavor to improve their systems in such a way as to render them impregnable. This is, of course, the aim of all cryptographic compilation bureaus at all times: knowledge that a given type of cryptography

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

has been solved by any government will at once greatly accelerate the process of research and development.

The publication in 1931 of Herbert O. Yardley's indiscreet book, [20] The American Black Chamber, had, indeed, precisely this effect: many governments, including some which were not even mentioned in the book (e.g. the Brazilian Government), at once began to prepare new types of cryptographic systems which would at least not be open to the specific kinds of attack which Yardley had shown to be successful. The cryptographic techniques which had been regarded as adequate in World War I were infantile when compared with those encountered in World War II, of which the "Purple" Machine is a conspicuous example. Had Yardley's book never been published, such a development in the cryptographic art might never have taken place.

Now that the solution of the "Purple" Machine has been disclosed to the world, all governments have been given notice that even a system of such high security as this is not invulnerable to attack. That several governments were aware of the existence of the system is a good presumption: at least two (the British and the German) are known to have attempted solution and failed, and their cryptanalysts (among the best in the world) may well have regarded a machine cipher of this type as indecipherable. Not only these two governments but all others

---

20. For a full discussion of this point, see Historical Background of the Signal Security Agency, volume Three, chapter IV.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

now know the contrary, and the race for a really indecipherable system will henceforth become much keener. It is not beyond the range of possibility that other governments will achieve success and that in a future war the enemy may have provided himself with an absolutely secure system.[21] The consequences of such a state of affairs to the gathering of military intelligence are, in the light of the recent development of the atomic bomb and its effect upon military techniques, incalculable. Yet even if the enemy does not devise an absolutely indecipherable system but only one of relatively high security, another war may then find the American signal intelligence services of that period without the forunate circumstances which, added to the skill of the cryptanalysts, made possible the solution of the "Purple" Machine.

D. Transposition

Transposition, long a favorite type of encipherment with the Japanese, became increasingly elaborate as new systems were introduced. Since new transpositions were usually introduced for basic codes already in use in older systems, the new systems were all the more readily solved. This was especially true of J-19 (JAE), a system put into use 1 July 1941. Although a difficult transposition problem with such complicating factors as a changing pattern of blanks within a matrix was

21. That this is perhaps not a purely academic possibility, but may be achieved before we realize it, is clear from developments in the cryptographic art. On this point, see volumes Eight and Nine.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

encountered in J-19, fortunately the known CA code was used for the base in a few early messages. The four daily keys, one for each of the four communication channels (Europe, the Americas, the Orient, and general) varied in length from 19 to 25 numbers. In addition to the daily changing keys, the pattern of blanks changed every ten days. Although the basic principles of this system remained practically unchanged during the two years during which it was used, certain changes were introduced in the second year of its existence. The same indicators were repeated, but changes were made in the sequences and patterns of blanks for the corresponding date of the previous year. Not only were the new keys recovered, but rules governing the changes were set up by which new keys could be predicted. A special auxiliary system (Q2 and Q3) involving a superencipherment was also encountered and solved.

In order to speed the solution of J-19, a special technique was evolved,[22] an adaptation of an IBM tabulator which would compare a sequence of cipher text with other sequences and show at what position digraphs most likely to occur could be produced. This machine, known as the electromechanagrammer, effectively reduced the time required for anagramming and increased the accuracy of the

22. By Messrs Rowlett, Ferner, Small, and Snyder.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

tedious operation.[23]

E. Organization of the Japanese Diplomatic Section

In September 1943 all Japanese diplomatic problems, formerly scattered according to their diverse cryptography, were brought together directly under one administrative head (Mr. Samuel S. Snyder) and designated B-III-c-4 (later B-III-f). The various phases of the work were divided among the following units: (1) Traffic and Indexing, (2) Purple Machine Cipher, (3) Decryptographing and Transposed Code Solution, and (4) Additive Problems.

The organization of the Section by the spring of 1944 is represented schematically in Tab . On 13 January 1945, when subsection B-III-f-1 handling Japanese diplomatic problems became section B-III-f, First Lieutenant (now Captain) Robert F. Packard was appointed Officer in Charge of the B-III-f Section.

F. The Work of the Section

The status of work on Japanese diplomatic systems in September 1943, when the group headed by Mr. Snyder was formed to handle all such problems, was as follows. The "Purple" Machine cipher system (JAA) had

---

23. Lieutenant John Skinner contributed much to developing the machine, and those who contributed to the recovery of keys included Messrs William Bryan, Joseph Petersen, Maurice Waltz, Sergeants George Hurley, Gwyn Evans, and Irving Massarsky, Misses Elizabeth Stephens, and Isabel Murdock, and Lieutenant Vilar Kelly. The J-19 section was headed for several months by Colonel J. J. Verkuyl of the Netherlands Army, who later became the head of the Netherlands cipher bureau in Brisbane.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

been solved three years previously, and all current traffic was in the stage of exploitation, and only occasionally (where new keys were used) of development. A cryptographic-instruction message had announced the termination of JAE (J-19) in July 1943. Several new Japanese diplomatic systems had been introduced: JBC, JBD, JBA, and JBB. JBB (transposition) was quickly solved in the J-19 unit with assistance from the Research Section of the General Cryptanalytic Section (B-3). As for JBA, a much more complicated transposition system, entry into the system was accomplished by the Research Section. This solution represents the accomplishment of an unusually difficult cryptanalytic task, the solution of an unknown code using two-letter and three-letter groups with an unknown transposition. On 15 December 1943 a change was discovered in the system whereby the pattern of blanks within the matrixes changed. Two recently introduced additive problems (JAM and JBC) were under study by a small unit, and the initial entry into the JAM system had been made. See Tabs 18 and 19 for JBA and JBC.

The newly organized Japanese Diplomatic Unit had made no provision for solving new systems. Available personnel was already devoting full time to the development of known systems and to exploitation. It was not possible to solve new systems in the scanty spare time that could be found for such matters. Accordingly, plans were made to install a special research group for these problems. The B-III Research Unit as it was then called, was asked to lend special assistance during

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

February and March 1944. The limitations that characterize the JBC system had been discovered, and through them entry into the system was made. Work on JBC went forward rapidly, once advantage could be taken of the limitation and of the additive pattern reflected in the cipher text. Solution of JBD was begun in March 1944. Development of JAM was suspended in December 1943 for lack of traffic in order to devote full time to the more profitable system, JBC; later, in September 1944, work on JAM was resumed. A study of the new systems introduced for the Greater East Asia Ministry (such as JBD and JBB) showed that they were of the same general type as the diplomatic systems.

A reorganization of the Japanese Diplomatic Section was required when, in March 1944, the Research Unit had progressed far enough with JBC so that the system was ready for exploitation. A Recovery Unit to handle JBC and JBA was set up. The decoding activities were thereupon transferred to the Indexing Unit. The Research Unit turned its attention in July 1944 to other unsolved problems (JAO, JBE, and others).

Although JBC and JBD had reached the stage of exploitation (the key books were completely recovered and all traffic was readable), the indicator systems remained unsolved. Messages could be placed in the key book by analysis and comparison of the pattern of the cipher text with that of the recovered key. In beginning work on the unsolved indicator systems, JBD was undertaken first, and it soon yielded to attack in June 1944. Following a similar procedure, the JBC indicator system was solved.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

G. Commercial Systems

Among the new systems facing the Research Unit was JBH, regarded as one of several new Japanese diplomatic systems. Unlike the additive systems (JBC, JBD, JAM) it used kana symbols. Since the Research Unit was concentrating all its effort on the additive problems, JBH was assigned in the spring of 1944 to a small group of cryptanalysts from the Machine Cipher Section. Both transposition and autokey substitution were involved. With the close cooperation of GCCS the traffic became readable and the system was then discovered to be commercial rather than diplomatic. It was concerned with the dealings of the great commercial companies in Japan, their subsidiaries, colonial development companies, and the various trade-control bodies in the government designed to exploit the conquered territories. The valuable economic information was welcomed by the Military Intelligence Service, and this provided an impetus for further work on commercial traffic.

Interest in traffic passed over the Japanese Domestic Network began in December 1943 with the visit of a British officer, Captain E. B. C. Thornett. The British considered that such traffic would be the main source of information after the War and of increasing importance during the War. It was not until the autumn of 1944, however,

---

24. An autokey system is defined in the ASA Glossary of Terms as an aperiodic substitution system in which the key following the application of a previously arranged unit of key is generated from elements of the plain or cipher text of the message.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

that interest became active. The reorganization to strengthen the Solution Unit made possible the handling of this additional traffic, which was of two main types, one sent in kana and the other in digits. Large commercial companies, banks, shipping firms, and consular offices all sent messages in many different systems over the Japanese Domestic Network, established for such purposes in the Japanese-controlled Greater East Asia area. This traffic was considered to be the best source of information on economic data, and the Military Intelligence Service valued it as much as the diplomatic information.

H. Liaison

Exchange of information and the sharing with cooperating cryptanalytic centers of responsibility for Japanese diplomatic problems had been the rule for several years. As early as 1938 collaboration with the Navy had become very close and a complete exchange of information was carried on. Between 2 February 1941 and June 1942 an unusual arrangement to share responsibility for Japanese diplomatic traffic was in force: the intercepted traffic was divided according to odd and even days of the month. Although this division was fair enough as regards credit, it was absurd from the technical point of view where continuity was essential. On his visit to GCCS during February and March 1941 Dr. Sinkov informed the British of the solution of the "Purple" Machine cipher system; since all their efforts to enter the system had failed, the British were delighted to receive the technical details of this solution. Of especial importance in liaison was the visit paid

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the Signal Security Agency in December 1943 by Captain E. B. C. Thornett, head of the Japanese diplomatic work at GCCS. During his two weeks' stay a conference on Japanese diplomatic solution work was held (20 December 1943) to analyze and perfect liaison between the British and American sections. Those participating in the conference were Major G. G. Stevens as British Liaison Officer, Captain Thornett as head of the British Section, Major Aurell as Chief of B-I, Major Rowlett as Chief of B-III, and Mr. Snyder as head of the Japanese Subsection of the Signal Security Agency. It was agreed that each section would inform the other of any cryptanalytic discoveries and would provide evidence in support of them; that messages of cryptanalytic value would be exchanged as well as texts of messages of intelligence value. It was also agreed that the American short titles would be used in referring to systems; a list of short titles with full description would be supplied Captain Thornett. Other data to be supplied included copies of work sheets, tables, IBM listings, JAA ("Purple" Machine cipher) development sheets, and a description of the IBM technique used on JAM traffic. GCCS would in turn supply messages and a report on JBG. There would also be a complete interchange of JBA traffic by cable to eliminate the serious traffic shortage. On 15 May 1945 many of the commercial systems (the readable systems JHE, JJI, JLV, JLA, JKC. JLR, JLS, and JLT) were turned over to the British as their responsibility. All the back traffic in these systems was sent to GCCS. The Signal Security Agency continued to be responsible for JHC, JLM, JLL, JJA-2,

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

JLW, JLD, JHC, and JLX.

Mr. Snyder went to Ottawa on 30 August 1944 to spend a week at the Canadian Examination Unit. After his return a new agreement was drawn up: results of research would be exchanged except for systems on which EU was known not to be working; IBM listings of research significance would also be exchanged as well as messages containing interesting cryptographic properties or cryptographic intelligence. EU would be notified of new systems and their short titles. A copy of the IBM decoding of JBC messages from Key Book I (prior to 1 February 1944) and selected translations on the Tokyo-Kabul, Tokyo-Kuibishev, and Tokyo-Vatican City circuits would be sent to EU. As cooperation went forward other material was also sent and the agreement was put to the test of application.

I. Training

Along with analysis and production, training was always a constant objective. From time to time special programs varying in intensity, length of time, and number of personnel involved were put into effect. Early in 1944 an extensive training program was instituted for all personnel in the Japanese Diplomatic Section. This was for several reasons:

1. To overcome isolation between groups formerly separated physically and administratively;

2. To make the Training Section more flexible by permitting easy reassignment of personnel within the Section;

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

3. To improve morale by showing the contribution of each person to the whole problem;

4. To develop personnel for newer and better jobs.

A course was given in cryptographic instruction in Japanese diplomatic systems; the general types, peculiarities, and analytic methods used on the systems were presented. An introduction to the Japanese language was offered by B-I in a two-week course constantly repeated for new classes of students. A few persons from the Section were assigned every other week to this special course. On the basis of performance in this introductory course, some students were selected to take the intensive six-month course in Japanese language given in the B-I school. Further cryptanalytic training was given to these graduates of the B-I school. From time to time also a short intensive course on Japanese diplomatic language was given for the benefit of the cryptanalysts.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER III. THE JAPANESE MILITARY ATTACHE SYSTEMS[1]

A. Early Work

The earliest Japanese military attaché systems known to the SSA were five codes studied by MI-8 in New York. The staff there referred to them regularly as "Army Codes" but the evidence is clear that they were the prototypes of the later JMA systems (Japanese Military Attaché). They were known as JK, JM, JN, JQ, and JR. JK was in use between May 1920 and February 1921, and was a syllabary using two-letter groups for plain digraphs and a few frequently-used words. It was not dissimilar from diplomatic systems of the same period. JM was a syllabary of the same type but was used (between October 1920 and January 1921) in eleven different encipherments, each with a distinguishing indicator. JN, in use between January 1921 and October 1922, was similar to JN, except that instead of using a single encipherment throughout a message, the code clerk might choose any of several, changing from one key to another merely by inserting a "switch group." JQ, in use between April 1921 and January 1922, and JR, used between November 1921 and January 1922, were both of the same type as JN.

---

1. The statements in this chapter are based largely on interviews with Mr. Samuel S. Snyder, Dr. Waldo H. Dubberstein, Captain Maurice H. Klein, and Mr. Edward E. Christopher, Jr., all of whom have long been associated with the problem, and upon the following documents: a. A. Sinkov and S. Kullback, diary kept during their study of JRL-3 (8 April--6 September 1938); b. S. S. Snyder, Cryptographic Description of the "88 .." System dated 21 July 1942; c. S. S. Snyder, Notes on RIK-5--JRN-4, dated 28 October 1944; d. Unsigned and undated description of JAQ; e. S. S. Snyder, diary of his work from 6 May 1940 to June 1942, the period of early study of JAS; f. Mary Hill and Kathryn Dubois (Buffham), Description of JAS (registered document 426-D). A report especially prepared for this History by Dr. Charles Prouty provided the main source of information for the later period.

Doc ID: 6554247

TOP SECRET CREAM

No other information is available concerning JMA systems until we come to the year 1938 when on 8 April Drs. Abraham Sinkov and Solomon Kullback first examined the current traffic in the system known as "RIK-International" or JRL-3 (Japanese Rikugun Letters No. 3). This system was in use from 1 January 1937 to 4 May 1939. Intensive study of the messages resulted in the discovery of the general outlines of the cryptography of the system and the reconstruction of 32 of the cipher squares used in it.

Following JRL-3, and for a short time concurrently with it, the Japanese used between 1 January 1939 and 31 January 1940 a system known in the SIS as "88.." (the four-digit discriminant regularily began with 88). It was partially solved during the summer of 1941 by Messrs. H. L. Clark and S. S. Snyder, who had, at the beginning of their work, the benefit of the solution by the British, brought back by Captain Sinkov on his return from his visit to GCCS in 1941, of the master additive chart used for the encipherment of the indicator, as well as the values of some of the four-digit groups.

Some progress was also made in still another system, JRN-4, (i.e., Japanese Rikugun Numbers, No. 4) in use during 1939. The analysts found that the basic code was the same as that of "88.." and that the additive keys were pages or blocks of 80 four-digit groups. The fourth of these earlier military attaché systems, Rikugunken, introduced in January 1937, was used during its six years of existence for material of low intelligence value. A

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

relatively insecure unenciphered trigraphic code, in 1937 it was reconstructed sufficiently so that the traffic could be read. The Japanese materially altered the system in October 1939 by changing the permutation table from which the code groups were generated, by enlarging the vocabulary, and by assigning code groups to plain equivalents after a new fashion. In a comparatively short time the revised code was recovered to the point where practically all messages could be read.

B. The Principal System (JAS)

By far the most important of the JMA systems, however, was that designated after September 1943 by the arbitrarily assigned short title JAS, formerly known successively as: RIK-2 (after Rikugun), "Scarlet" (a cover name), JRL-4, JMA (Japanese military attaché), and JAP (a short title). Introduced by the Japanese on 1 February 1940, JAS was the principal means of communication employed during the War for intercommunication among Japanese military attachés and between them and Tokyo. The cryptographic structure of JAS, while somewhat akin to its immediate predecessors, is much more complicated. JAS is an enciphered code. The code is based on: (1) a digraphic chart of 676 groups used to represent kana syllables, Japanese characters, punctuation, paragraph headings, and numerals; and (2) a tetragraphic chart of 676 groups, of which half represent further kana symbols and characters, the other half place names and the letters of the Cyrillic alphabet.[2]

---

2. These are necessary in order to spell Russian place names.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Encipherment is by digraphic substitution using a cipher square of 26 alphabets. The earliest square contained symmetrical standard alphabets but later mixed alphabets were used symmetrically, and finally, after 26 October 1943, 26 different mixed alphabets were used. The key is taken from a key book containing a random sequence of 135,200 letters arranged in five-letter groups, ten rows and eight columns on each of the 338 pages. The pages were designated by two letters (AA to MZ) and the second half of the alphabet provides variants (AA = NA). The ten rows and eight columns are designated by letters in a random sequence different for each page.

The code clerk, having encoded his message by the use of the two charts, writes out a key sequence over the code text and then converts by means of the cipher square to enciphered code text. He has chosen the key sequence at random, and so he must show by an indicator the point in the key book at which he began. The Japanese also indicated (though this was not technically essential but was added as a check on accuracy) where the encipherment stopped, by another indicator. The indicators are then enciphered by the use of a 26 x 26 chart, each of the cells containing four letters chosen at random. Finally, the message serial number is also enciphered by use of a 10 x 8 chart containing 80 five-digit groups of key to be used for this purpose. (The indicator was formerly enciphered by a prearranged group on a page of key book; the page was indicated by the control located in the first textual

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

group).

All five elements change at irregular intervals; furthermore, the serial number chart and the indicator key chart are integral parts of the key book and change as it changes. On 1 January 1945, for example, the third code chart, the ninth (or "I") key book, and the thirty-sixth cipher square were in current use. Aside from these periodic changes of the three elements of JAS cryptography, the principal cryptographic improvement in the system noticed since 1940 lay in the change in the type of cipher square used. The first contained standard sequences slid against each other; although the second to twelfth squares used a mixed sequence, the square still exhibited direct symmetry; finally beginning with square 13, introduced on the 26 October 1943, twenty-six unrelated random-mixed sequences were adopted. The Japanese, well aware of security requirements, in introducing these numerous changes in the elements of the system created a variety of cryptanalytic problems, no two of which were cryptanalytically alike. The extent of these changes is well shown by the following list of cryptanalytic achievements: 41 conversion squares recovered (12 had a single mixed sequence, and the remaining 29 were made up of 26 differently mixed sequences in each square); eleven[3] serial number key tables reconstructed, together with more than 16,000 letters of indicator key, and 862,000 letters of key

3. The serial number chart for JAS-1 has been recovered.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

in eight[4] key books recovered. At the end of the War the third code chart, the tenth key book with its subtractor and indicator key chart, and the forty-first conversion square were in use.

The successive changes (with American designations) are listed below:

code chart	key book	square no.	type of square	date introduced
1	A	1	Vigenère, standard sequence	1 Feb. 1940
2	B		standard	25 Jul. 1940
	C			4 Apr. 1941
		2	single-mixed	20 Aug. 1941
	D			25 Nov. 1941
		3	single-mixed	20 May 1942
	E			30 Jul. 1942
	F			1 Feb. 1943
		4	single-mixed	11 Feb. 1943
		5	single-mixed	22 Mar. 1943
		6	single-mixed	22 Apr. 1943
		7	single-mixed	25 May 1943
	G	8	single-mixed	10 Jul. 1943
		9	single-mixed	25 Aug. 1943
	H	10	single-mixed	18 Sep. 1943
		11	single-mixed	27 Sep. 1943
		12	single-mixed	5 Oct. 1943
		13	random-mixed	26 Oct. 1943
		14	random-mixed	10 Nov. 1943
		15	random-mixed	22 Nov. 1943
		16	random-mixed	1 Dec. 1943
		17	random-mixed	11 Dec. 1943
		18	random-mixed	21 Dec. 1943
3		19	random-mixed	1 Jan. 1944
		20	random-mixed	11 Jan. 1944

4. No key has been recovered in the first or "A" key book, or in the second or "B" key book. These were already obsolete when solution began, and the traffic is not thought likely to be of sufficient interest to justify the labor of solution at this late date.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

code chart	key book	square no.	type of square	date introduced
		21	random-mixed	21 Jan. 1944
		22	random-mixed	1 Feb. 1944
		23	random-mixed	15 Feb. 1944
		24	random-mixed	14 Mar. 1944
		25	random-mixed	4 Apr. 1944
		26	random-mixed	25 Apr. 1944
	I	27	random-mixed	11 May 1944
		28	random-mixed	1 Jun. 1944
		29	random-mixed	15 Jun. 1944
		30	random-mixed	5 Jul. 1944
		31	random-mixed	1 Aug. 1944
		32	random-mixed	17 Aug. 1944
		33	random-mixed	6 Sep. 1944
		34	random-mixed	14 Oct. 1944
		35	random-mixed	15 Nov. 1944
36		36	random-mixed	17 Dec. 1944
		37	random-mixed	28 Jan. 1945
		38	random-mixed	5 Mar. 1945
		39	random-mixed	10 Jun. 1945
	J[5]	40	random-mixed	6 Mar. 1945
		41	random-mixed	10 Jun. 1945

This list reveals that, except for the date of the original introduction (1 February 1940), the Japanese have never introduced a new code table, a new cipher square, and a new key book simultaneously. At every change in the system, at least one of the three elements remained unchanged, and for the most part two remained unchanged. Not until 10 July 1943, when key book G and square 8 were introduced simultaneously, were the analysts forced to reconstruct both a new square and a new key book at the same time. Even then, the square introduced was of the same general type as its predecessor.

---

5. Used concurrently with I-period key book from 5 March 1945.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

C. The Cryptanalytic Attack

By 1 February 1943 the cryptography of the system was clearly understood, and methods of cryptanalytic attack on the problem had been developed. Some preliminary study had been conducted by the Signal Security Agency in 1940. In November 1941 the British Government Code and Cypher School (GCCS) informed the Signal Security Agency by cable that it was concentrating on JAS and presented its achievements. These consisted in the identification of the serial numbers, the control, the structure of the serial number key chart, and the discovery that the groups now known to be the enciphered indicators were nontextual. A month later GCCS had discovered the nature of the indicator, its control, and the use of the variant in one of the letters indicating the page of the key book. This use of a variant was for some time a troublesome problem, since GCCS thought that a table 13 x 26 (instead of a standard square 26 x 26) was used to encipher the first page letter. This problem was finally solved by the Signal Security Agency in June 1942 after recovery of the first mixed square (the second cipher square used).

In the meantime further progress had been made. The dates of various changes in the system were ascertained, and traffic could thus be studied in the proper groupings. In April 1942 Colonel Tiltman of GCCS, who had made the initial entry, visited the Section, bringing with him the results of his study and the pertinent data on a long series of London-Tokyo messages. These messages were carefully studied with the result that the page numbers of the key book which they used were recovered. The true

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

structure of the key-book page was at last understood to be ten rows and eight columns of five-letter groups.

GCCS had begun the study of the more recent material and in June 1942 reported the first successful entry into the text of JAS messages. British intercept stations had gathered, in very complete form, a special series of messages broadcast from an illicit station later identified as Budapest. Because these messages were found to be enciphered consistently with key beginning in the top left corner of every other successive page, and because plain-text cribs were available, it was possible to superimpose messages and to derive code values, first for numbers and then for punctuation and simple kana. This series was the basis of code reconstruction, which proceeded rapidly when other messages broadcast in normal channels (traffic between Tokyo and military attaches in various capitals) were included in the overlaps. In October 1942 structure of the tetragraphic code chart was established, and a rapid recovery of code groups was effected by reason of this knowledge.

With this successful entry into the plain text messages, the various problems of recovering key from overlaps were first encountered. It was decided to concentrate all efforts on the most recent traffic available, that of the "C" and "D" (arbitrary designations assigned by the SSA) key books: "C" was in use from 4 April 1941 to 24 November 1941 and "D" from 25 November 1941 to 29 July 1942. Preliminary study was made of the newly instituted "E" period, but it was realized that traffic would have to accumulate before a successful attack could be made.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

During the ensuing months traffic in both "C" and "D" periods was read, and "E" period messages were gradually placed in depth and indicator keys recovered.

D. Production Methods

The experience gained in the early recovery work proved of inestimable value. Various cryptanalytic techniques involving indicator, key, and conversion square were explored. The recovery of key from overlaps was studied from many points of view; frequency tables, grilles used in conjunction with charts of logarithmic value, frequency of code digraphs, and isologs were all examined and exploited as a means of rapid key recovery. Growing experience and a study of solved messages for stereotypes led to an increased production of key and deciphered messages. The Section began to divide into groups of specialists who became exceedingly proficient in their respective tasks. The Traffic group processed all incoming messages and listed the important cryptographic data of each message on a five-fold card, three copies of which were used for research purposes. The Research Group recovered serial numbers, key charts, indicator keys, and conversion squares to give the Overlap Unit the correct placement of messages in depth and the squares necessary for the recovery of key. The Processing Unit prepared the deciphered and decoded messages for the translators. See Tab 20.

From that time on the Section made a notable record of production and subsequent solution. For example, the possibility of a simultaneous

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

change of key book and conversion square had long been regarded as posing an exceedingly difficult problemn. Such a change was first made on 10 July 1943. The fact that the order for the change sent by Tokyo was read in a cryptographic-instruction message saved considerable time. On 25 August recovery of the cipher component of the new square was completed by the section and sent to GCCS. From then on solution proceeded rapidly. Of somewhat less importance, perhaps, was the discovery by the SSA that the cipher square introduced on 25 October 1943 consisted of 26 differently mixed sequences. Hence the immediate development of new techniques of indicator key recovery was necessary since the "H" period had begun only on 18 September, and the key recovery was not complete. Moreover, the technique that had been developed for use with a square having a single mixed sequence was no longer possible. Since the new type of square required more traffic and more study for its recovery, the time lag at first was from three to four weeks. Gradually techniques were improved to the point where squares were recovered within three or four days of their introduction. In this work, the analysts were materially aided by the fact that key had been recovered so extensively that messages enciphered by means of the new square could be placed by matching key to pairs of cipher and plain text that conform to limitations of the square; i.e., because of the structure of the square certain constatations signified that identical letters of key had been used and a search in the key book could be made to locate repeated letters at the same intervals as those between the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

significant constatations. In the subsequent reconstruction, personnel experienced in overlap work and translators did excellent work in recovering plain text. The great success of this unit in rapid square recovery led GCCS to request its liaison officer to report in detail on the techniques employed.

Courses in key recovery from overlaps developed the talents of new members of the Section, and courses in research techniques made experienced specialists available. Of great assistance in speeding up production were the electromechanical deciphering machines. By depressing successively the keys on a typewriter keyboard to correspond to successive elements of the text, electrical impulses were set up which were then combined by means of a plugboard with electrical impulses corresponding to the successive elements of the key. A printer then printed the resultant text. These machines made it possible to place messages before indicator keys were solved and in general performed tasks that had hitherto been regarded as impossible because of the man hours required for the manual performance of such tasks.

Another great timesaver was the use of an IBM procedure evolved after the introduction of the square employing 26 different mixed sequences. Listings of all possible decipherments of a column of an overlap doubled the speed of key recovery. During the winter of 1943-44 the code texts of a large number of deciphered messages were prepared, and an index of solved messages was printed by IBM. This index, showing code text which

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

had in previous messages followed each digraph, was most valuable in key recovery. At about the same time work was begun on a noun and topical index of JAS traffic. This, too, has been fruitful especially in cases where only a few messages used the same key or where the content and structure could be inferred. In addition it was found by B-III in January 1943 that Tokyo sent out each Saturday beginning 17 January 1943, a multipart stereotypic report on the progress of the war in all theaters. This report, as was discovered in B-II on 31 May 1944, was duplicated in Japanese Army systems, and the isologs thus available were exploited by both Sections. Repeated messages and messages containing reference to other messages were also a fruitful source of partial cribs which increased production.

The most serious problems facing the research group following the "G" period and the subsequent introduction of the square using 26 different mixed sequences were the "I" and "J" periods, when the Japanese changed key book and conversion square simultaneously. In preparation for such a problemn the research group had already made intensive studies, using "H" period traffic for experiments in the use of new techniques. The experience and techniques gained from this study indicated that solution was possible if enough traffic was available and if the Japanese code clerks continued to follow their customary practices in the use of code and key materials.

In both instances, the Japanese inadvertently afforded considerable help. Before 11 May 1944, the date of introduction of the "I" book,

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

two valuable messages had been read. The first of these revealed that because of travel difficulties, Madrid could send to Tangier by cable (using the "H" book) two new conversion squares for use with the "I" book. Since these were to be sent by cable, it was questionable whether copies could be obtained. Work proceeded on the basis of the second message, which revealed that Bucharest would continue using the "H" book and the current conversion square. This meant that all circulars out of Tokyo would be sent in both "H" and "I" books and that plain text would be available for the "I" messages. From these isologs the limitations of the new square were determined; that is, the letters missing from the columns of a square, each row of which contained a different mixed sequence. Recovery was proceeding slowly but was speeded up when GCCS obtained copies of the Madrid-Tangier messages containing one of the cipher squares.

The introduction of the "J" period on 5 March 1945 brought additional difficulties: it was known that key book and conversion square would both be changed and that the Japanese were taking precautions to avoid sending isologs. A special system for circular messages was established since the Japanese had been unable to provide Madrid and Lisbon with new cryptographic materials because of the allied blockade. Fortunately however, the attaché in Cortina d'Ampezzo never received the special instructions for circular messages, and some eighty messages sent to him in the usual way provided the needed isologs for the messages in

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the special circular system. These isologs were quickly and effectively compared by rapid cryptanalytic machinery (RAM) in a search for instances where the plain fit the cipher text and for two such instances falling on the same page of the key book. Several overlaps, established in record time, made possible the reconstruction of the current cipher square and the recovery of indicator key. At the present time indicator key recovery is very nearly complete; 144 overlap pages have been set up, and 21,000 letters of key have been recovered. As traffic accumulates the recovery of the remaining key will proceed, and the information received and sent by the military attaches and the War Office in Tokyo will be available.

By 31 May 1945, 40,028 message parts sent to or by Japanese military attachés and the War Office in Tokio had been processed by the Section for translation; 17, 565 such messages represent a complete coverage of all JAS traffic from 18 September 1943 to 5 March 1945. During this period nearly half of the messages received were available for translation within a few hours of their receipt. And even now, after a series of changes in cryptography has posed difficult cryptanalytic problems, some messages are read upon receipt. The intelligence contained in this traffic has been of great interest to G-2, who consider JAS to be the most important and reliable source of information out of Europe during the War. Indeed, it has been remarked that the Japanese military attachés were the most valuable secret agents working in Europe for the United States. The language is extremely technical and the diversified subject matter includes detailed descrip-

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

tion of German equipment, installations, and troop concentrations. One group of messages contained information of such vital importance about German installations on the French coast that they were flown immediately to the President and the Prime Minister in conference in Teheran.

E. Other JMA Systems

Another military attaché system that has yielded valuable information is JAT. It was instituted in February 1943 exclusively for the transmission of cryptanalytic material. Until November 1941 such traffic had been sent in JAS and from that time until February 1943 in an adaptation of JAS using an obsolete key book. JAT traffic, though infrequent, did yield results when studied; it was found to be enciphered by a 10 x 26 square and to use stereotyped message beginnings. The conversion square, which was in use during the entire life of the system, was recovered, and the traffic was read. A lapse in the use of this system from October 1943 to July 1944 prevented any further study; but with an increase of traffic after July, study was resumed, and the successful overlapping of messages resulted.

References in JAS traffic revealed the general nature of some of the JAT traffic. In addition the specific content was sometimes known; e.g. U. S. State Department cryptographic materials. With this information analysts were able to secure the correct materials and use them as cribs. The key thus recovered was used to read a long sequence of

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Helsinki traffic, which revealed cryptanalytic work on American systems. Outlines of Russian codes, descriptions of Russian, American, and Turkish systems as well as raw American and Turkish traffic constitute some of the substance of the traffic of this system, practically all of which has been read.

Two other systems, JAR and JAS-1, have been examined by the Section. The former, used exclusively by the attaché in Moscow and occasionally by other attachés, is known to be a one-time system, consequently little hope of solution can be offered. JAS-1 used key book "M" or 13 and a separate set of conversion squares, but it is cryptographically identical with JAS. Introduced in February 1944, it was discontinued in January 1945. The bulk of its traffic dates after August 1944 and is known to consist of technical data and reports sent from Germany to Japan. Research is continuing, even though solution seems unlikely. GCCS regards the problem as unsolvable with the available traffic considered inadequate for successful analysis.

F. Liaison

Close operational liaison has always been maintained with GCCS. Telegrams, letters, and packages are sent and received daily. Information received from the British regarding Japanese military attaché problems antedates Pearl Harbor; in November 1941 a telegram was received containing observations on the encipherment of the message number. Exchange of information became more and more frequent as progress was made in both agencies. In April 1942 Colonel Tiltman of GCCS visited

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the Section and brought material with him. By October 1942 it was agreed that the two sections divide the work of recovering the key book, each section being responsible for the recovery of one-half of the total number of pages. This arrangement proved satisfactory and had continued for the recovery of subsequent key books. The relative contributions of the two centers cannot really be evaluated, but GCCS contributed more in the way of original entry into the system, and the SSA more in the enormous number of keys and sequences which it recovered and in the constant research and techniques which it developed for recovery after a change in one of the elements.

G. Personnel and Training

A number of cryptanalysts have been associated with the Japanese military attaché problems. Preliminary analysis was carried on by Colonels Kullback and Sinkov. Mr. S. S. Snyder had the longest experience: he made the preliminary studies in 1940 and carried on his work from November 1941 to June 1943. Mr. Frank Lewis contributed various techniques of indicator recovery. Dr. Ronald Cassity was in charge of indicator research from October 1942 to 1943.

The present Research Unit has had the benefit of a nucleus of the same personnel since work began on the "G" period in July 1943. Mr. E. E. Christopher has been in charge during this entire period, and with him have been Mr. Emmett Bennett and Dr. Charles Prouty.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Others who have been associated with the problem are Mr. Dale Underwood (summer of 1942 until May 1944) Dr. William M. Seaman, (September 1943 until February 1945), Mr. Gustavus Swift, and Miss Virginia Alexander.

Following Mr. Snyder's departure from the JMA Section, Captain Donald McCown became head of the Section, and when he left for overseas duty in March 1944, his assistant, Captain Maurice H. Klein, became head. Dr. Waldo H. Dubberstein has been in charge of all overlap work since the autumn of 1942.

Among the senior members of the overlap group are Miss Anne Barker, who has been with the Section since July 1942, Mr. Laurence Bordy, who has been in charge of the swing shift since April 1943, Miss Lorna Pottberg, with the Section since September 1942, Miss Dorothy Moore, Mrs. Peyton Jacobson, and Mrs. Edith Wright.

The personnel of the Section, now numbering more than eighty persons, is subdivided into a number of units, but this organization is not rigid and personnel may be shifted easily from one to another as occasion demands. The units are:

1. Research Unit (Mr. Edward E. Christopher, Jr.)
2. Key Recovery or Overlap Unit (Dr. Waldo H. Dubberstein)
3. Traffic Unit (Miss Nellie Butler)
4. Records Unit (Miss Anita Schwab)
5. Machine Unit (Mrs. Katherine Zimmerman)
6. Aids to Translators Unit (Miss Josephine Worth)
7. Administrative Services Unit (Miss Lena Robertson)

The functions of most of these Units are explained by their titles;

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the Records Unit performs the task of decoding and deciphering by hand methods, while the Machine Unit performs the same operation by machine methods. The Aids-to-Translators Unit renders valuable service to the translators who are, however, not an administrative part of the JMA Section but belong to a Unit of the Language Branch (B-I), which occupies contiguous quarters and works in the closest of liaison with the JMA personnel. It is deemed worthy of nothing that the integration of cryptanalytic and translator personnel within the same section contributed much toward the high efficiency of the Section. Such integration was not applied in the case of other Sections of the SSA engaged in work on Japanese communications. This Unit (B-I-m), under Mr. Francis R. Millard, translates all the messages which the JMA Section has made readable and also gives much needed linguistic assistance to the research and key recovery units of the section. This form of cooperation between the branches has been carried on officially since 1 July 1943, but before that period certain Japanese experts from B-1, notably Dr. Percy Buchanan and Mr. Charles M. Legalley, had been more or less permanently on loan to the JMA section.

The achievements of the present JMA section may be attributed in large part to the fact that for more than two years a large section has been continuously at work on one principal problem. More than two hundred different persons have now been part of the JMA section, of whom more than eighty are still present. (These figures are exclusive of the 18 persons in B-I-m.) More than fifty of the eighty persons in the Section had been in it for more than a year on 1 January 1945.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER IV. GERMAN DIPLOMATIC SYSTEMS[1]

A. Early Work

Exploratory work was first done on German diplomatic systems in 1937 by Dr. Solomon Kullback while he was stationed as a cryptanalyst in the Hawaiian Department.[2] Upon his return to Washington in the spring of 1938 he began to develop a German section by interesting a number of other cryptanalysts in the problem.[3] The first task was the reconstruction of the unenciphered German code book DESAB No. 3 (the discriminant and abbreviation for Deutsches Satzbuch). This code book, insofar as the literal groups were concerned, was made largely readable before the book itself was compromised in July 1940, when the FBI obtained a copy in Panama while going through the effects of an unregistered German diplomatic agent. Other problems that engaged

---

1. Source material for the statements in this chapter include reports on file in the German Diplomatic Section and the General Cryptanalytic Branch, and interviews with Dr. Carl P. Klitzke, Dr. Ray W. Pettengill, Colonel Solomon Kullback, and Mr. T. A. Waggoner.

2. On his work in this period, see Historical Background of the Signal Security Agency, Volume Three, Chapter VII.

3. Among those associated with German diplomatic solution in the early period were the late Dr. Charles J. Mendelsohn (who had been a member of MI-8 in World War I and was at this time a reserve officer); Messrs Frank Lewis; Robert O. Ferner; Samuel S. Snyder; Miss Delia Ann Taylor (Mrs. Sinkov); and Dr. Ray W. Pettengill. Later the section expanded rapidly as solution progressed. By the summer of 1943 it was organized as follows under Lieutenant (now Major) Leonard J. Seidenglanz with a total strength of nearly 100 people: Analysis (Messrs F. A. Brugger and C. E. Reed); Files, Production, and Translation (Lt. G. H. Mundinger); Special Problems, New Problems (Lt. A. T. Prengel); Related Problems and Reading.

Doc ID: 6554247

TOP SECRET CREAM

the attention of the analysts in the early days were an encipherment by the Kryha Cipher Machine of the Rudolf Mosse Commercial Code, some clandestine systems used in South America, and the Port au Prince digraphic substitution system. But the principal problems and greatest achievements lay in the solution of the so-called Keyword, or "Floradora",[4] system (GEC), and the one-time pad system known as GEE.

B. The Solution of GEC

GEC was the most important German problem in respect to volume of traffic and value of intelligence, at least until the solution of GEE, which did not occur until 1945. By September 1939 the GEC system was in full use between Berlin and the German diplomatic missions throughout the world and therefore carried information concerning Nazi political intentions and operations. Early examination revealed the use of additive-enciphered five-digit one-part code; later investigation led to the recovery of a key book of 10,000 lines of basic additive to provide double encipherment, books of daily indicator keys, and a conversion square. The Germans, relying for security on the double encipherment, made continual changes in the daily indicator keys, changed the basic text additive book once during the War, and introduced changes in the manner of indicator and text encipherment. The underlying code (DESAB Code Book No. 3) remained in effect for several years. On 1 January 1942 it was superseded, except in Dublin, by Code Book No. 4,

4. This name is a good example of the spontaneous coinage of vigorous and humorous terminology by GCCS.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

which had been compromised by the Navy about July 1941. Each of the two text additive key books contained 5,000 lines of six five-digit groups (apparently made up at random) and 5,000 lines complementary to the first 5,000. A message was normally subject to double encipherment; one line of additive was first applied to the plain-code text and then a second line of additive was applied to the sum thus produced. Since, when the system was being solved, there were 10,000 lines in all and each line of basic additive could be combined with itself and with all other lines, the effect was a potential resultant additive key of 100,000,000 ÷ 2 lines, each containing six five-digit groups.[5] This eight-digit indicator for the two lines of additive used was enciphered by an eight-digit indicator key which changed every two days. These keys probably were, as later discovered, made up by the same machine[6] (with alterations) which was used to make up the GEE additive. There were several different books of these keys for each station for different types of traffic.

Initially, the entire cryptographic system was deduced at the SSA strictly by analysis. The British, who were aware of the nature of the system through information furnished by agents, had given up the system as hopeless and had stopped intercepting the traffic. Solution at first

---

5. This was true potentially, but of course the system was not initially set up in such a way that there could be no repetitions of additive lines. Actually, lines were reused and this fact permitted recovery of key by the overlap method. Later modifications prevented deliberate reuse of resultant key.

6. See section C below.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

involved discovering messages enciphered with the same combination of additive lines and recovering the combined additive and the two-day-period indicator keys. Early in the analysis, the two-day period for the encipherment of the indicator, its bipartite nature, and the fact that additive was arranged in six five-digit groups to a line were recognized.

The assumptions about the indicator were verified when, in 1940, copies of indicator keys to be used for 1941 were obtained from material also compromised by the FBI in Panama. The Germans added constants to these keys in order to disguise them for use after their compromise until new keys could be provided. [redacted]

[redacted]

EO 3.3(h)(2)
EO 3.3b(6)
PL 86-36/50 USC 3605

[redacted] Of great importance in the more rapid derivation of basic additive key from the combined additive key already recovered was the first 50 lines of the basic additive book, which had been turned over to the British by a French agent after the fall of France. With the occupation of Iceland, some complete and partial substitution tables were captured which led to the solution of that traffic which contained isologs of Keyword traffic. In April 1942 worksheets found by British agents in a waste basket in the German consulate in

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Monrovia provided the clue to a new procedure used in the double encipherment. Throughout the work such cribs as circular numbers, signatures, and isologs in other readable systems, especially the solved Port au Prince system, proved helpful. Early in 1941 the code clerks in Buenos Aires and Rio de Janeiro fell into the habit of preparing in advance combined additive lines using shifting starting points in order to save the time and trouble of adding different lines together; thus, a number of messages were readable before the system was completely solved.

The problem facing the German Diplomatic Section from the beginning was one of recovering the 5,000 lines of basic additives from which the 50,000,000 lines were to be made up. The compromise of the first 50 additive lines by the French agent in 1940 speeded the solution because, through the use of the 50 compromised basic lines of additives, any combined additives which contained one of the 50 lines could be split and the other line of the combination be determined. Progress was rapid, and the cooperation with GCCS was of great importance in speeding the work. The first translation was submitted in March 1941. By April 1942 recovery of basic additives was progressing rapidly, for, as more additives were accumulated, more messages could be superimposed and more basic additives and two-day period keys could be derived. Also, there was the consideration that the recovery of one basic additive yielded its complementary line as well, so that the solution of one additive key yielded two. By 15 February 1943 all of the 5,000 basic lines of additives of the first book (TANGENSTAFEL) had been

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

derived. By late August 1943 all of the basic additives of the second book (GRADTAFEL), which had come into effect in most stations on 1 January 1942, had been derived. Recovery of the latter was speeded (1) by the fact that resultant additive was used as soon as recovered either by combining two lines from one book or a line from each book, and (2) by the fact that many isologs were sent. By May 1943, 50 per cent of the back traffic and 25 per cent of the current traffic was readable. Full-scale production methods had been in the process of being set up. Earlier the magnitude of the problem had made it imperative to devise for current traffic machine methods of indicator-key recovery. New procedures were added for handling a growing accumulation of traffic that became available for development and exploitation once the original entry was made. A process of IBM decoding of messages was worked out, but the greatest contribution of IBM to the problem lay in the field of two-day period key recovery, a method being devised which ran a possible crib through 50,000,000 possibilities in two hours. A system of priority rating speeded the handling of the most important messages. By the summer of 1943 some 500 messages a week were being decoded, of which 350 were translated and published in the Bulletin. In 1944 some 4,000 messages were read, approximately 95 per cent of the traffic intercepted. The intelligence in these messages included among other things the most secret diplomatic transactions, commercial dealings, and the reports of German spies throughout the world. Since this system continued in use to the last chaotic days of the War, even when the location of the German Foreign Ministry

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

was unknown, the German Diplomatic Section was able to maintain its production of valuable intelligence to the very end.

C. The GEE System

The chief efforts of the German Diplomatic Section were directed in 1945 to the solution of the German Foreign Office cryptographic system, which was designated by the Signal Security Agency as GEE. This system had been in use since at least 1925 for the highest-security traffic, and a tremendous volume of intercepts had been accumulated in GEE. Early study had indicated that GEE was an example of a one-time pad system. As this term is defined within the Signal Security Agency, a true one-time system involves encipherment by a completely random key specially prepared for use with a single message and of such length that it does not repeat within a message. One-time systems are of two basic types: (1) those which use pads of key sheets which are torn off and destroyed when they have been used, and (2) those which use tape which can be fed into a cipher machine and then destroyed. It was known that in GEE the Germans were using the pad system because some of these pads had been captured in 1940 by the FBI from a German agent passing through the Panama Canal. Since the cryptanalysts of the Signal Security Agency believed then, as they still believe, that a system which uses a completely random key never repeated either within a message or in other messages, is indecipherable, there was little hope in their minds that GEE could be solved unless keys were reused. Therefore,

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

except for comparison of key recovered from cribs with captured pads, work on the problem was abandoned in 1940, though traffic was still intercepted and stored. In September 1943 the research was taken up again by Mr. Thomas A. Waggoner, at that time head of the Cryptanalytic Unit of the German Section, and was continued with some difficulty until approximately March 1944, when a few workers were assigned to it for clerical assistance. From August 1944 until January 1945 the research was carried on by Mr. Waggoner and a staff of from 10 to 18 of the clerical personnel.

Research had begun to a certain extent in 1940 when the pads of additive were taken from the agent in Panama. At that time, a standard IBM Index, referred to as the "XYZ Index", was made up, and the distribution of five-digit groups was of random expectation.

Research was then dropped, but it began again in September 1943 on the supposition that GEE additives had been reused as, indeed, some cryptographic instruction messages read in GEC had directed. In a long and careful study of data collected in testing this hypothesis, it was natural that a close scrutiny should be directed to the series of captured pads of additive already mentioned. Finally, however, it was decided to study all the compromised additives and all additives which could be derived from GEC-GEE circular isologs in the same index. This complete additive index revealed relationships between the additive digits on various pages of a number of pads, so that it became clear that the additive groups comprising the key were not really random, as had

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

been supposed.

This discovery was like a shot in the arm to the personnel of the German Diplomatic Section. In December 1944, shortly after the discovery was made, the entire Research Group together with a great number of new personnel was assigned to the GEE problem.

This arrangement was to continue for many months, and most of the normal increment of the Branch was earmarked for it. By June 1944, 110 people were working on the problem. GCCS was, of course, promptly informed of every step in progress from almost the very beginning of the early discoveries. The first real entry into the system is dated from January 1945, when a message was read in the SSA through the prediction of the additives employed in its encipherment.

In the course of one and one-half month's research following the initial discovery that the additive groups were only apparently random, the cryptanalysts discovered the principle by which the additives had been constructed. The discovery of relationships between corresponding digits on different sheets of the same and of different pads made it possible to reconstruct 240 basic sequences of digits used in the construction of a homogeneous block of sheets. When those were studied, it seemed probable that some kind of machine had been used in the construction of the additive. The recovery of the elements of the machines used in the construction of the compromised additive and of the additive derived from GEC-GEE isologs made much easier the recovery of the elements in other homogeneous blocks of material used.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

The cryptanalysts of the Signal Security Agency did not know exactly what the German machine was like, nor did they need or wish to know, but the principles of key reconstruction discovered were incorporated by them into a specially designed additive-generating machine which greatly facilitated the exploitation of unread messages, especially in the case of the traffic sent between Tokyo and Berlin.

A working plan for the exchange of cryptanalytic information with GCCS proved most satisfactory in keeping the two centers thoroughly up to date in matters of sequence solution and identification, indicator systems, and the like. Certain special cribs, together with cribs provided by messages in GEC, aided considerably in the placement and solution of messages. In order to produce current intelligence, translations were made directly from the overlapped messages. After the 240 sequences for a given setting of the additive-manufacturing machine had been derived, the Research Section was faced with the problem of determining the setting point for each of the 240 wheels. Moreover, when the wheels were reset by hand for a new batch of material, the settings for each of the wheels had again to be determined. In most cases earlier settings of the wheels in the machine were of no help in determining later resettings of the wheels. These resettings, many of which were recovered, were solved on overlaps in which the arithmetic of solution of normal additive was supplanted by the arithmetic of a machine-generated sequence. With the pressure for intelligence, means of rapid recovery and

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

production, IBM processes for slide-testing cipher text against known settings of the additive machine were devised as well as high-speed decoding methods for large quantities of messages. Various IBM listings for the purpose of studying all pad sheets which had not been placed on the Berlin-Tokyo and Tokyo-Berlin circuits were tremendous time-savers and facilitated all phases of the work beyond all possible hand methods.

Vital intelligence of immediate value was supplied to persons or agencies requesting this priority material. In the case of several long, partially-placed messages containing important intelligence, the Director of MIS made a special request for urgent action in order to complete them. Many other messages containing intelligence of special interest to MIS were processed upon receipt of priority request lists. According to a member of MIS, the intelligence recovered was of utmost importance in the spheres of politics, scientific advance, technical data, and production (especially of aerial and other munitions). For example, these messages revealed that the Japanese were using a medium tank, certain types of aircraft, and a jet-propelled jeep hitherto unsuspected. As regards knowledge of enemy materiel, these were the most noteworthy bits of information received in the final months of the War.

It is only proper to say, in the case of both GEC and GEE, that even though solution <u>was</u> theoretically possible without the material compromised by the FBI and by the French agent, both solutions would

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

have been highly unlikely without that material. As for GEC, overlaps on the 50,000,000 possible lines of combined additives were very scarce. In fact, it is doubtless the case that, given the total bulk of traffic in GEC, many of the 50,000,000 lines were never used more than once. In the case of GEE, however, the most important factor in making solution possible was that GEC had been solved previously, thus providing cross-system cribs from which very valuable additive could be removed. The books of additive compromised by the FBI, in addition to the thousands of additive groups available from the cross-system cribs, facilitated solution immeasurably.

It might be said, therefore, that the cryptanalytic achievements in the solutions of GEC and GEE stand about on a par with one another, considering all aspects of both solutions. The GEC solution was certainly more painfully laborious than that of GEE, and in some points it was more difficult; but the fact that the GEE system had long been put aside because it was known to be a one-time system caused the success in solving the system to seem far more spectacular than had seemed the success achieved with GEC. The GEE solution caused debate as to whether or not the system were really a one-time pad system, since the additives, when looked at in the one right way of the all but countless numbers of possible ways, was <u>not</u> random in the strictest sense of the term. Nevertheless, the solution emphasized the fact that the sole weakness of many a so-called "one-time" pad system might

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

lie in the nature of the construction of the key, and also raised the question whether or not the keys used by the Signal Security Agency for American one-time systems were really random.[7]

The whole question had an interesting sequel when the Signal Security Agency began to obtain the studies of German signal-intelligence services based on captured documents and interrogation of prisoners (the TICOM Studies). Evidence has come to light that the Germans called the machine which they used for producing the GEE keys the "Nummerier-maschine" or "Nummerierwerk"; that they had three such machines, introduced in 1925, 1927, and 1933; that these were nothing but job presses with an arrangement for printing digits by means of 240 (in a later model 250) wheels on the periphery of which were embossed printing types. The machines were so arranged that these wheels could be prevented from stepping for 30 impressions; that is, if desired, 30 copies of each printed page could be made before stepping would take place. But in actual practice they printed only two copies of each page: one for enciphering, the other for deciphering. How the machine worked was, for the most part, not known. The foregoing statements are based largely on a folder containing papers (TICOM 1282) relating to the maintenance of the machines.

From a British source, however, it is known that in 1925 a Mr. Lorant of the British firm, Loranco Limited, offered the British

7. See volume Eight.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Foreign Office information concerning a machine which they were supplying to the German Government. The cryptanalysts of GCCS did not show much interest in this machine, but it was clear from the description that the Germans would use the machine for precisely the same purpose as the "Nummeriermaschine" described above. The captured documents, however, contain no hint that the source of the machines was British: they rather point to certain German manufacturers known by name. It therefore becomes doubtful as to whether the machine of which the British knew as early as 1932--the year Mr. Lorant divulged the information to the British Foreign Office--was exactly the same one now under discussion; but it seems clear that it was the source of the idea for the "Nummerierwerk". It is interesting, however, to speculate on what savings of time and money might have been made had the British attempted to exploit in the solution of GEE traffic the information they had obtained in 1932.

D. Miscellaneous Systems

A special adaptation of the Keyword system was introduced late in 1941 for Dublin, where the Germans found it impossible to deliver new key books or code books safely. Three lines of additives were used in the encipherment of the message which gave cryptographic instructions for the system, involving elaborate disguises and a transposition of the digits of the additive. But, despite the additional complexity of the system, the Dublin two-day period indicator keys were recovered,

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

and by May 1943, 90 per cent of the traffic was readable.

In 1944 instructions came for a new system of encipherment of certain portions of the total GEC traffic with three additive lines, which were to be obtained by a special usage of the two-day period indicator keys. The nature of the special usage of the indicator keys and certain pattern limitations in the construction of the indicator keys made possible, in many cases, the solution of the three additive lines used.

The reconstruction of DESAB (plain code called GED), an unenciphered one-part code in use since 1922 and the underlying code of GEC and GEE, was an easier task than the solution of GEC and GEE but quite laborious. About 90 per cent of the traffic was readable from a partial reconstruction, and the first translation was submitted in 1940. When a compromised copy of the code was obtained in July 1940, the work of the code reconstructors was verified, and the analysts could devote all their time to key recovery in GEC.

The Port au Prince digraphic substitution system, GEB, in use between 16 November 1939 and 15 July 1941 and solved early in 1942, employed 100 tables and 1000 keys. Isologs in GEC proved of great benefit to the solution of this system, which in turn, made available isologs to be used in the solution of GEC.

Another solution was that of the so-called "FELIX" system, an encipherment of the one-part Rudolf Mosse Commercial Code, used for espionage in South Africa. Still another system was the GEG system,

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

employed in Las Palmas, which was put into use on 15 January 1943 and on which work began the following November, the first translation being submitted on 5 June 1944.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER V. THE ITALIAN SYSTEMS[1]

A. Early Work

Active work on the solution of Italian cryptographic systems began in the SIS toward the end of 1938, though traffic had been collected over a period of four years. In charge of this study was Dr. Abraham Sinkov[2], who was assisted at various times by a group of cryptanalysts, among whom were Messrs Samuel S. Snyder, Albert W. Small, Vernon E. Cooley (April 1939-May 1940), and Mrs. Wilma Z. Berryman (November 1939-February 1942).

Since the new Italian Section possessed no information concerning current Italian systems or any used in previous years,[3] attention was turned to a general examination of all available intercepts, to the segregation of homogeneous bodies of traffic, and to a study of the systems in which sufficient traffic seemed to justify a hope that solution was possible.

---

1. The statements made in this chapter are based on the personal recollections of Mr. A. Ferdinand Engel, who during 1942 prepared an account of the progress made up to that time in solution of Italian systems. This account was, in 1944, brought up to date by Captain George E. McCracken.

2. Dr. Sinkov, who was one of the earliest cryptanalysts to be employed by the SIS, was from 1936 to 1938 at work at Headquarters, Panama Canal Department, in cryptanalytic activity. While there, he had first studied Italian diplomatic traffic, but not much progress was made before he was ordered back to Washington. During World War II he was on active duty and rose to rank of Colonel.

3. An attempt had been made during the First World War to solve one Italian system, but no success had been realized.

Doc ID: 6554247

TOP SECRET CREAM

A large two-part pentagraphic code (AR30 = ITD), tentatively designated as "X", and a smaller one-part code (RA = ITI), tentatively designated as "TRUJILLO" from the fact that it was the only system used for communication with Ciudad Trujillo, received the special attention of the small group of analysts during the year 1939. AR 30, only recently introduced by the Italians but very widely distributed, was at first believed to be unenciphered. It was discovered, however, that a simple transposition of the elements of each code group was used in the case of some stations, but, since most of the traffic came from stations which did not use this transposition, the effect was almost the same as if no transposition had been used. When, in 1944, a photograph of the code book became available, it was discovered that all[4] of the traffic was transposed, but by then the effect of the transposition had been completely minimized, since the reconstructions had all been made in the most widely used transposition.

Meanwhile, occasional circular messages sent elsewhere in AR 30 were sent also to Ciudad Trujillo in RA-1, a circumstance which afforded an entry into the latter system, even though little traffic was then available. By February 1940 solution of both AR 30 and RA-1 had progressed to a point where the problem had become increasingly linguistic. To meet this need, Mr. A. Ferdinand Engel joined the staff, and in April 1940 Mr.

---

4. As a matter of fact, it was later discovered that a very small number of messages had been received in which the form of the code group was identical with that in the code book.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Edward E. Christopher, Jr. joined the cryptanalysts at work on the Italian problems. Dr. Sinkov, Mrs. Berryman, and Messrs Engel and Christopher continued to devote most of their time to the reconstruction of the AR 30 code book, and, as new traffic permitted, to that of the RA-1 code book as well. Though progress was necessarily slow (since AR 30 contains more than 30,000 groups), the results of this work were generally reliable, so that by the end of 1940 occasional translations were possible in both systems. From that point on it was a matter merely of carrying forward the day-to-day study of the partially recovered text to increase the breadth and prediction of the identified vocabulary.

Early in 1941 Dr. Sinkov was temporarily relieved of his duties with the Italian Section and ordered to active duty as Captain in the Signal Reserve for the purpose of making a visit to the British Government Code and Cypher School (GCCS) in London in connection with Anglo-American plans for cooperation in the cryptanalytic field. The choice of Dr. Sinkov for this mission proved especially lucky, for the British were prepared to make their first major contributions to American cryptanalysis precisely in the Italian sphere. It is gratifying to recall that the accuracy of the first American solutions in the Italian field was fully confirmed by the longer experience of the British analysts.

Consequently, upon his return to Washington in April 1941 Captain Sinkov was in a position to extend the activities of the Section to those Italian systems which formerly had been impossible to solve

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

chiefly because the Section was not familiar with Italian cryptographic habits. To help handle the greatly expanded activities of the Section, six reserve officers, all with some training in cryptanalysis, were assigned to the Italian Section in May 1941: Lieutenants M. E. Rada, C. H. Hiser, O. W. Stephenson, P. E. Neff, C. E. Girhard, and L. G. Derbyshire,[5] of whom all but the last were transferred to other sections or sent into the field in the course of the following year.

Besides the continuation of the studies of AR 30 and RA-1, cryptanalytic attention was turned to new systems for which a considerable backlog of traffic was available:

1. RA-1, in a more difficult encipherment than the one already studied;
2. AR 38 (tentatively called "Y"), a two-part code similar to AR 30, to which some study had already been devoted;
3. Additive encipherments;
4. Impero code reconstruction;
5. AR 25 code reconstruction.

This additional work involved the solution of digraphic substitutions as well as additive and code recovery.

Captain Sinkov, Mr. Christopher, Mrs. Berryman, and the officers devoted their attention to problems of encipherment. After having acquainted himself with these, Mr. Engel turned to the problems of code recovery, especially to that of Impero, for which the British had

5. Major Derbyshire was Officer in Charge of the Romance Language Section at the time of his reversion to inactive duty in October 1945.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

supplied a partial reconstruction. Current traffic, almost always readable, was light. For this reason, and because of insufficient personnel, code recovery of one of the codes (AR 25) was abandoned until the following year, when special circumstances made a restudy of this code imperative. As soon as possible after the return of Captain Sinkov from England, two specialists in the Italian language, Miss Elizabeth S. Doane and Mr. Henry A. Sauerwein, Jr., were added to the Section in order to satisfy the greatly increased linguistic needs. Thus, extensive code recovery and, for the first time, regular translations of current messages in several systems were made possible. Regular exchange of information with the Italian Diplomatic Section of GCCS was mutually advantageous in the recovery of substitution tables, additives, and the code values. Less specific but equally important was the information which the British generously made available from their previous experience to fill the American picture of Italian cryptographic history.

At various times in the first half of 1942 the Italian Section was increased by a number of persons.[6] The new personnel made up for the

6. These included Miss Olga Brod, Private Stuart W. Frazier, Captain (now Major) Gordon T. Fish, Dr. Burton Phillips, Sergeant (afterwards Lieutenant) Joseph Greenberg, Dr. Margaret J. Rickert, Dr. Mary T. Campbell, Dr. Collice H. Portznoff, Miss Frances G. Blank, Mrs. Frances R. Moss, and Sergeant (now Lieutenant) Donald F. LaSala. Miss Blank is the only one of these persons who had remained with the Section continuously; Dr. Campbell, after nearly two years in the Military Cryptanalytic Branch, has recently returned.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

gradual loss, in the course of the preceding year, of the reserve officers who had been transferred elsewhere and also for the departure of Mr. Sauerwein in June 1942. A very serious loss was caused by the transfer of Major Sinkov in May 1942 to the Cipher Bureau, Brisbane, at which time he was succeeded by Captain Derbyshire with Mr. Engel as technical director.

Up to this point all work on Italian cryptographic systems had been carried on by a single unit. While additive recovery and code recovery frequently require somewhat different skills not always united in a single person, both operations are best carried out by personnel working side by side, with constant collaboration resulting in advantage to both. Such collaboration had been constant in the administrative organization of the SIS during the period when it was housed in the Munitions Building. When, however, the units were transferred to Arlington Hall Station on 24 August 1942, a radical change was made in the administrative arrangements of all units in what was then called "B Branch", the cryptanalytic branch of SIS. The older sections, organized around the various languages, were broken up and a new arrangement made on the basis of method. Thus all additive units were brought under one administration and all code units under another. The old Italian Section was divided into two units, one of which was assigned to code recovery and put under Captain Fish, while the other, made up of the additive recovery personnel, was placed under Dr. Phillips, since Captain Derbyshire was relieved

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

at this time of his duties with either unit.[7]

After the abandonment of the linguistic organization, constant liaison was necessary between the two Italian units, located as they were, at a considerable distance from each other. A compromise arrangement was made by the assignment of two members of the Code Recovery Unit to the Additive Unit while remaining, administratively, part of the Code Unit. Still later it was possible for the two units to be quartered in the same wing of Operations B Building, and finally, in the summer of 1943, the two units were administratively reunited under Lieutenant Duke, who had in May succeeded Major Fish as Officer in Charge of the Code Unit.[8]

The Code Unit continued the study of Impero, RA-1, AR 30, and AR 38. Another code (AR 40) of the same type as AR 30 and AR 38 was introduced in June 1942. The problem of reconstruction was undertaken by Miss Doane.[9] By October 1943 current traffic was almost completely readable. Meanwhile, the British sent a compromised copy of an older code, RA Tascabile,

---

7. Shortly before the change was made, First Lieutenant (now Captain) Francis Duke had joined the Section, and simultaneously with the change First Lieutenant (now Captain) George E. McCracken was also added. Both of these officers were assigned to the Code Recovery Unit under Captain Fish.

8. At this time Captain Derbyshire, who had rejoined the Additive Unit as its supervisor in January 1943, was assigned elsewhere.

9. Miss Doane was assisted at various times by Lieutenants Harold M. Barnes, Jr., and Glanville Downey.

TOP SECRET CREAM

Doc ID: 6554247

the predecessor of RA-1, which thereby relieved the American analysts of this task. They also sent a copy of Y-1, which proved useful in additive recovery and permitted the decoding of a small number of older messages, which, had they been readable when received, would have had a high intelligence value.

Upon resuming his direction of the Italian Additive Recovery Unit in January 1943, Captain Derbyshire, with the assistance of an enlarged staff (11 new members), laid the groundwork for a new attack on Italian additive and digraphic-substitution encipherment. This work was greatly impeded, however, by a decline in the bulk of intercepts in the enciphered systems. This decline had begun as early as November 1942, when Chile broke relations with the Axis, and the volume of intercepts continued gradually to decrease until the fall of Mussolini on 25 July 1943. As an aid to additive recovery, the older messages in AR 25, which had not been seriously studied since 1941, were again examined through the preparation of completely new message print. This new message print was necessary because the encode of AR 25 was now being used for generating additive sequences. The successful solution of traffic in an Italian commercial system, which had been received ever since 1940, was accomplished between February and April 1943. When the encipherment was removed, the basic code proved to be a repagination of a standard, non-secret Italian commercial code.

Most of the Italian diplomatic systems were in code, but one cipher

Doc ID: 6554247

TOP SECRET CREAM

system, the so-called Digepol (Direzione Generale di Polizia), used since the end of 1941 by secret service agents in East Africa, was examined by the Cipher Section (then called B-III). The nature of the cipher was discovered, and key recovery was progressing rapidly in the Cipher Section when a complete solution was received from the British in April 1943; thereafter the traffic was processed by the Decryptographing Unit (B-I-c), and translated by the Italian Section.[10]

It was in August 1943 that the two Italian units were finally reunited under Lieutenant Duke, but this arrangement was of short duration, owing to the fact that after the fall of Mussolini in July, traffic declined to such an extent that there was too little work for the large staff. Accordingly, on 27 September 1943, Captain Duke was given administrative duties elsewhere, and at the same time Lieutenant McCracken, Miss Doane, Dr. Campbell, Dr. Rickert, and Mrs. Moss, were transferred to a new unit, leaving to carry on the Italian systems only Dr. Silber, Miss Blank, and Miss Price. Soon afterwards Dr. Silber was also transferred elsewhere and Miss Price was reassigned, with the result that for the first six months of 1944 the Italian Unit consisted solely of Miss Blank.

---

10. Two new persons were added to the staff in the early summer, Dr. Gordon R. Silber and Miss Jehanne Price, who were responsible for the solution, in October 1943, of the Funchal digraphic substitution system.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

A description of Italian problems was begun by Mr. Engel in the autumn of 1942 and carried on by him until he left the Italian Section in the summer of 1943; it was finally completed and edited by the co-operation of members of that Section, particularly Dr. Silber and Miss Blank. This was issued as Italian Codes and Ciphers 1939-1943, a landmark in the description of foreign cryptographic materials and their solution. In October 1944 the study was continued by Lieutenant McCracken, then a member of the Recorder's Section, in Epilogue: Summer 1944, which completed the story of Italian solution to that date.

Since the autumn of 1943 intercepted Italian traffic continued to remain at a low volume. The enciphered codes, AR 30, AR 38, and AR 40, were still used by such European stations as continued operations. The most striking change, however, was the great rise in the use of plain text for governmental traffic, particularly in the Far East, where the representatives of the Republican Fascist Government were not, at least at that time, permitted to communicate with their government in code. Occasionally they used Japanese systems for their messages, but for the most part they employed plain text. The existence at the same time of two Italian governments created some confusion, but in the end no system was used in identical fashion by both governments, though each government continued to use some of the older materials in different ways.

The year was marked by a new form of Impero traffic (ITA), introduced in 1944 by the Royalist government. This was similar to the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

older form of ITA used by the Mussolini government prior to 1943, that is, the Impero code enciphered by five-digit additive. The additive sequence is taken from the encode of the Impero code itself, of which a photograph is available. A polyalphabetic substitution cipher was introduced for communication between the Royalist military attachés at Madrid and Ankara. The British were fortunate enough to intercept information giving most, if not all, of the details, so solution was rapid.

The Republican Fascist government introduced a new encipherment of the old book RA-1 (IMS), solved even though only seven messages were available. The encipherment consisted of a seven-digit running additive. The same government also introduced a new code of the general type of AR 30, AR 38, and AR 40, which, providing sufficient traffic is intercepted, will yield to code recovery, and a second system of which little is yet known. Later the Italians were once more permitted to employ code communications in the Far East, using AR 38 in two forms of encipherment, one very simple transposition, the other not yet solved.

The most significant developments of the year, however, involved, not the current traffic intercepted, but the fortunate capture of a large number of cryptographic materials which did much to increase our knowledge of the various cryptographic bureaus maintained in the past by the Italian ministries of Foreign Affairs, War, Navy, Aeronautics, and Interior. These materials were obtained partly by capture in the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

course of military operations and partly as a result of diplomatic negotiations made possible after Royalist Italy became an ally of the United Nations. Included are copies of all but one of the Italian diplomatic codes which had been studied and many others which had been used prior to American interception (one 30 years old), as well as three diplomatic codes which were apparently available for future use but had never been found in traffic intercepted here. In addition, the Italian Section now possesses copies of ten military codes ranging from large two-part codes for use by highest echelons to divisional and regimental units, and also some codes for highly specialized purposes, as well as two naval codes and one used for police work by the Ministry of the Interior. All of these materials are discussed in the Epilogue: Summer 1944 already mentioned.

The most gratifying result of the receipt of this material is to be derived from a careful comparison of the captured codes with the reconstructions made in the Signal Security Agency. No essential feature of these systems escaped the notice of the cryptanalysts engaged in their reconstruction. Objective tests to prove the accuracy of the identifications of code-group values showed that the reconstructions were extremely accurate.

In the following list are presented the results of a comparison of a hundred groups, chosen at random from each of the five codes indicated:

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Code	Percentage Identical	Percentage Nearly Identical	Total[11]
AR 25	50	45	95
AR 30	51	44	95
AR 38	47	32	79
AR 40	53	32	85
Impero	54	38	89
Average	51	37	88

This means that an average of 88 per cent of the code groups in the reconstructions were correctly identified. The 12 per cent incorrectly identified would not greatly effect the accuracy of translations, since it may be presumed that these were groups which occurred but rarely in the traffic. One of the erroneous identifications in AR 38, for example, was a group which had occurred but once in more than 10,000 messages. It may therefore be stated with confidence that accuracy of the translations approximated 100 per cent.

In the year which has passed since the receipt of the captured cryptographic material, the Section has continued to read with little difficulty the systems used by the Republican Fascist Government, though minor changes had been made. The Allied Control Commission in Rome required the use of deposited cryptographic material. When Allied control ceased in May 1945, the Italian Government instituted new systems, which at the end of the Fiscal Year 1945 had not been read, though excellent

11. An Analysis of Captured Italian Cryptographic Material, a summary of Epilogue: Summer 1944 to Italian Codes and Ciphers 1939-1943) is presented in IL 3834-A.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

progress had been made on their solution, particularly in the traffic of the Rome-Washington circuit.

Captain Duke, who served as American representative on the Cipher Security Mission in Rome, returned to the SSA with added insight into the cryptographic habits of the Italians. The information gained from cooperation with the British in this mission will doubtless be useful for a long time to come.

A summary of the achievements of the Italian Section include the following:

1. Independent solution of several two-part codes and several systems of encipherment, as well as the completion of many partial solutions supplied by the British.

2. Correlation of fragmentary information gathered by both the Signal Security Agency and the Government Code and Cypher School by cryptanalytic means, together with the evidence presented by the captured documents themselves, into a fairly complete picture of Italian cryptographic habits, not only for the period of five years when active cryptanalysis of Italian systems was being carried on in the Signal Security Agency, but also throughout the last 30 years.

3. Production of a considerable volume of translations of the Italian diplomatic correspondence in the period 1939 to the present, containing intelligence of value to G-2.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER VI. THE FRENCH SYSTEMS[1]

The history of the solution of systems used by the various French governments may be divided into three periods: (1) the period from April 1941 to June 1942, when all work on French systems was concentrated in a single section;[2] (2) the period from June 1942 to September 1943, when the different functions of solving and processing French traffic were performed in a number of smaller units, each charged with a single operation; and (3) the period from September 1943 to the present, when all of these operations were once more united in a single French Section.

A. The Early Period (April 1941 to June 1942)

Work began in April 1941, or perhaps a little earlier, in a new unit which was known simply as "Mr. Bearce's section," from the name

---

1. The statements made in this section are based on interviews with the following persons; Majors Stanley Clark and John N. Seaman; Captains William S. Smith, Thomas H. Glenn, and John E. Carroll; Drs. Caleb Bevans, Albert Howard Carter, Ruth Cherniss, and Katheleen Munn; Miss Helen J. Bradley; Mrs. Helen Siegel; Mr. Paul K. Hartstall; Miss Katharine L. Swift; and Mrs. Marjory M. Max-Muller. In addition, the following progress reports were examined: Captain John E. Carroll (1 September 1942 to 29 January 1944); Captain Thomas H. Glenn (22 February 1943 to 29 January 1944); Captain William F. Edgerton (8 and 15 February 1943); First Lieutenant Lee P. Howard (10 November 1942 to 17 April 1943); a special report by First Lieutenant Stanley Clarke (31 August 1942); records of the French Decode Unit kept by Miss Katharine L. Swift (16 October 1942 to the present); and a volume containing information pertaining to all French systems. These documents are now on file in the French Section (B-III-a-1).

2. Until January 1942 this unit also had in its care those systems in Spanish and Portuguese which then received any attention, but in that month the so-called South American Section was formed, and these systems were thereafter studied in it. See chapter IX. See Tab : a diagram showing the successive changes in the administration of the French problems.

Doc ID: 6554247

TOP SECRET CREAM

of its supervisor, Herrick F. Bearce, who was identified with work in French until shortly before his transfer overseas as Captain Bearce at the time of the North African invasion.[3]

This was, of course, a period of pioneer work, and the staff was also responsible until January 1942 for traffic in all other Romance languages except Italian,[4] which, since late 1938, had been studied in a special unit.[5] In spite of the extent of this task, the staff had by September 1941 succeeded in isolating from the voluminous traffic then available two French systems, both unenciphered codes: one a one-part code (FBT) with a five-letter group; the other, a two-part code (FAV) with a four-letter group. Progress on the recovery of FBT, carried on up to this time by Mr. Garman alone, was more advanced than that on the other. IBM indexes had been made, and the result of the combined efforts of Messrs Garman and Smith was that, in mid-December 1941, the one-part code was readable. The capture by the Canadians of the Miquelon copy in January 1942 compromised this system. Progress

---

3. He had with him Mr. (now Major) James Moak; Lieutenant (now Major) E. Dale Marston; Miss Rosalie Harding (Mrs. Bash); and Miss Sudie Jones (Mrs. Hanson); and, for the language aspect of the work, Mr. Allen D. Garman, for many years a federal translator; and later in September 1941, Mr. (now Captain) William S. Smith. In October 1945 Lieutenant Colonel Bearce became Officer in Charge of the Romance Language Section.

4. As a matter of fact, only a few systems in French, Spanish, and Portuguese were being studied at this time.

5. See chapter V.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

on the two-part code was less satisfactory until on 26 December 1941 the Section received from the British a partial reconstruction of the code. The British also sent partial reconstructions, from 15 to 30 per cent complete, of seven Vichy French digit codes (FAC, FAH, FAD, FAE, FAF, FAG, and FAI) which had not hitherto been studied. The discriminants for these systems, though solved in London, had not been recovered here. Translations were possible at once in the case of FAC and FAH, and code recovery could be carried on in the other systems.[6]

In January 1942, the Section established a swing shift of four persons, the members of which tried their hands at solution of the substitution encipherments of other French systems ultimately compromised in November 1942. In March 1942 a compromised copy of the Hanoi code (FBM) and some information concerning the additive encipherment used with it was received from the British. By early summer of 1942 the strength[7] of the Section was about 25 persons, who performed the

---

6. From November 1941 to April 1942 the staff was expanded by the addition of a number of persons: Mr. (now First Lieutenant) Richard Hallock; Sergeant (now Major) Carlisle C. Taylor; Mr. G. F. Swift; Mr. John R. Rafferty; Sergeant Willis Russell; Sergeant (now Captain) Gerrett L. Ewing; Sergeant Patrick F. Quinn; Lieutenant Stanley Clarke; Mr. (now Major) Edward Quereau; Dr. Albert Howard Carter; Mrs. Jeanne S. Fish; and Mrs. G. L. Lattin. Most of these persons know French, particularly Mrs. Fish and Mrs. Lattin, who are natives of France.

7. Before May 1942 the Section had again expanded by the addition of another group, comprised in the main of French specialists. These included: Drs. Caleb Bevans and Vista Clayton; Lieutenants John E. Carroll, Donald Miller, Reuben Y. Ellison, and Scott F. Runkle; Miss Helen J. Bradley; Mrs. Ray Pettengill; and, for a short time only, two cryptanalysts: Mr. Edward E. Christopher and Mr. Norman Dillinger.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

operations of cryptanalysis, code recovery, deciphering, decoding, and translating the French traffic. Though at this period much had already been accomplished, the larger achievements of the French Section were still to come. It was at this point that the move from the Munitions Building to Arlington Hall was imminent. Before the move took place, however, changes occurred which were to dissolve the unit as it had previously existed, and, as a result of the general reorganization that took place in the Signal Security Agency in the summer of 1942, Lieutenant Bearce was promoted to head a larger section (then called B-II-a).

B. The Period of Division (June 1942 to September 1943)

The reorganization, which also affected many other units, was based on the new principle of arrangement of function by type of cryptanalytic operation rather than by government, language, or homogeneity of traffic, a principle which had previously been followed. As a result the existing French Section was broken up into four smaller units, each of which assumed one of the functions which had previously been part of the assignment of the larger section. The function of decoding the traffic, however, was not performed in any of these units but in a new organization which decoded traffic in the Japanese and Spanish languages as well, formed somewhat later (September 1942) than the others. The new administration was as follows:

1. The French Cipher Unit, under Mr. William S. Smith, assigned to all French problems involving types of enciphered code other than those based on additive encipherment;

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

2. The French Additive Recovery Unit, under Lieutenant Stanley Clarke, assigned to the solution of the encipherment of codes enciphered by additive;

3. The French Code Recovery Unit, under Lieutenant John E. Carroll, assigned to problems of code recovery, both unenciphered and those from which encipherment had been removed;

4. The French Translation Unit, under Lieutenant Lee P. Howard, assigned to translation of decoded messages and plaintext traffic in French; and occasionally to special translation problems; and

5. The Decode Unit, under Mrs. Jean Reischauer, assigned to the task of decoding, in addition to certain systems in the Japanese and Spanish languages, all French messages in systems sufficiently solved to permit decoding with little or no recovery work.[8]

While the traffic studied by these five units was homogeneous in that it was all transmitted by the Vichy French Government, the units themselves were not united administratively. The Cipher Unit, for example, was part of what was then called B-III, a cipher section under Lieutenant Frank B. Rowlett; the Additive Recovery Unit was part of B-II-b, then under Captain Leonard Bickwit; the Code Recovery Unit was part of B-II-a, then under Captain Bearce; while the Translation Unit and the Decode Unit were both parts of B-I, a group of service units under Captain Verner C. Aurell.

The dissolution of the old French Section into these units was not, however, completed on a single date. The Cipher Unit and the Additive Recovery Unit were first separated from the others and

---

8. For a discussion of the work of this unit as a whole, see section G.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

moved to Arlington Hall Station in July 1942, whereas the others were not formed until the removal of the last of the Signal Security Service on 24 August 1942. Later, when a need for closer cooperation between the units arose, a central committee was formed to discuss technical problems with a view to the proper assignment of new traffic and the avoidance of duplication of effort. As of August 1943, this committee consisted of Lieutenant William S. Smith for the Cipher Unit, Dr. Caleb Bevans for the Code Recovery Unit, and Miss Helen J. Bradley for the Additive Recovery Unit, which by this time was performing preliminary research on new systems. The work of this committee helped in eventual amalgamation of all the French units in a single French Section on 21 September 1943; but before discussing that reorganization, the history of the various smaller units during the period of division will be considered.

C. The French Cipher Unit

B-III-d, as it was called in July 1942, was one of the first units to be separated from the original French Section and moved to Arlington Hall Station. It was under the direction of Mr. William

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

S. Smith until 15 December 1942.[9]

The work of the French Cipher Unit was the study of Vichy French enciphered code systems, except for those employing additive encipherment. The encipherment of the system now called FBB was solved very early and the traffic turned over to the Code Recovery Unit with about 50 tentative values established. Some progress was also made on the substitution encipherment of the system now called FAO. In November 1942 the capture of copies of this code and several others on which the French Cipher Unit was working compromised the system and reduced the problem to the level of production in a few enciphered code systems.

Lieutenant Smith left the French Cipher Unit in December 1942 and was succeeded by Captain Edwin R. Phillips as head of the Unit, the function of which was by that time limited to a considerable extent, because of captured material, to training. In February 1943 the Unit took over the cryptanalysis of two Swiss systems (SZM and SZN), and in May it began to study some Chinese enciphered codes. The French

---

9. Within a few weeks of its organization Messrs Hallock and Swift, who had come with Mr. Smith from Lieutenant Bearce's section, were transferred to the Japanese Military Attaché Section and were replaced by new personnel. The persons who spent the longest time in this unit in 1942, all of them new to the organization, included: Miss Marjory MacLeod (Mrs. Max-Muller); Miss (now Lieutenant) Mary Charlotte Lane; Mrs. Marion Nagel; Dr. (now Master Sergeant) Daniel M. Dribin; Dr. Leslie A. Rutledge; Dr. (now Captain) Edd W. Parks; and Miss Jeannette Early. Besides these, there were Lieutenants Edwin R. Phillips; Saul K. Raskin; Cyrus H. Gordon; Joseph R. Salem; Mr. Wayne S. Barker; Corporal Ruell E. Dawson; and Sergeant Frederick McComas.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Cipher Unit as such was absorbed into the general Cipher Section in July 1943 and continued to work on the French (and Swiss) problems only until September 1943, when the French Section was once more activated.

D. The Additive Recovery Unit

B-II-b-1, which was also one of the first units to be moved to Arlington Hall Station, was under the direction of Lieutenant (now Major) Stanley Clarke.[10] In early September Captain Clarke was selected for overseas duty and was succeeded by Captain William F. Edgerton; but on 1 February 1943 Captain Edgerton exchanged positions with Captain John E. Carroll, head of the Code Recovery Unit, and the latter remained in his new post until 29 January 1944, when he was transferred to the Military Cryptanalytic Branch (B-II). He was then succeeded by Miss Helen J. Bradley, who remained supervisor of the Additive Recovery Unit until the reorganization of August 1944, at which time she became head of the French Section as a whole. At first the Unit continued research, which had already begun in the Munitions Building, on French colonial additive systems. Shortly after the move to Arlington Hall, the British sent decodements of three

10. He had with him at the beginning Lieutenant Reuben Y. Ellison and Miss Helen J. Bradley. Shortly afterwards, there were added in succession: Mr. Norman Dillinger and Mrs. Helen Siegel (both temporary); Mr. Robert O. Moore; Lieutenant (now Captain) Stanley Simonds; Dr. Calvin Brown; Miss Kathryn Wood; Miss Harryett Willis; Mr. Edward Quereau (temporary); and Corporal Sidney Jaffe.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

messages in FBM, a system which they had previously compromised by capture of the basic code book, though the exact nature of the additive table used with it was unknown. By using the three decodements, however, it was possible to begin placing new FBM traffic in depth, and solution of the additive keys could now be achieved. Study of other colonial additive systems was carried on chiefly by Dr. Brown and Mr. Dillinger. Of these FBN, FBO, FBP, FBQ, and FBR, have remained unsolved for lack of traffic. At the time of the invasion of North Africa, however, the Canadian Examination Unit discovered that Vichy was sending identical news reports to Hanoi in FBM and to the other colonies in the system known as Colonial E-5. The basis of E-5 was a two-part code using a pentanomic group. Each colony used a different additive key book. By use of Hanoi cribs, about 600 relative code values and the corresponding amount of additive keys were recovered. The additive system FBI (Chinov) was compromised in its entirety, and the little traffic received here was deciphered and translated. [11]

Shortly after the invasion of North Africa all Vichy colonial traffic ceased except the Vichy-Hanoi system (FBM) which became very

---

11. Prior to 1 January 1945 the following persons were added to the Unit: Misses Marion Lathrop; Alice Van Hoesen; Rosamund Deutsch; Constance Hyslop; Charlotte Morris and Dr. Vista Clayton; Sergeant Harold Spain; Corporal Ralph Carl; and Mr. Paul K. Hartstall. Sergeant (now Lieutenant) Jaffe was sent to Officer Candidate School in December 1943 and was replaced by Lieutenant (now Captain) Seymour Bloom.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

light.[12] In April 1943, however, an examination of the Free French traffic, which hitherto had been stored, began. Systems proving to be unenciphered code were turned over to the Code Recovery Unit, the first of these on 2 May 1943. Codes enciphered by means other than additive were sent to the Cipher Unit. Additive systems, such as FFC, FMB, FMF, FMD, and FME, were retained. The first of these was isolated on 19 April 1943. All of the additives for FME (a daily strip system based on a five-digit code) were recovered, but since only 30 messages were received, code recovery was impossible. Both FMB and FMD, however, became readable; the code recovery for the former was done in the Code Recovery Unit under the direction of Dr. Clayton. FFC, a naval system, was turned over to the Navy in November 1943, but a fair amount of additive had been recovered under the supervision of Mr. Hartstall. FMF, based on a five-digit code, yielded several good columns of additives but was not read before the spring of 1944 because of lack of material. On 23 June 1943 a Free French transposition system (FMC) was turned over to a new unit recently formed for problems of this kind under the direction of Mrs. Siegel.[13]

In July 1943 work on unknown systems was taken over by the French

---

12. As a result, between January and April 1943 Mr. Dillinger, Dr. Brown, Sergeant Spain, Miss Hyslop, and Lieutenant Bloom were transferred to other units.

13. See page 129

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Cipher Unit under Lieutenant Smith.[14] The status of the systems being worked on in this Unit was reported on 3 July 1943 as follows:

Vichy systems (retained by B-II-b-1):

FMB (Vichy-Hanoi) - nearly 50 per cent solved; i.e., the enciphering keys used with a compromised code were solved in 90 out of a possible 186 cases.

"E-5" - 615 relative code groups recovered, and additive groups used in enciphering most of the messages sent in November and December 1942 recovered.

French Mission systems (retained by B-II-b-1):

FMB - 170-digit repeating additive based on a one-part code; code recovery and translation were done in this unit. The first translation made on 6 June 1943, shortly after traffic had ceased.

FMF - in research

FME - Daily additive key, two of which have been reconstructed.

FMD - a strip additive, in research.

French Mission systems (not retained by B-II-b-1 after isolation):

FMA - unenciphered code using old Vichy DX code, sent to Code Recovery Unit.

FMC - the so-called "Eel" system, sent to the Cipher Unit.
FMH - the so-called "Jelly-fish," sent to the Cipher Unit.

Free French Systems (retained in B-II-b-1):

FFC - the so-called "Lib-7," a four-digit additive, sent to the Navy on 9 November 1943.

---

14. By August the Unit had expanded by the addition of Misses Kathryn Clark (Mrs. Novak); Helen Smith; Janet Hunter; Betty Casassa; Lieutenant Talbot O. Ferguson (WAC); and Sergeant Mary B. Vanderhoof.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Free French systems (not retained by B-II-b-1 after isolation):

"Lib-8" - a Navy system sent to the Navy in May 1943; no real study made in this unit.

FFA - the so-called "Fido," unenciphered two-part code sent to Code Recovery Unit.

FFB - the so-called "Fraco," unenciphered two-part code sent to Code Recovery Unit.

FFE - the so-called "Lib-1," a substitution and transposition sent to the Cipher Unit.

FFD - the so-called "Lib-2," and

FFF - the so-called "Lib-3," both unknown systems sent to the Cipher Unit.

Five additional systems were isolated but not identified. These were also sent to the Cipher Unit.

At this period (July 1943) 20 systems were known to have been used by the French Mission and the Free French government, of which 20 had been isolated. Such was the situation at the time B-II-b-1 was united with the other French units on 23 September 1943.

E. The Code Recovery Unit

This Unit (B-II-a-1), with Lieutenant John E. Carroll as head, was moved to Arlington Hall Station on 24 August 1942.[15] The function of

15. The staff included at the beginning: Mr. Allen D. Garman; Dr. Caleb Bevans; Mrs. Constance Clark; Miss Mary B. Francis (Mrs. Vandenberg); Dr. Vista M. Clayton; Mrs. Jeanne S. Fish; Mrs. G. L. Lattin; and Corporal (now Captain) Paul Everett. Mr. Edward Quereau and Lt. Richard Ligon were also with this Unit for a short period, and in 1943 Lieutenant Victor A. Noel and Mr. E. Prentice Abbott were added.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the Code Recovery Unit was the recovery of the French unenciphered codes and of codes from which the encipherment had been removed.

On 1 February 1943 Captain Carroll exchanged positions with Captain Edgerton, who had been supervisor of B-II-b-1 since September 1942, but Captain Edgerton remained in his new post only for two weeks, when he was succeeded by Captain Thomas H. Glenn, who had been a member of the Code Recovery Unit since 15 December 1942. Captains Carroll and Glen remained heads of B-II-b-1 and B-II-a-1 respectively until 29 January 1944, when they were both transferred to the Military Cryptanalytic Branch (B-II). On 1 March 1943 the transfer to another station of Captain Ulrich S. Lyons, the head of the Swiss Unit, left that Unit without a supervisor, and the Swiss Unit was amalgamated with the French Code Recovery Unit under Captain Glenn. This arrangement continued until August 1944, when the Swiss Unit once more became independent.[16]

On 1 September 1942 Captain Carroll reported that in addition to completely compromised codes, his unit was then working on the following systems, all of which were two-part codes having 10,000 groups:

Code	Percentage recovered	Percentage doubtful	Messages per month	Identifications per month
CV (FAV)	60	few	500	120
DE (FAE)	55	20	330	300
DV (FAH)	50	10	200	250
DQ (FAD)	53	20	200	150
DS (FAF)	35	no information	40	150
DT (FAG)	52	no information	50	125-150
DO (FAC)	40	20	35	60-90
DX (FAI)	35	30	25-30	60-90

16. See chapter VII.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

On 19 November 1942 Captain Carroll was able to report that his unit had recovered and sent to the British 1625 code values since 29 September 1942 and had in the same period received from the British 1575 values. Ten days later the FES code had been received from the Cipher Unit, and Mr. Hallock and Mr. A. Ferdinand Engel, a member of the Italian Code Recovery Unit, were at work on its recovery. The DR code (FAE) had been recovered sufficiently to be sent to the Translation Unit on 17 October 1942. The last report signed by Captain Carroll as supervisor of B-II-a-1 (1 February 1943) gave the following as the status of the systems then being studied:

Code		Percentage recovered	Readability
DS	(FAF)	42 %	95.6 %
DT	(FAG)	59 %	98.4 %
DX	(FAI)	37 %	95.0 %
FEA	(two-part, 35000 groups)	8 %	
FES	(two-part)	17 %	74.0 %

In his first report as supervisor of B-II-a-1 (22 February 1943) Captain Glenn stated that identifications had been made during the preceding week in the following systems: FAF, FAG, FAI, FAL, FAU, and FBB. The report for 15 May 1943 listed new identifications in FAD, FAE, FAF, FAG, FAI, FAU, FBB, FBT, and FBU and noted the following systems as compromised at this time: FAL, FAM, FAN, FAO, FAT, FAV, and FBX.

In addition to the work on Swiss systems already mentioned, the Code Recovery Unit also carried on study of systems in the French

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

language sent by two other governments, those of Belgium and Haiti,[17] until 24 August 1944, when a special unit for these two governments was formed.

On 9 May 1943 the Code Recovery Unit was further enlarged by the personnel and functions of the French Translation Unit directed by Lieutenant (now Captain) Lee P. Howard.[18] In June 1943 the enlarged staff began work on FMC, from which the encipherment had been removed in the Transposed Cipher Unit directed by Mrs. Helen Siegel,[19] and progress was rapid. They also studied an unenciphered code (FFA). On 23 September 1943 this Unit was amalgamated with the other French units to form the present French Section.

F. The French Translation Unit

This Unit was first designated B-I-f and supervised by Lieutenant Lee P. Howard. It was formed on 24 August 1942 from personnel of the French Section directed by Lieutenant H. F. Bearce, and continued to exist as a unit until 9 May 1943, when it was amalgamated with the French Code Recovery Unit. Its function was the translation of all French plain text and of messages sent in such systems as had been

---

17. See section I, page 130.

18. This brought Lieutenants Howard, George M. Sayre, and Clelland D. Jones, Dr. Ruth Cherniss, Misses Noe Cox, Martha L. Little, and Anne O'Brien into the Code Recovery Unit.

19. See page 129.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

compromised or rendered readable by analysis to such a point that further cryptanalysis was unnecessary. At first the systems so processed were FBT and FBU. On 16 November 1942 it was reported that the French Translation Unit had prepared a French version of the instructions used with the U.S. M-138-A cipher device, but for the most part the translations made in this unit were from French to English. A week later the Unit received another French code (probably FAE). Priority was given at this time to messages to and from Panama, then to Buenos Aires traffic, Washington traffic, and Santiago traffic, in that order.[20] Collaboration with the Japanese sections in the translation of French messages sent in Japanese systems was reported on 10 January 1943. The Unit was working at this time on FAC, FAH, FAT, FAV, and FBT, and during January translated 185 plain-text messages and 224 code messages. By 1 February 1943, B-I-f also was working on FAD and FAO. On 20 March 1943 FAE and FAG were reported as 90 and 80 per cent complete respectively. A week later the Unit examined a large number of photographs taken in the French consulate at Los Angeles and prepared translations of those which were of interest. Reports ceased on 17 April 1943, but the amalgamation of B-I-f with B-II-a-1 did not take place until 9 May 1943.

---

20. At this period the French Translation Unit consisted of Lieutenants Howard and Sayre and two clerks. On 6 December 1942 Lieutenant Clelland D. Jones and Miss Charlotte Morris were added. Miss Morris was replaced on 26 December 1942 by Dr. Ruth Cherniss. Miss Anne O'Brien and Lt. J. C. Apollony were added on 20 February 1943, but the latter left for another section within a week.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

G. The French Decode Unit

Until the time of the breaking up of the French Section in August 1942, the task of decoding French messages had been one of the functions of the entire staff, but with the formation of the smaller units, this function was handed over to a newly organized unit known familiarly as the Decode Unit, at first under Mrs. Jean Reischauer, but soon afterwards under Lieutenant (now Major) James C. Taylor. In addition to the French traffic, chiefly in two systems (FBT and FBU), this Unit also processed messages in the Spanish and Japanese languages.[21] The French part of the Decode Unit was never formally activated but grew out of the Decode Unit (B-I-c) of which it remained a part until 21 September 1943. The following is a list of French systems on which this Unit worked prior to the amalgamation of all French units on 21 September 1943:

Before 12 October 1942	FBT,	a captured code;
	FBU,	a variant of FBT, encipherment recovered;
1 November 1942	FAE,	reconstructed at Arlington Hall
	FAH,	a code of which about 89 per cent was captured, the remainder recovered;
	FAV,	a captured code;
18 January 1943	FAC,	encode captured with part missing;
25 January 1943	FAO,	a captured code discontinued July 1943;
1 February 1943	FAD,	a captured code;

21. Until 12 October 1942 the French traffic was handled by Mrs. Helen Siegel and Dr. Ruth Cherniss, who were joined on that date by Miss Katharine L. Swift. Others were added later under the supervision of Miss Swift.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

15 February 1943	FAG,	Reconstructed at Arlington Hall;
8 March 1943	FAM,	a captured code, but some of the indicator tables were not captured and the Decode Unit solved these;
5 April 1943	FAN,	a captured code; indicator tables recovered as in the case of FAM;
19 April 1943	FBX,	a naval code turned over to the Navy after one week.

On 21 September 1943 the French Decode Unit was separated from those processing Japanese and Spanish traffic and was then amalgamated with the other French units to form the present French Section.

H. The French Transposed Cipher Unit

In May 1943 a new French Cipher Unit was formed with the object of studying transposition encipherments. Mrs. Helen Siegel, who had worked in other French units and on a Japanese transposition problem, was made the supervisor.[22] The solution of the FMC problem was aided by the receipt of two work sheets which had been carelessly handled by the code clerk in Washington and were made available for use through the alert cooperation of the Laboratory Branch. These work sheets showed the manner of encipherment and revealed the fact that, as had been suspected, FMC was a four-digit code enciphered by route and columnar transposition according to a mixed key sequence. As a result, the solution of the two keys made available by the intercepted work

22. Mrs. Siegel was assisted at first by various members of the larger Cipher Section under Lieutenant W. S. Smith and including Mrs. Genevieve G. Feinstein, Lieutenants Elwood Hill, J. C. O'Neill, Richard Hallock, and Dr. Calvin Brown.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

sheets produced code groups in about 50 messages sent in those two keys and led to the preparation of frequency distributions for this code which were useful in solving additional keys by anagramming. For illustration of captured FMC work sheets, see Tab 21.

Another French transposition encipherment (FFE) had begun to be studied shortly before the amalgamation of the French Transposed Cipher Unit with all the others engaged in studying French traffic on 23 September 1943.

I. September 1943 to the Present

During the first half of 1943 the French units described in the preceding paragraphs worked independently of each other, though with frequent liaison, which constantly increased after the formation of the central committee in July. At this period a reorganization of what was then called B Branch of the Signal Security Agency was under discussion, leading ultimately to the consolidation of all units except the Japanese Army Section into a section known as the General Cryptanalytic Section (B-III), later to become the General Cryptanalytic Branch in 1944. It was therefore proposed that the various French units, then five in number (since the Cipher Unit, originally B-III-d, had largely turned to problems other than French) be amalgamated in a French Section formed to process all French government traffic, and in addition the traffic of the Belgian and Haitian governments in French,

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

and of the Swiss government in French and German.[23] The consolidated French Section, designated as B-III-d, was placed under the direction of Major William F. Edgerton, who, after leaving French problems in the preceding February, had been Director of Training for the Signal Security Agency. Lieutenant Sidney Jaffe served as Major Edgerton's administrative assistant. The new section contained the following subdivisions:

1. The Additive Recovery Unit under Captain Carroll (after January 1944 under Miss Bradley);

2. The Code Recovery Unit under Captain Glenn (after January 1944 under Mr. Hartstall);

3. The Cipher Unit under Mrs. Siegel;

4. The Decode Unit under Miss Swift;

5. The Traffic Unit under Miss Ruth Adams.

The functions of the last group had previously been performed in the Traffic Section of the entire Branch, but this section was now broken up and the personnel assigned to the language units with which they had previously worked in liaison. One other change in function was made: the Cipher Unit under Mrs. Siegel now assumed both preliminary research and all encipherment problems except those based on additive. The other groups functioned as before.

Major Edgerton and Lieutenant Jaffe continued to direct the French Section until they were relieved, Major Edgerton in May 1944 to become

---

23. Though the language of part of the Swiss traffic is not French, cryptographically the German and English versions of the Swiss codes are identical with the French versions and, therefore, are handled together.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

acting chief of B-III during Lieutenant Colonel Rowlett's tour of duty at GCCS, and Lieutenant Jaffe in June for overseas duty. With the departure of Major Edgerton, the French Section was united with the other Romance language sections (Italian, Spanish, and Portuguese) under Captain Lowell G. Derbyshire (B-III-a), who for a short time continued to have jurisdiction also over the Near and Middle East Unit and the Chino-Thai Unit. The French Section continued as part of the Romance Language Section. Under Captain Derbyshire's supervision Miss Helen J. Bradley became supervisor of French problems, on 24 August 1944, Miss Kathryn Wood was appointed to head a new unit for Belgian and Haitian traffic, and the Swiss systems were once more given autonomy under Dr. Robert H. Weidman. The French systems were now once more reorganized as follows:

1. The Cryptanalytic Unit under Mrs. Siegel, charged with preliminary research, solution of cipher and encipherments including additive problems;

2. The Language Unit under Mr. Hartstall, charged with code recovery, decryptographing, and translation;

3. The Traffic Unit under Miss Adams.

Since January 1944 a group of expert cryptanalysts in B-III-a have been available for consultation by other units. Those who have worked principally with French problems are Dr. Caleb Bevans, Dr. Calvin Brown, and Miss Elizabeth S. Doane. The French Section suffered a sharp reduction in personnel on 29 January 1944, when seven officers

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

were transferred to the Military Cryptanalysis Branch (B-II).[24]

In September 1943 FMF was still in the process of solution; FMN, another pentanomic code, and FMJ, a tetranomic code, both used with additive encipherment, were well under way when instructions were received in November 1943 to drop work on all save FBM. This suspension was made necessary to enable transfer of personnel to more urgent problems elsewhere. In February 1944 work on FMN was resumed, and wherever sufficient traffic was received to provide the necessary depth, additive was solved and code recovery was possible. The same basic code was also used with another current system (a transposition known as FMX). FMJ became obsolete and was laid aside until January 1945, when it was successfully solved. FMF proved to have the same basic code as a transposition system FFY, and at present all additive in sufficient depth is recovered, after which code recovery, still in progress, is possible. Solution of FMS, a Free French additive system based on the compromised code known as CTX-1, had been begun in cooperation with the British and Canadians. The first overlaps were, however, solved in the Additive Recovery Unit. Later, changes of indicator were solved, and the production of intelligence from FMS messages was carried on by the Additive Recovery Unit until August 1944.

---

24. These were Captains Carroll and Glenn, Lieutenants Brown and Seele (who had been working chiefly on Swiss systems), and Lieutenants Bloom, Jones, and Noel.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

The first translation in FMD was prepared on 18 October 1943, only two days after Lieutenant Jaffe, who had at the beginning the benefit of only 246 values recovered by the Canadians, had begun to work. On 4 November 1943 FFA was compromised by the British, who sent also some information on an encipherment of the FFB system known as FFE. By 18 November 1943 the Code Recovery Unit was engaged mainly in decoding and translation except for work on FMA.

Traffic in FCB was reported for the first time on 27 February 1944. Meanwhile the Vichy additive system (FBM) underwent a number of major changes. The indicator was simply enciphered during a period beginning 1 August 1943, and the method of using the additive cards was changed. The new indicator was located and the new method of using the keys was revealed by a Code-Instruction message. On 1 January 1944 the encipherment of the indicator was again changed, and once more solved. Further complications introduced into the method of applying the encipherment were overcome. Moreover, methods of overlapping old traffic dating from 1941 to 1943 were devised. When traffic ceased in August 1944, about 75 per cent of all additive cards in depth had been recovered.

The solution of FFE, begun in May 1943 by the discovery of two messages which showed clearly that they were transposed code, was continued in the Transposed Code Section. This involved the development of new cryptanalytic techniques for solving two messages containing the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

same text but enciphered by transposition taken from matrices of different width. While FFE traffic was never heavy, this technique proved useful in other problems, notably FMP. The system called FCD, used by the Vichy government between late 1943 and August 1944 for communications on a few circuits, proved upon solution to be a system of digraphic substitution in which every fifth digit of the plain-code group was omitted and then enciphered in pairs.

FMV, solved 10 June 1944, ten days after the introduction of the system, proved to be an encipherment, using a daily additive of five digits, of the older basic code FAI. An additive system (FMF), which had been earlier attacked but abandoned because of pressure of work, was solved, as was also the indicator system. Another transposition system (FFY), used by the French Military Mission between 5 October 1943 and 26 January 1944, was solved on 23 March 1944, chiefly on the basis of a message in which many three-digit repetitions were to be seen. At first the system was thought to be unenciphered three-digit code, but attempts to fit the text in matrices of varying widths revealed five-digit code groups in the same basic code as was used with FMF, when a certain mixed key sequence was used. This sequence was found to be used with all messages after November and a second sequence to be used with all prior FFY messages. The code also proved to be the same as that used with FMP, so traffic in FFY, FMF, and FMP, could be used for code recovery.

The first French military cipher solved in the Signal Security

TOP SECRET CREAM

Doc ID: 6554247

Agency was FMP of which there were three varieties (FMP-A, FMP-B, and FMP-C). FMP-A was introduced late in 1943 but solution was not possible until the interception on 28 April 1944 of two messages bearing the same serial number and group count, and having almost the same frequency counts, but different indicators. It was assumed that the two messages were identical in plain text but had been enciphered by transposition from matrices of different widths. Using the same technique as had already been devised for FFE, a solution was reached and a report forwarded to the British and Canadians on 8 May 1944. The two sequences which were thus recovered proved to be based on the phrases VACCINATION ANTITYPHOIDIQUE and SECRETAIRE GENERAL which were later found to be code groups in the code itself. Consequently, the recovery of new key sequences may prove helpful in code recovery as well, and vice versa.

Progress was also made early in 1944 on code recovery of FFW, a one-part code with a five-digit group. The accuracy of the reconstruction was found to be very high when a captured copy of the code was received in January 1945. In May 1944 code recovery was begun on a basic code which, in various encipherments, was known as FMF, FFY, and FMP. The basic code was a large two-part military code using a five-digit group. Early progress on this project was slow because of the nature of the encoded messages containing many unfamiliar military abbreviations, but the patience, experience, and skill of the analysts

Doc ID: 6554247

TOP SECRET CREAM

finally brought the work to a satisfactory state of advancement. Though this is a large code, solution has been accomplished without the aid of an isolog or any assistance from the British and Canadian cryptanalysts.

Reconstruction of another code used with additive encipherment (FMN) and transposition encipherment (FMX) had been begun in the Additive Recovery Section early in 1944 but was laid aside for a time.

The task of decoding all French traffic was given to the decryptographing group of the French Section in January 1944. The task was formidable: the Vichy systems being read at that time numbered 16, but the group found time to do a certain amount of code recovery in two systems (FAC and FAH) which had been captured in incomplete form. At later periods four other Vichy systems were added. The translation of the huge amount of traffic was carried on by a group of about six persons. These Vichy codes provide information concerning such topics as bombings in the Far East, the state of mind of the Japanese people, relations between French Indo-China and Japan, intimations of impending political crises, reports on military and naval operations, and the like.

In the same period five Free French systems were read and translated regularly and code recovery on FAI was continued. FAI and FMV, its enciphered form, produced an enormous volume of traffic in 1944: in FAI 16,446 messages and in FMV 2,500. Complete decodements were

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

thus made impossible, but every message was treated to an operation known in the Section as "spot decoding"; i. e., enough was decoded to determine the subject matter. Complete decoding was then performed only in the case of those messages with intelligence value. Traffic in the Free French system FMS provided information on the situation in Syria and Lebanon and gave reports of the Russo-Polish problems, as well as on vital developments in Turkey and the Balkans. The other Free French systems being read at present are FMO and FFA.

Mention has already been made at many points of assistance derived from the British Government Code and Cypher School (GCCS) in London. The French Section also profited frequently by assistance from the Canadian Examination Unit (EU) in Ottawa. An exchange of technical information, progress reports, and traffic was carried on regularly at the time this history was written with both EU and GCCS. As a result progress was greatly accelerated and new sources of intelligence made available.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER VII. THE SWISS SYSTEMS[1]

In December 1942 a unit was formed in the Romance Language Code Recovery Section (then called B-II-a) to solve the cryptographic systems used by the Swiss government. Priliminary cryptanalytic research was carried on by Captain (now Major) Ulrich S. Lyons, assisted by Lieutenant Theobald E. Frizelle, but both of these officers left the Swiss Unit when the problems became predominantly linguistic.[2]

About 1 March 1943 Captain Lyons was transferred, and the Swiss systems, together with the personnel studying them, were united with the French Code Recovery Unit (B-II-a-1), then under the direction of Captain Thomas H. Glenn, an arrangement which continued until 28 August 1944. Thus, the larger resources of

---

1. The statements made in this section are based upon interviews with Captain W. Edward Brown, Miss Madeline Cournoyer, Dr. Robert H. Weidman, Mrs. Constance Clark, and Miss Alice Joys, and upon the following documents: a. Progress reports of the French Code Recovery Unit (1 March 1943 to 24 August 1944); b. miscellaneous reports of the Swiss Section.

2. Lieutenant (now Captain) W. Edward Brown was added almost immediately. His knowledge of both French and German proved of advantage to the Section, since the codes of the Swiss government are based on both these languages as well as English. Two other specialists in French joined the unit in January 1943. Lieutenant Richard Litton remained only for two months, but Miss Madeline Cournoyer remained until the summer of 1945.

Doc ID: 6554247

TOP SECRET CREAM

the French Unit were made available to the Swiss Section.[3]

After eighteen months as an integral part of the French Code Recovery Unit, Swiss systems were separated from the French Section and the Swiss Unit was again activated on 28 August 1944, headed by Dr. Robert H. Weidman, who had previously done considerable work on German and French translations and, while a member of the Cipher Section, had worked on some of the Swiss ciphers. By this time the problem had largely become one of production, and the strength of the Unit varied from 18 to 20 persons.

Captain Lyons and Lieutenant Frizelle began by sorting the accumulated traffic and, before the arrival of Lieutenant Brown, had edited a sufficient body of this traffic for IBM processing. The

---

3. Messrs. Allan D. Garman and E. Prentice Abbott and Lieutenant Victor A. Noel were responsible for certain Swiss systems; Major and Mrs. Gordon T. Fish and Dr. Caleb Bevans assisted in the work as time permitted. To help with the German codes, Lieutenant Keith C. Seele was now transferred from the German Section and remained until January 1944. At about the same time came Miss Mary Bidwell, who remained with Swiss Problems until October 1944, and Miss Caroline Kennedy, who arrived in July and is still at work; they have spent most of their time on Swiss code recovery in French. Lieutenant Frizelle was transferred on 31 April 1943. From September 1943 to October 1944 Dr. Ruth Staley worked on code recovery problems in German. Early in 1944 Mrs. Constance Clark and Mrs. Mary B. F. Vandenberg, members of the French Code Recovery Unit for more than two years, spent some time on Swiss problems; and, later, Miss Margaret Fanning and Mrs. Antoinette Nelson were added. Dr. Helen Emerson, Dr. Walter Wall, and Miss Alvina Helmke joined the Unit to work primarily in German. Members of the Research Cipher Sections who worked on Swiss systems include Mr. Robert O. Ferner, Mrs. Genevieve G. Feinstein, Dr. A. H. Carter, Captain Herbert Maass, and Miss Betty Sherer.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

first group of messages sent to the Machine Room consisted of traffic in what was afterwards designated as the three systems SZA, SZB, and SZC. These codes were used exclusively by the Swiss for communications discussing the interests of the various belligerents whom the Swiss were representing. The confusion of the three systems in one index was natural: all three systems used the same code groups (each consisting of two digraphs of the vowel-consonant form), and the groups representing numbers had the same plain equivalents in SZA and SZB. The discriminants had been solved by the British, but the information did not reach the Signal Security Agency until January 1943. The method was quite simple: messages encoded in SZA were preceded by the date followed by the message number; messages in SZB used the reverse order for the number and date; while those in SZC omitted the date entirely.

The early index and message print had to be scrapped, since they contained heterogeneous material, but a new index and message print were completed on 22 February 1943. Several characteristics of Swiss cryptography provided fairly easy entry, and the first translation was prepared exactly two months later. The codes were uneciphered and one-part. The traffic from any station bore message numbers taken from the same series, and this included not only code messages but those in plain text as well. Thus, very early in the examination of the traffic the plain text was given careful attention.

[redacted]

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

The British sent some additional information concerning these codes. They knew that most page symbols had a variant taken from the latter part of the alphabet, and that there was some sort of preliminary section placed before the vocabulary, but they seem not to have made much progress in the solution of these systems, and they sent no identifications. It was Lieutenant Brown who discovered the pattern for the digraph representing the line symbol for both the first variant code group and the second. In the case of the latter, the digraph was printed on the page in normal alphabetical order but with random omissions, each page following its own pattern, though there was some repetition of patterns.

The discovery was made on 28 March 1943 that each line of the code contained not one plain equivalent but two. The second was usually a spelling group, frequently, though not always, one composed of the first few letters of the plain equivalent which stood first on this

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

line. At the bottom of each page the compilers had provided a begin-spell group for use with such spelling groups, and also a few groups for punctuation, as well as some blanks for addenda.

Another characteristic of Swiss cryptography which proved very helpful in analysis was the precision with which the code clerks indicated the exact inflectional ending desired. The cryptanalysts soon learned to take advantage of the aid.

At the outset of the work the English form of the code (SZC) did not appear in very great volume, but when traffic discussing the business of the English-speaking governments in the Far East began to be received, there was sufficient volume to justify an attempt at solution. Captain Glenn and Dr. Bevans worked for five days on this code early in April 1943. After that, there was a period when the system was neglected; in seven weeks several persons gave it some attention, estimated at about the time of one person for one month. Then on 18 June 1943 Mr. Abbott took over this work and produced the first decodement a week later.

In February 1943 the first solution of an SZD message was reached by the Cipher Section (B-III-c), which continues to process this traffic but sends it to the Swiss Unit for translation and reference.

The initial inquiry concerning Swiss systems elicited from the British the facts about SZA-SZB-SZC already noted, and also partial reconstructions of the two codes. The first was a trigraphic one-part

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

enciphered code with French and German versions (SZG and SZH); the second, a tetranomic one-part enciphered code, also with French and German versions. These reconstructions were completed in the Signal Security Agency.

Another body of traffic early studied was found to be a trigraphic enciphered code with French and German versions (SZM and SZN). The solution was begun in the Swiss Section but in its initial stages was turned over to the Cipher Section. The encipherment was successfully removed with the collaboration on linguistic problems of the Swiss Section. Finally, the unenciphered material was returned to the Swiss Section in relative form for code recovery.[4] The first translations in this one-part code of 2000 groups was produced in a remarkably short time. Thirteen days, after code recovery began, sufficed for the French version, and only eight for the German. A compromised copy of each version was made available by the British on 25 September 1943. At the present time the process of removing the substitution encipherment of current traffic is performed by an electrical device consisting of two typewriters connected by a complex of wiring.

SZQ designates another pair of companion codes used by the Swiss for their most secret communications. Traffic in these codes produces

4. Lieutenants Brown and Seele worked on the German version (SZN), and Lieutenant Noel, Mrs. Clarke, and Mr. Garman did the work on the French (SZM).

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

a high percentage of useful intelligence.[5] Work was begun in September 1943 but was soon laid aside since personnel was badly needed elsewhere. In the following month a partial reconstruction of the two codes (about three identifications on each page) was received from the British. The British also sent three keys for the encipherment. The study of the systems was thereupon resumed, and by March 1944 about a hundred keys had been recovered here.[6] Code recovery is now advanced to the point where every message can be translated.

SZR is the latest Swiss code to be studied, the only one in which much code recovery is still needed. While in many ways similar in type to SZA-SZB-SZC, it is two-part, and is the only code of this type used thus far by the Swiss. If there is a German version, it has not yet appeared in the traffic. The traffic is used exclusively for discussion of the interests of the belligerents represented by Switzerland. In December 1944 about 2,000 identifications had been made; the maximum number of permutations of the code group was 14,400, the largest of the known Swiss codes.[7]

---

5. The preliminary research was performed by Miss Alice Joys and Miss Louise Koegel, assisted by Lieutenant Sidney Jaffe, a member of the French Code Recovery Unit.

6. The work on code recovery was performed in the case of the French version by Dr. Marion Griggs and Lieutenant Noel; in the case of the German version by Dr. Staley.

7. The work on code recovery was performed by Miss Madeleine Cournoyer, Miss Caroline Kennedy, and for a time by Miss Mary Bidwell.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

There remain to be mentioned two systems which were solved by the Cipher Section in 1943. SZP, the first, was a polyalphabetic substitution cipher using 10 alphabets. It appeared in traffic between Bern and all parts of the British Empire except London. Solution was reached, except for some minor details, in June 1943. SZS, the second, was another cipher system using 20 alphabets, which appeared only in the Bern-Caracas circuit. It was solved by the Cipher Section in October 1943.

Except for traffic in SZR, on which work is constantly in progress, all Swiss systems thus far observed have been solved except for a few messages which start in SZA-SZB-SZC and then switch to an unreadable system. This traffic is too light for solution and may be an encipherment of the basic code by displacement or by some form of substitution.

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

The Swiss also used for [redacted] This traffic, which was given the short title SZD, was regularly studied by the Machine Cipher units but was sent upon solution to the Swiss Section for translation.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER VIII. THE SPANISH AND SPANISH-AMERICAN SYSTEMS[1]

As in the case of the French systems, the study of the Spanish and Spanish-American systems began in the unit known simply as "Mr. Bearce's section,"[2] which was formed about April 1941 and given the assignment of analyzing all systems using the Romance languages except Italian.[3] Some research on Spanish-American problems had been performed at an earlier period (1936-1938) by Dr. Abraham Sinkov on duty at Quarry Heights, Panama Canal Zone.[4] His report for the quarter ending 31 December 1937 is available (IR 5001). According to this report the Mexican government had previously used a polyalphabetic cipher with 15 random, unrelated alphabets (of which one set of alphabets had been solved) and a five-letter code. Work on Colombian traffic had revealed that the Colombians were using polyalphabetic ciphers based on five alphabets, each diplomatic representative being assigned a different set of five. The sets used in the Rio de Janeiro, Rome, and Washington circuits had been recovered. All that had been learned of the Venezuelan systems was that they were similar to the Colombian,

---

1. The statements made in this section are based on interviews with Colonel Solomon Kullback, Major Javier H. Cerecedo, Captain Saul K. Raskin, Dr. James V. Rice, Mrs. Delia A. Sinkov, Mr. R. Woodrow Harrison, Mr. Donald L. Fabian and Misses Gertrude E. Ullman and Ann Davis.

2. See chapter VI, section A and footnote 2, page 112.

3. For beginnings of which, see chapter V, section A, page 98.

4. MI-8 had, between the years 1917 and 1929, done considerable work on systems in the Spanish language but the continuity had been broken in 1929. See Historical Background of the Signal Security Agency, volumes Two and Three.

Doc ID: 6554247

TOP SECRET CREAM

but traffic intercepted was too small in volume for solution. As for Costa Rica, the report states that there had been great difficulty in intercepting messages from Costa Rica and suggested that steps be taken to arrange for interception of Costa Rican traffic at some other station.

No further progress had been made on Spanish-American traffic, and Mr. Bearce's section seems to have been concentrating its efforts on Mexican traffic. Some progress had been made subsequent to April 1941 in the Signal Intelligence Service at the Munitions Building on certain Mexican cipher systems (MXC, MXD, MXE, and MXH), on a Colombian cipher (COA), as well as upon Brazilian code traffic, but continuity with the past had been broken, and knowledge of this early work was lost.

Shortly after Pearl Harbor--it is not certain whether in December 1941 or January 1942--a part of Mr. Bearce's staff was withdrawn and activated as the so-called South American Section under Lieutenant (now Major) Leroy M. Glodell. In spite of its designation, the Section studied traffic of both the Iberian governments and of some Central American governments as well.[5] The following types of traffic

5. With Lieutenant Glodell was Miss Rosalie Harding (Mrs. Bash), and, by January 1942, Lieutenant (now Major) Raymond R. McCurdy and Miss Delia A. Taylor (Mrs. Sinkov). Messrs. Wayne S. Barker, Hugh Davidson, Robert Evans, and Mortimer Proctor were in the Section by 1 March 1942, when Captain Javier H. Cerecedo joined the South American Section. They began work on SPA, a Spanish government system based on a compromised code enciphered with additive.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

were being studied during the first few months:

Spanish government traffic
Mexican code traffic
Mexican cipher traffic
Argentine code traffic
Chilean code traffic
Colombian cipher traffic
Dominican cipher traffic
Venezuelan cipher traffic
Brazilian code traffic
Portuguese code traffic

The last two could have been studied in the South American Section for only a very short time, for on 8 January 1942 all work on both Brazilian and Portuguese systems was suspended, not to be resumed again until just before the dissolution of the South American Section in August 1942.[6]

In the period from March to June 1942 the South American Section, in common with the entire Signal Intelligence Service, underwent considerable expansion.[7] The enlarged staff performed the operation of additive recovery, code recovery, cipher solution, and translation of

---

6. See section D.

7. The following persons were added in this period: Lieutenants John H. Utley, George M. Sayre, and Jose Quintana; Sergeant Jose Armendariz; Drs. Revilo P. Oliver, James V. Rice, and Lowell B. Ellis; Messrs. Donald L. Fabian and Julian DeGray; Mrs. Marjorie Thielmann; and Misses Charlotte Morris, Ann O'Brien, Gertrude Ullman, Nancy McWhorter, and Martha Montooth. The Section now had the advantage of including several persons who had done graduate work in Spanish (Utley, Oliver, Rice, Ellis, Fabian, Ullman); another group for whom Spanish was a native language (Cerecado, Quintana, Armendariz); certain others who, belonging to neither of the first two categories, nevertheless spoke Spanish extremely well (Glodell, DeGray), besides a somewhat larger group containing cryptanalysts and others who knew Spanish well enough for the tasks before them.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the resultant plain text.[8]

The progress of cipher analysis in the Section may be measured by the solution of the Mexican two-alphabet cipher and the Mexican "Guion" cipher (MXG) before April 1942, and of the Chilean five-alphabet cipher (CLE) in June. During the summer Colombian (COA), Dominican (DOA), Cuban (CUB and CUD), Venezuelan (VZB), and Mexican (MXC, MXE) ciphers were solved.

Another feature of the work of the South American Section was collaboration with the Office of Censorship in the cryptanalytic examination of certain questioned documents intercepted in the mail. This involved the reading of a considerable amount of material in an effort to discover open code. Most of the results were negative, but one letter, written in Catalan, was found to contain a polyalphabetic cipher concealing reports on espionage in Spanish ports.

In June 1942 the South American Section was gradually dissolved, as was the French Section from which it was an offshoot. Certain units were among those first moved to Arlington Hall in that month. Among these was a new unit formed by Lieutenant McCurdy and Mr. Evans which

---

8. Lieutenant Utley and Mr. DeGray worked principally on Mexican codes (MXA, MXB); Mrs. Thielmann and Sergeant Armendariz chiefly on the Chilean code (CLA). Captain Cerecedo and Mr. Davidson were responsible for ARB and Mr. Fabian for ARA. Messrs. Proctor, Evans, and Barker attacked the cipher systems, and Lieutenant McCurdy and Miss Taylor (who, however, did not remain long in the Section) worked on the removal of the additive used with the Spanish code (SPA).

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

continued to solve the additive encipherment of SPA. Shortly afterward, the study of Brazilian systems was resumed by Lieutenant Glodell and Dr. Revilo P. Oliver (who had recently joined the South American Section). Lieutenant Glodell and Dr. Oliver were detached, after the South American Section was moved to Arlington Hall in August 1942, to become the nucleus for the new Portuguese-Brazilian unit.[9] On 24 August 1942 the Spanish-American Section was broken up into four new units:

1. The Spanish Code Recovery Unit;
2. The Cipher Solution Unit;
3. The Translation Unit; and
4. The Spanish Additive Unit.

A. The Code Recovery Unit (B-II-a-5)

The new Unit was placed under the direction of Captain Javier H. Cerecedo, and formed an integral part of the Romance Language Code Recovery Unit (B-II-a), which was for a short time under Captain H. F. Bearce and then under Captain Gordon T. Fish, and which at this time contained the Italian, French, and Portuguese-Brazilian Code Recovery Units. Captain Cerecedo remained in charge until April 1943, when he was placed in charge of all additive-recovery units. His successor was Lieutenant Utley, who was transferred to another station in September 1943 and was succeeded by Lieutenant Carl McGee. Lieutenant McGee directed the work until February 1944, when the present head

9. See chapter IX.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

of the unit, Mr. Donald L. Fabian, took charge.[10]

The task of the Spanish Code Recovey Unit was, in general, the study of all codes used by Spanish-American governments, except the Mexican and Chilean codes, which were already assigned to the Translation Unit. Because some of the Spanish-American governments were at this time using only cipher systems, other government systems were not being intercepted at all, and some code traffic was not processed for lack of personnel, the Spanish Code Recovery Unit studied in the first few months of its existence the code systems of only five governments (Argentina, Bolivia, Chile, Ecuador, and Venezuela).

Since the codes used by Spanish-American governments were generally one-part with an occasional simple encipherment, the problem was largely one of code recovery. Such additives as were used presented no special problems, and there was no need for a special additive-recovery unit. The Spanish Additive Unit, under Lieutenant McCurdy, was engaged solely in the solution of Spanish government traffic, and there was no correspondence between this problem and those in Captain Cerecedo's unit.

Code systems have now appeared from all Spanish-American governments except Costa Rica,[11] which appears not to use cryptographic

---

10. Besides Captain Cerecedo, the following persons constituted this group: Lieutenant Utley, Dr. Rice, Messrs. Davidson and Fabian, and Mrs. Thielman; and Lieutenant Maurice Silverstein soon joined the staff.

11. Strangely enough, it did during World War I.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

communications. Traffic from Paraguay is received but not studied, and Honduras traffic has not yet been identified as code or cipher. Code traffic from all other Spanish-American governments has been studied and the systems for the most part solved, so that at the present time the work of the Spanish Code Recovery Unit is largely in the production stage.

Three Spanish-American codes (MXA, MXB, and CLA), though belonging to the general field included in the assignment of the Spanish Code Recovery Unit, were sufficiently recovered to be turned over to the Translation Unit. The separation of these codes from the others proved unsatisfactory; eventually most of the personnel of the Translation Unit and all of its functions were absorbed by the Spanish Code Recovery Unit.

The Spanish Code Recovery Unit was not responsible for Spanish-American cipher systems, as they were assigned to the Miscellaneous Cipher Unit of the Cipher Section. In the summer of 1943, however, B Branch of the Signal Security Agency was reorganized in order to group the subsections according to language rather than cryptographic method. As a result, the Spanish-American cipher systems, by this time more or less solved, were turned over to the Spanish Code Recovery Unit. The absorption of both the Translation Unit and the Cipher Unit expanded the function of the Spanish Code Recovery Unit to include the study of all cryptographic systems employed by Spanish-

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

American governments.[12]

At present most of the systems have entered the production stage; i.e. messages in cipher systems can be deciphered completely, or new keys solved upon receipt, and messages in code systems are for the most part readable. There remain, of course, a few cryptanalytic problems.

B. The Cipher Solution Unit

In August 1942, at the time of the move to Arlington Hall Station, a new Cipher Unit was formed from the old South American Section by the transfer of Mr. Proctor as head, and Misses Ullman and McWhorter as his assistants. The new unit formed part of the Cipher Section (then called B-III), under Lieutenant Frank B. Rowlett, and was known as the Miscellaneous Cipher Unit to distinguish it from units working on other specialized cipher problems. Its mission was the solution of all cipher systems not specifically belonging to the other cipher units, but in actual practice all of the systems studied turned out to be Spanish-American in origin. Heretofore, all of these ciphers had been substitution systems, but now transpositions were studied for the first time.

---

12. The personnel transferred from the Translation Unit included Dr. Lowell B. Ellis, Mr. Julian DeGray, and Miss Betty McCann. Lieutenant Carl McGee joined the Unit in December 1942 upon receiving his commission. In 1943 Miss Noma Riley, Mr. Humes H. W. Hart, Miss Louise Walker, and Miss Margaret Woods were added, as was also Lieutenant J. C. Apollony. For a time Lieutenant Apollony was detached to be in charge of the Plain Text Unit, which existed between August 1943 and February 1944. Of these persons all have since been transferred elsewhere.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Miss McWhorter was responsible for the solution of a number of transposition problems especially through the application to them of the electromechanagrammar. A loss was sustained when Mr. Proctor resigned at the end of October to enlist in the Army. Mr. Proctor had invented the process of rapid key recovery for Mexican MXC, recovered (on the basis of Lieutenant Barker's earlier work) substitution tables for MXE, and advanced the solution of Chilean ciphers. He was succeeded by Lieutenant Raskin, who had been working in the French Section.[13] Finally, after most of the cipher systems used by Spanish-American governments had been solved, the Cipher Solution Unit was joined, so far as its functions were concerned, with the Spanish Code Recovery Unit to form the present South American Section of B-III-a. The personnel, however, was transferred elsewhere.

C. The Translation Unit

At the time of the move to Arlington Hall Station (24 August 1942), a new unit, known as the Translation Unit,[14] was organized with Lieutenand Gordon W. Ross as its head.

---

13. Lieutenant Raskin was in charge until March 1943 when he was succeeded by Lieutenant Louis Smadbeck, who, with Lieutenant Robert C. Masenga, had joined the Cipher Solution Unit somewhat earlier. Lieutenant J. C. O'Neill was a member of this Unit for a time in 1942, as were Mesdames Phyllis Rhodes and K. Burn, Miss Julia Barker, and Mr. Roscoe Adkins.

14. Not to be confused with the French Translation Unit (B-I-f) coexistent with it.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

The Translation Unit, charged with the translation of all plain text except the French, took over the task of rendering into English messages sent in certain Spanish-American codes (MXA, MXB, and CLA), which, having been sufficiently recovered, had reached the translation stage. It translated all traffic in solved Spanish-American cipher systems, but it did not translate the messages from the Spanish Code Recovery Unit under Captain Cerecedo, or from the Spanish Additive Unit under Lieutenant McCurdy; for these two units did their own translating.

Decoding and deciphering were not performed by the Translation Unit but by a part of the Decode Unit (B-I-c).[15] It was found, however, that the codes which the Translation Unit had already received, frequently involved considerable code recovery before a message could be translated. Furthermore, any cryptanalytic skill which the members of the Unit might develop (and at least two members of the staff did possess considerable skill in this direction) would be lost to the cryptanalytic units. It had always been the experience of the Signal Security Agency, moreover, that messages in one system, or even in plain text, might discuss subjects also treated in systems less completely solved and such isologs could be used to best advantage only when all the traffic of a government was processed by the same groups of persons. Dissatisfaction with the divided arrangement brought about a gradual

15. See chapter VI, section G.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

transfer of personnel to other units, the personnel working on Spanish traffic rejoining the Spanish Code Recovery Unit.[16] Lieutenant Ross was transferred elsewhere in June 1943, and after that the Translation Unit was abandoned and the function of translation was assigned to the several cryptanalytic units.

D. The Spanish Additive Unit

At various times separate units were formed for the purpose of studying the Iberian systems. Currently (August 1945) the South American and the two Iberian groups operate as three separate sections, but the original studies were made by members of Lieutenant Glodell's unit.

The first project undertaken by the Spanish Additive Unit in January 1942 was recovery of additive used to encipher the code held by the Spanish

[redacted]

16. Among these were Mr. DeGray, Dr. Ellis, and Miss McCann. Others who belonged to this unit included Lieutenant Carlos Bernstein (later transferred overseas) Mr. R. Woodrow Harrison (who later rejoined the Portuguese-Brazilian Section) Mr. Charles W. Wonder, and Sergeant Fred Allred.

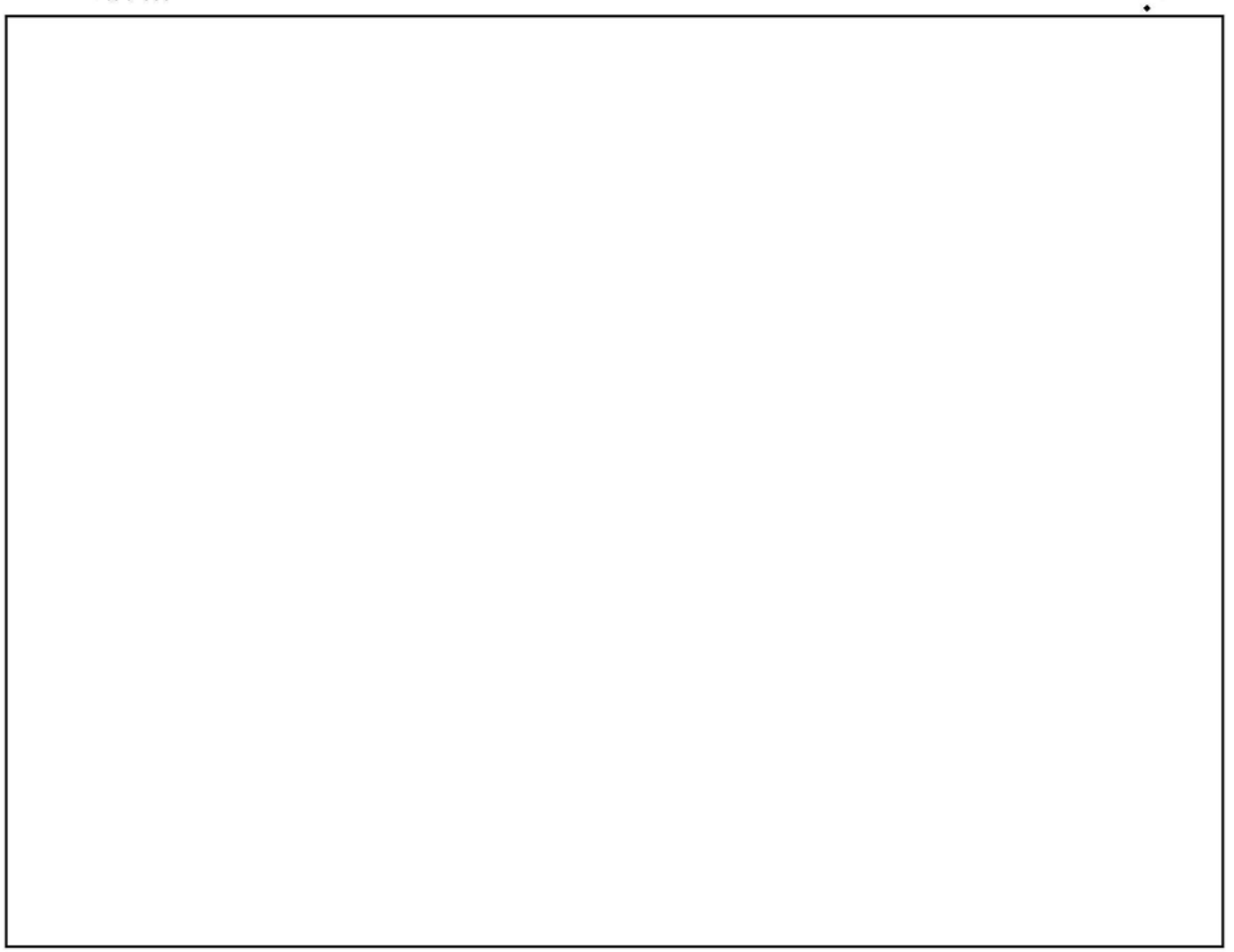
TOP SECRET CREAM

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

Doc ID: 6554247

TOP SECRET CREAM

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)



Later the Spanish Additive Unit received from GCCS a photographed copy of the code book for SPE, another enciphered code system used by certain Spanish consular offices. In May 1945 the group received from the same source a copy of part of the additive tables used for the Istanbul circuit. Work on SPB, a diplomatic system using a re-paginated version of a one-part code published in 1915, yielded

---

17. Ways and means were found to obtain a copy of a number of such tapes while they were current.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

consistently satisfactory results. A Spanish colonial system (SPC) in use between Madrid and Santa Isabel has been in research, but all results to date have been negative. SPD, a military attaché system, presumed to be machine cipher, has also been studied without satisfactory results.[18]

In addition to the three Spanish language units already described, there was a group, functioning as part of what was then known as the Decode Unit (B-I-c), which decoded the traffic in Spanish language code systems later to be translated in the unit under Lieutenant Ross.[19] Systems processed by this group included those of the governments of Argentina (ARB), Chile (CLA), Mexico (MXA, MXB), Cuba (CUA), Spain (SPB), and Venezuela (VZA). Toward the summer of 1943 the group also assisted in decoding traffic in some of the Portuguese systems. The Spanish Group of B-I-c was abandoned in July 1943 and its functions, as well as some of its personnel, were transferred to the Spanish Code Recovery Unit, which thus became responsible for all Spanish-American systems.

---

18. Since April 1944 Miss Ann Davis has been in charge of the Spanish Section, with Miss Erma Taylor, Miss Clara Sigafoose, Miss Mary Leon, and Miss Ruth Peters responsible for cryptanalytic and linguistic phases of the work. Other personnel aid in logging and decoding.

19. The supervisor of the Spanish group of B-I-c was Miss Betty Moulton (Mrs. Leonard) who had with her among others, Miss Alda Ross, Mrs. Clara Weeks, Miss Fairfax Haar, and Miss Jean Brown.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER IX. THE PORTUGUESE AND BRAZILIAN SYSTEMS[1]

The first examination of Portuguese and Brazilian traffic in the Signal Intelligence Service was made in the spring of 1941, when Mr. Bearce's section was formed to work on the Romance language traffic.[2]

Only a small amount of information was available at the time, that produced by the cryptanalytic unit operating in Panama. The report of this work for the quarter ending 31 December 1937 (IR 5001) states that the permutation table of a Brazilian five-letter system (BZC) had been reconstructed, and it was known that the Brazilians were also using another five-letter system (BZD?) and a digit system (BZI?) as well. In December 1937 it was not known that the code groups of BZC were taken bodily from the first edition of the Mascotte Commercial Code (Hamburg, 1922). The Portuguese systems were examined in 1942 by Mr. Wayne S. Barker, who joined the Signal Intelligence Service in that year.

The results of some early work on BZD was received from the British after May 1941, when two members of Mr. Bearce's section, Mr. Allen D. Garman and Mr. G. W. Ross, assisted at times by Lieutenant Commander Rhodes of the United States Coast Guard, did some work on Brazilian traffic. A message print and index of the traffic in both

---

1. The statements made in this chapter are based on interviews with Dr. Revilo P. Oliver and upon one document (undated), History of Portuguese-Brazilian Section, prepared by Dr. Oliver in the spring of 1943 with the help of Captain Leroy M. Glodell. See also Portuguese Codes and Ciphers 1941-1944 (IR 4051).

2. See chapter V, section A, page 112.

Doc ID: 6554247

TOP SECRET CREAM

BZC and BZD were prepared, with the result that the alphabetical range of many BZC pages was determined by the identification of the more common groups. It was also discovered that the book contained a preliminary section of punctuation and special signs, as well as an appendix of proper names. Additional identifications were made in BZD, but since the code is repaginated (i.e. partly one-part, partly two-part), progress was much slower. Translations of BZC messages were also prepared in some cases, but at this time only about half the groups in any BZC message had been identified.

Before January 1942 a small machine index of traffic in other Brazilian systems used in the Washington circuit and another index of Brazilian five-digit traffic used in various European circuits were prepared. This was the status of work on Portuguese and Brazilian systems when Lieutenant Glodell was directed to suspend temporarily all operations on those systems. Interception, however, continued, and, in the first half of May 1942 (the only period for which records are still available) 97 Brazilian and 141 Portuguese messages were received and filed for future use. In June 1942 Dr. Revilo P. Oliver, later to be closely identified with every phase of the solution of systems in the Portuguese language, joined Lieutenant Glodell's unit, and permission was obtained for him to resume the study of Brazilian (but not the Portuguese) systems. Since BZC was at that time readable, and the major part of most messages could be translated, attention was directed primarily to the traffic in this system and to a lesser degree to

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

BZD, in which, about 1 August 1942, the first translation was prepared.

Soon after the arrival of Dr. Oliver a new unit was formed to work on all Portuguese and Brazilian systems and placed under the direction of Lieutenant Glodell, with Dr. Oliver and two clerks as the staff. The assignment at first did not include cipher systems, which at this time were being studied in a special unit. Since only one cipher system had been intercepted, however, the unit under Lieutenant Glodell was actually working on practically all Portuguese language traffic. A little later the two clerks were replaced by two enlisted men, Sergeant Robert Armstrong and Corporal Cecil Porter. The solutions of the two cipher systems POP and POQ were completed by Corporal Porter on the dates when the first messages were received.

Another period of expansion in the organization of the work on Portuguese and Brazilian systems took place in late November and early December 1942, when a group of officers were assigned to the unit.[3] These officers confined their attention to Brazilian systems. When Captain Glodell was transferred on 1 May 1943, Lieutenant Haggard succeeded him as Officer in Charge of the Portuguese-Brazilian Section, a post which he has held ever since, except for about three months in the summer of 1944.[4] Of these officers, only Lieutenant Haggard had had

---

3. Lieutenants John V. Haggard, Eugene F. Frey, Wilbur Myers, Theodore F. DeGomar, and Alvaro F. Galvan.

4. Lieutenant Frey was transferred to another station in February 1944, as Lieutenant Myers had been somewhat earlier. Lieutenants De Gomar and Galvan were relieved of their assignments in 1944, but the former was returned to the unit in October.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

academic training in the Portuguese language, and Lieutenants Frey and Myers had taken a short course in Portuguese at the Officer Candidate School, Fort Monmouth. It cannot be said that, with the exception of Lieutenant Haggard, any of these officers possessed adequate linguistic training for the difficult tasks that they faced.

During the spring of 1943 both Sergeant Armstrong and Sergeant Porter were relieved for duty elsewhere. From time to time, beginning as early as November 1942, certain civilians had been added to the unit.[5]

In January 1944 Captain Lowell G. Derbyshire assumed direction of B-III-a, a section then comprising all units working in Romance languages, except French, and in other languages. He adopted at once a policy of greater fluidity in the work of the section under his command. In line with this policy and to make Dr. Oliver's experience available to other units, the latter, though still responsible for cryptanalytic progress in the Portuguese-Brazilian systems, was placed in charge of research in B-III-a. A further change was the use of clerical personnel in more than one unit. For example, decoders might be shifted at times from Spanish problems to Portuguese and vice versa.

---

5. Mr. Sidney Glazier, Miss Eleanor Ely, Miss Letitia Williamson, Mrs. Inez Wright, and Miss Mary Dunn, the last two being still on the staff. In November 1943 Mr. R. Woodrow Harrison was assigned to work on the Brazilian systems, chiefly BZD and BZF; he recently completed in 1944 the reconstruction of the permutation table of the former system.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Foreseeing the ultimate transfer of most of the military personnel in the Portuguese Unit, Captain Derbyshire instituted a course in the Portuguese language, which was taught by Dr. James V. Rice, who had been for about two years a member of the Spanish-American Section. This course was attended by about twenty persons, military and civilian, with the result that the better students were able, after six weeks (three hours a week) to read ordinary Portuguese plain text. It was hoped that by training a number of persons, a few at least would gain sufficient knowledge of the language for assignment to the Portuguese-Brazilian Section. Though this course, good as it was, was too short for adequately training any personnel to do code recovery in the Portuguese language, many of the problems had reached the stage at which they could be managed by less skilled personnel. Some students of the course are now engaged in decoding and translating traffic. Yet it cannot be said that the need for well-trained experts in Portuguese has ever been met.

After January 1942, active work in Portuguese systems did not begin again until midsummer, by which time the importance of Portuguese traffic had increased, since Lisbon had become one of the few neutral capitals still in contact with sources of information in the Axis countries. The newly activated unit under Lieutenant Glodell therefore turned the major portion of its attention to the Portuguese traffic.

Examination of the messages on the Washington circuit established

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the fact that several systems were in current use. Two enciphered codes were recognized, POD and POJ. Without a machine index, about 150 identifications had been made in POD, and a few tentative conclusions about encipherment of POJ had been reached, when, in September 1942, photographs of British work on both POD and POJ were received. In this, all common groups had been identified, and the cipher equivalents of about 80 per cent of the pages had been determined. Translation of current POD messages could now begin. The general outlines of the basic POJ code had been reconstructed by the British, and they had made progress on the substitution tables and transposition. Soon full tables of substitution and transposition were reconstructed. The British also knew that POK was only another encipherment of the basic code underlying POJ, and not, as had been supposed, a different book; so this system too could speedily be solved. Moreover, the British supplied information concerning the encipherments of POF and POI: a large number of groups in these encipherments had been correlated with the POJ encipherment. Work was at once started on POF and POI, and although at first messages could not be fully decoded, values were steadily recovered and partial translations were soon possible.

Late in September 1942 the unit received, through the cooperation of the FBI, photographs of two Portuguese codes. One of these proved to be the fourth edition of the diplomatic code, now known in three

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

encipherments (POA, POB, and POR). Traffic in POA was relatively light; the system was even then practically obsolete. The relationship, however, between this code and the POB encipherment used in Mexico City traffic was recognized, and it was soon possible to submit partial POB translations also. The second code (the fifth edition) received from the FBI was used on the New York circuit; although unimportant in itself, this material proved to be extremely helpful in the solution of other Portuguese systems because of their relationship.

The substitution and transposition patterns of POH were solved, and a beginning was made on the recovery of values, with the result that the first translation was made about the first of December 1942. Traffic on the Buenos Aires, Ankara, Budapest, and Bucharest circuits was recognized as an encipherment of the sixth edition (POJ), and a beginning was made on what was then the most complicated Portuguese system (POG). Solution of this system was facilitated by the interception of a series of messages discussing the same subject in other systems, and the first translation was made on 23 December 1942.

By the beginning of 1943 the Portuguese Unit was reading current traffic in POA, POB, POC, POD, POE, POF, POG, POH, POI, and POJ. Translations were made of at least part of every message. Since the staff was too limited at the time to handle both the diplomatic and colonial systems, it was decided to do nothing with the less important colonial traffic. Later, however, in the summer of 1944, when the British sent

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

reconstructions of a number of colonial systems, active work was taken up on the colonial systems so far as the scant volume of intercepted traffic permitted.

Early in 1943 a beginning was made on POK, which is a secondary encipherment added to POJ. In the first six months of 1943 also appeared the first Portuguese cipher systems: POQ appeared on 13 April 1943 and POP on 6 June 1943, and in both cases the first messages were solved on the day they were received. POR appeared on 20 April 1943 in the Washington and Mexico City circuit and was soon recognized as distinct from POA or POB but based on a repagination of the same code. POL appeared on 7 July 1942, but little was done on it until 1943, by which time sufficient traffic had appeared for a machine index. About this time a photograph of the sixth edition of the Portuguese diplomatic code was received from the FBI. This has proved invaluable, since this edition has been used with no fewer than eight encipherments up to the present.

In the autumn of 1943 the Portuguese colonial office adopted the Hagelin machine. This traffic, like later military ciphers, is processed by the Hagelin Section and sent, when deciphered, to the Portuguese Section for translation.

As for Brazilian systems, it was found that not only BZC and BZD but at least three other systems were present in the traffic, including

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

a pentagraphic system with transposition or other encipherment, and a second with tetragraphic groups. The latter (BZF), which included the largest bulk of the traffic, was studied first. The system of "dominant letters" (a code-group limitation) used in the third position of each tetragraph was identified, and a message print and index was prepared. About 150 identifications in BZF had been made when it was decided to suspend work on it in order to give more time to Portuguese traffic. At the same time a general survey of other Brazilian systems was undertaken. The cipher system BZD was segregated and turned over to the Cipher Section for solution. A large part of unreadable traffic from Caracas, Mexico City, Bogota, and Ciudad Trujillo was recognized as a series of encipherments of the BZF system. Messages from Cayenne were in a code (BZH) not otherwise known and set aside for accumulation of traffic. Traffic in BZE, on the New York circuit, had been examined and sufficient identifications made to indicate its unimportance. It was later discovered to be nothing more than the second edition of the Mascotte Commercial Code in both enciphered and unenciphered forms. The importance of BZH was recognized, but no study of it was made for lack of sufficient personnel.

In August 1942 the attention of the Portuguese-Brazilian Section was largely focused on Portuguese systems, to the neglect of Brazilian systems, and this condition prevailed until November, when Mr. Glazier began work on BZC and BZD. Soon afterwards, Lieutenant Frey took over

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

BZC, and in March 1943 Sergeant Armstrong took over BZD. At about the same time an index of BZF traffic was made, and active work on this system was initiated, the first translation being prepared in March 1943. Copies of British work needed to be done before current traffic could be completely read. In the case of BZA, traffic had almost entirely ceased.

In 1944 new systems were introduced but in such limited volume that solution was impossible, though the general nature of the new systems was understood. The chief solutions in the field of Brazilian cryptography include BZC, BZD, BZF, and, though less complete, BZH. BZA and BZM, systems based on the same compilation as BZD, have been solved. Lack of traffic has caused 16 of the known systems to remain unsolved. Of these, six are known only from British information (BZR-1 to BZR-6); five are ciphers in which little traffic is intercepted (BZB-1, BZB-2, BZO, BZP, BZR-7); two (BZG and BZR-8) are special purpose codes used very infrequently; and the remaining three (BZL, BZN, and BZQ) are codes with a limited distribution, introduced too recently for an adequate accumulation of traffic.

Descriptions of the cryptography and cryptanalysis of all Portuguese and Brazilian systems studied in the Signal Security Agency have been prepared for the Cryptanalytic Series: Portuguese Codes and Ciphers 1941-1944 (IR 4051) and Brazilian Codes and Ciphers 1917-1945 (IR 5044).

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER X. THE SYSTEMS OF THE NEAR AND MIDDLE EASTERN GOVERNMENTS[1]

On 17 December 1942 a newly formed group, at first known as B-II-a-13 (later as B-III-a-5 and now as B-III-d-3) was assigned to cryptanalysis of systems used by governments in the Near and Middle East. These included at first the following governments: Egypt, Iran, Iraq, Saudi Arabia, and Turkey; Ethiopia was added to this list in June 1944. The task of this group may be presented as follows:

Arabic: Iraq (one system: IQA[2]); Saudi Arabia (two systems: ABA and ABB);[3]

English: Ethiopia (one system: ETB);

French: Egypt (one system: EGA); Ethiopia (one system: ETA);

Persian: Afghanistan (two systems: AFA, AFB); Iran (three systems: IRA, IRB, IRC);

Turkish: Turkey (ten systems: TUA, TUB, TUC, TUD, TUE, TUF, TUH, TUJ, TUK, TUL).[4]

When the group was activated, it consisted of two persons:

---

1. This chapter is based on interviews with Lieutenant Joseph R. Salem, Mr. Hughes O. Gibbons, and Sergeant Oliver F. Egleston and upon the progress reports of the Near and Middle Eastern Section from December 1942 to the present, signed by Lieutenant Cyrus H. Gordon, Lieutenant Joseph R. Salem, and Messrs. Hughes O. Gibbons and Lewis E. Bates.

2. At the time two encipherments of this IQA were recognized (IQB and IQC) and were thought to be separate systems.

3. Two encipherments (ABC and ABD) were recognized at the time and were taken for separate systems.

4. Two encipherments of TUE (TUG and TUI) were regarded as separate systems.

Doc ID: 6554247

TOP SECRET CREAM

Lieutenant Cyrus H. Gordon, a professional Semitist with four years of graduate work in American universities and four years of travel in Arab lands, and Lieutenant Joseph R. Salem, a native of Syria with an excellent knowledge of colloquial Arabic. Less than a month later two other persons joined the group: Lieutenant Benjamin Schwartz, an Indologist with 16 years of experience in the Indic languages and Corporal Oliver F. Egleston, who had lived two years in Palestine and had studied Arabic in Harvard and Yale Universities.

Within the first few months the group was expanded by the addition of a number of other persons who possessed some previous acquaintance with one or another of the Semitic languages.[5] But not one was an expert in Turkish; indeed, only Lieutenants Schwartz and Downey had even slight acquaintance with it. In Persian and Turkish therefore, the unit lacked trained personnel entirely. The situation in Arabic was somewhat better, but none of the persons available was, at the time he entered the unit, able to read a newspaper in Arabic. Some of them knew colloquial Arabic well enough for conversational purposes, and Lieutenant Gordon knew it from the philological point of view, but, in general, adequate training in contemporary literary Arabic was lacking.

---

5. These included Miss Clarice P. Bailey, a graduate student in Arabic in Columbia University; Lieutenant Glanville Downey; Mr. Lewis E. Bates; Mr. Hughes O. Gibbons, a librarian who had taught for five years on the faculty of the American University in Cairo; and Miss Ethel R. Albert, who, though born in America, is of Syrian descent and speaks Arabic.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Linguistic deficiencies as serious as these might have been supplied by recruiting either professional scholars fully acquainted with the three languages or Americans long resident in the oriental countries, or even naturalized Americans who had been born in those countries. But professional scholars in these languages are few in number, and only one (Mr. Gibbons) was ever recruited from among the resident Americans of the second group; considerations of security made recruiting in the third category unattractive. Repeated attempts to recruit military personnel trained by the Army Specialist Training Program always resulted in failure.[6] The result was that the group working on systems of the Near and Middle East had to carry on its work with a staff insufficiently trained at the outset to perform the necessary linguistic tasks. This experience is in marked contrast to that of GCCS, which had the incalculable advantage of an adequate number of experts in all of the oriental languages.

The primary task, therefore, was that of increasing the knowledge of Arabic of those who already knew something of that language and to train the entire staff in Turkish. This situation was acute because of the volume of the traffic. The traffic in the Turkish systems was moreover, the most voluminous, and the importance of Turkish traffic

---

6. This failure is surprising since in at least one instance an enlisted man working on Japanese problems in this Agency, reported that he had had ASTP training in Turkish!

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

from the point of view of intelligence was, as always, greater than that of any of the other systems studied. It was necessary therefore to give instruction in Turkish to two groups: (1) persons already acquainted with one or another related language, and (2) persons without such experience but with aptitude and energy sufficient to approach a language unlike European tongues. Accordingly, an extensive program of training in Turkish was, almost from the very beginning, a constant feature of the work of the unit, at times as much as an hour a day being spent in such instruction. The burden of this instruction fell largely upon Lieutenant Schwartz; Sergeant Egleston completed, on 5 August 1943, a grammar of the Turkish language presented in eight lessons which drew illustrations from Turkish telegraphic texts. The training program was a decided success. Meanwhile, cryptanalytic problems were not ignored.[7]

When work began in December 1942 attention was directed to Iraqi traffic, though Turkish and Iranian were also studied, but by the end of the first month the emphasis had shifted to Turkish where it remained thereafter. For three weeks Lieutenant Salem and Corporal Egleston were detached from the unit to transcribe in the Library of

---

7. Among the cryptanalysts were the following who joined the unit early in 1943: Mrs. Flobeth Ehninger, Miss Elmire Lobeck, Miss Sally Peebles, and Miss Mary M. Bennett. Others who have made substantial contributions to the cryptanalysis of the systems include Miss Margaret H. Holliday, Miss Margaret J. Craugh, Miss Gloria Templeman, Miss Jane E. Dunn, Miss Mary Keith, Miss Helen Rotter, Miss Marjorie Walker, and Mr. N. Lloyd Hampton.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Congress an Arabic-English, English-Arabic glossary of more than 10,000 modern terms, which had been prepared by the Office of Strategic Services. Work continued in the unit on studies of plain-text frequencies in Arabic, and the traffic was edited for IBM processing. By 14 February 1943 the traffic in TUB, a Turkish two-part code using a four-digit group, was ready for processing, and the work was begun on TUA, a one-part code with a five-digit group. About the beginning of March 1943 work on a biographical file of prominent persons in all countries in the Near and Middle East was undertaken. This continued to grow and at present contains about 4000 entries. Later in the same month two forms of TUA (the so-called "01" and "98") were correlated, and language studies of Turkish were made by IBM methods. By this time the solution of an Iraqian cipher had been advanced, and by 4 April most of the groups for numbers in the Turkish TUB system had been recovered, the first current TUB was ready on 15 May, and the first translation appeared in the Bulletin on 21 May 1943. By the end of May four Turkish, three Iraqi, one Egyptian, and one Afghan system were under study, and by the first of July another Turkish system had been added.

In the middle of July GCCS sent photographs of three compromised Iranian codes (IRA, IRB, IRC) and their reconstruction of the basic Afghan code (AFA, AFB). These were transcribed from the Persian script into the Western form for use in the unit. The reconstructed

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

TUB was also received about the same time. In this period 24 Turkish systems were recognized, but later study reduced this number to 12 basically different systems which employed only 8 different codes.

A report for 10 September 1943 shows the status of the various systems as follows:

> Turkish: TUB is compromised and everything of consequence in it is translated. TUA is far advanced and three people are working on code recovery. Two are working on the recovery of TUE--half of the groups in current messages are already identified. TUD has just been solved, while TUJ, a similar problem involving the encipherment of the first three digits of the four-digit TUB, is being cryptanalyzed. Three people are engaged in solving the forty-digit additive of the secret traffic from Washington, London, and the other cities.
>
> Persian: Under control. All encipherments of the compromised code are solved by Mrs. Ehninger and the messages are promptly translated by Mr. Gibbons. The latter is also working on the recovery of IRC.
>
> Afghanistan: Two people are simultaneously attacking this enciphered trigraphic code in Persian from the points of view of encipherment and code recovery.
>
> Iraqian: Solved and translated promptly.
>
> Egyptian: Over a third of the groups appearing in current messages are now translatable. One person is working on code recovery.
>
> Saudi Arabian: The two short messages that have reached us have been carefully analyzed, but we must have better coverage for a solution.

On 1 October 1943 Lieutenant Gordon was transferred, and Lieutenant Salem assumed charge of the unit, a position which he held except for five months (May-September 1944) until 19 May 1945, when he was transferred to the Supply Branch. About this time GCCS sent 3,000

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

identifications in TUE. Of the 1,200 which had been recovered by the Signal Security Agency, 200 were not duplicated in this list. Early in October 1943, five days after the receipt of the first message, the unit solved ABB, a cipher used by the Arabian princes on their visit to the United States.

Throughout 1943 the unit continued gradually to expand and by the end of November had reached a strength of 20 persons. Soon afterwards, however, three persons were detached to work on Japanese problems. January 1944 saw a change in policy. Higher authority decided that the Signal Security Agency would turn over to GCCS the chief responsibility for processing traffic in the systems used by the governments in the Near and Middle East, maintaining, however, as a nucleus for cryptanalytic continuity, a small section of six persons. Accordingly, 14 of the members of the unit went to other units. Shortly thereafter the critical situation as regards personnel eased up somewhat, and the need for the intelligence produced by the unit was recognized. Hence, the Branch reactivated the original unit with its former personnel. Two returned in February, three in March, one at the beginning of April, and by 13 May 1944, all but one of these persons were again at work in the unit, which, with the addition of other personnel, now had a strength of 21.

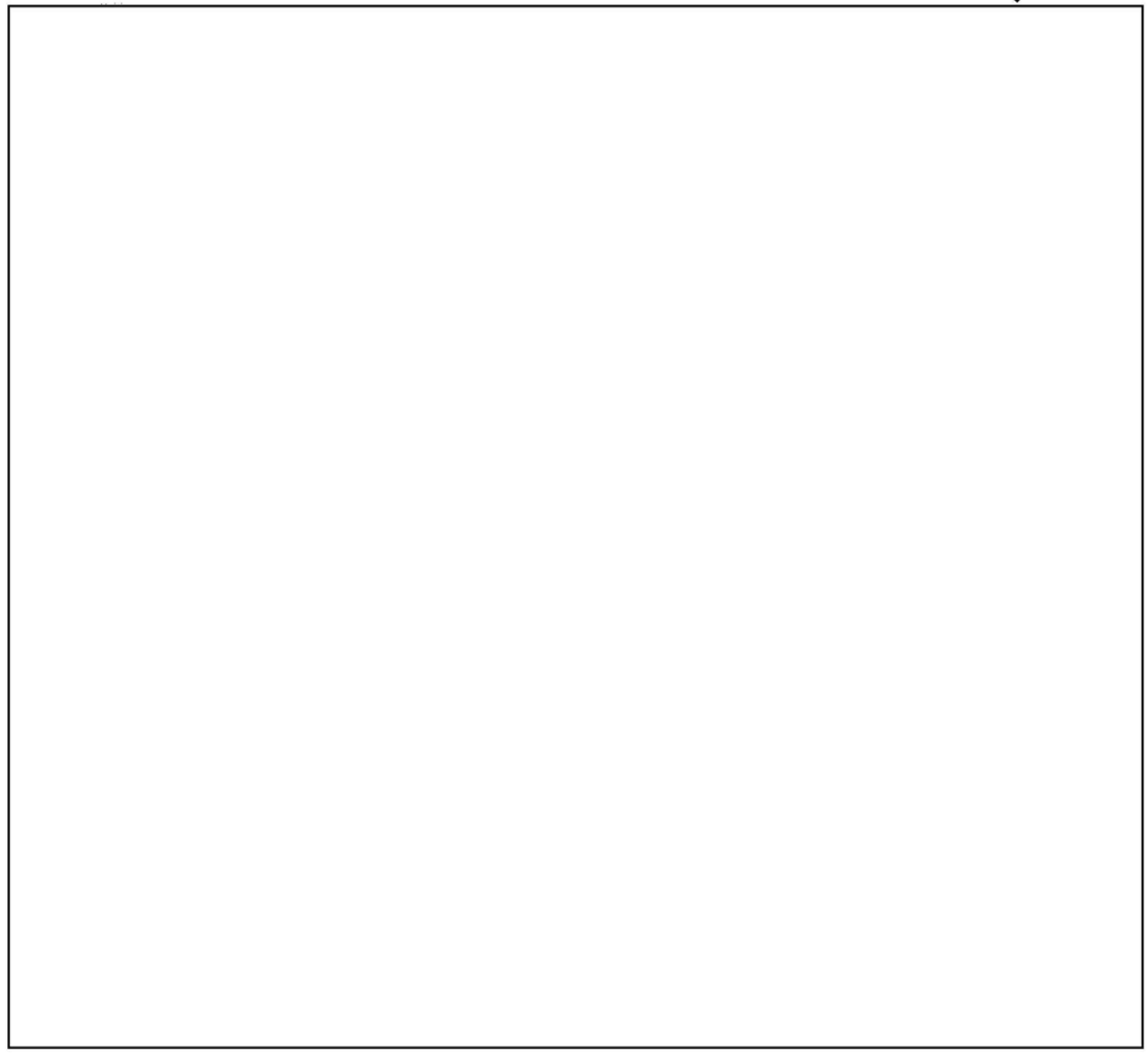
On 28 April 1944 Lieutenant Salem, relieved for other duties, was succeeded by Mr. Bates, who himself resigned on 1 September 1944. During September Mr. Gibbons directed the Near and Middle East Section

TOP SECRET CREAM

Doc ID: 6554247

until Lieutenant Salem returned on 1 October 1944. In November Sergeant Egleston brought back with him the great advantage of experience gained during several months of work in collaboration with British cryptanalysts.

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)



Doc ID: 6554247

TOP SECRET CREAM

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

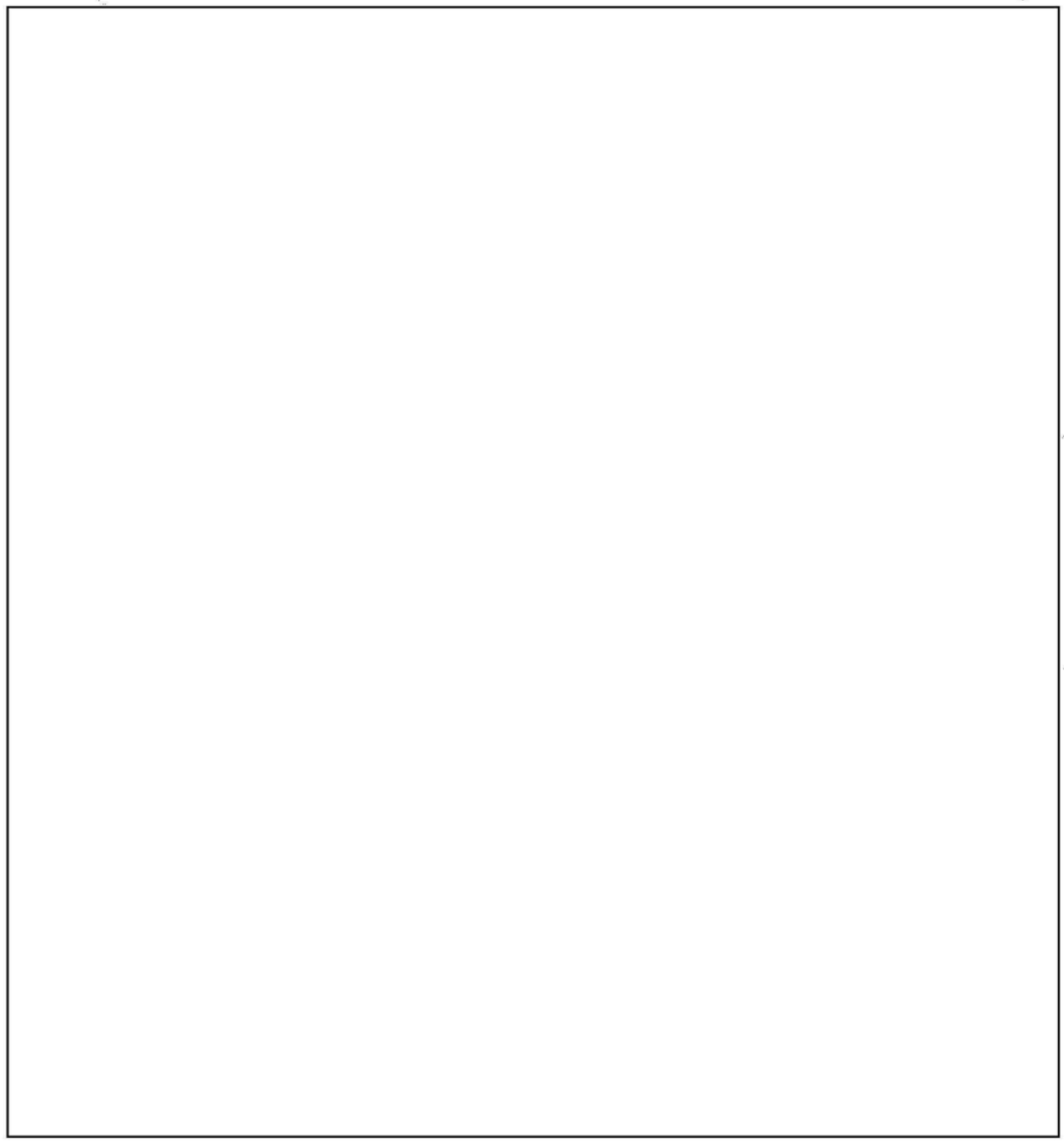
TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

X. The Systems of the Near and Middle Eastern Governments 179



TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XI. FAR EASTERN AND CENTRAL EUROPEAN SYSTEMS[1]

A. Chinese Systems

B-III-d-2 is at the present time (August 1945) charged with the production of intelligence from the traffic of certain governments in the Far East and in Central Europe. The governments in the Far East included at one time or another the Chungking government, the Nanking puppet government, the puppet government of Thailand, and the puppet government of the Philippines. The countries of Middle Europe included the Nazi government of Bulgaria, the royalist government of Yugoslavia, the puppet government of Croatia, the Czechoslovakian government in London, the Slovakian puppet government, the Polish government in London, and the royalist government of Greece. The two groups, though not related geographically, are combined in one unit because they require similar cryptanalytic techniques.

Chinese systems were the first to be studied in a unit composed largely of linguistic experts. Soon afterwards the system used by Thailand (THA) was added. As work progressed, however, more cryptanalysts were needed, and two separate units were formed. They had contiguous quarters and were finally united administratively in 1944. In the course of solving the encipherment of the Chinese systems, the staff of the cryptanalytic unit developed considerable skill precisely

---

1. The statements made in this section are based on interviews with Dr. Leslie A. Rutledge, Lieutenant Laurence P. Roberts, and Mr. Raymond P. Tenney.

Doc ID: 6554247

TOP SECRET CREAM

of the type needed for other problems; so it was natural that when interest arose in 1944 in Balkan cryptography, the several Balkan systems, not easily fitting into any other then existing unit, were assigned to the now combined Far Eastern unit, which thus became a sort of catchall for many systems hard to classify elsewhere.[2]

Work began on Chinese systems in a unit organized in January 1943 under the direction of Captain (now Major) Franklin F. Russell, who had been for some time in the Japanese Military Attache Section. The chief expert in the Chinese language was Mr. Raymond P. Tenney, who for 20 years had resided in China as a member of the United States Consular Service and as an employee of the Chinese Government Salt Monopoly (the Salt Gabelle). Lieutenant Laurence P. Roberts, in civilian life Director of the Brooklyn Museum, had studied the language in China. For a short time Lieutenants Harry Koslow and John Haynes, both of whom had lived in China and knew colloquial Chinese, were with the unit before being transferred elsewhere. A little later Lieutenant Rudolph McShane, whose avocation for many years had been Chinese, and Miss Hazel Gosline, who had taught in China for 17 years and is skillful in Chinese calligraphy, joined the unit. Several other persons with some knowledge of Chinese, who joined the staff in 1944, are now at work: Miss Margaret Sells, who had been a missionary in

2. Rumanian and Hungarian systems, though geographically akin to other Middle European systems, were studied in another unit.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

North China for some years; Mrs. Elizabeth Warner; and Private First Class Robert King, one of the few persons trained by the Army Specialist Training Program in languages rarely studied in this country to come to the Branch. While the staff was at all times adequate in quality for the tasks at hand, sufficient personnel were never available for the linguistic problems.[3]

The unit began by sorting all of the accumulated Chinese traffic, a task which took some time since there were many systems and many circuits represented in it. Eventually the traffic in certain unenciphered codes was isolated and prepared for IBM processing. Among these codes were the Chinese Ming Code (CNA), available in the open market, and the secret codes Dryo (CNB), Win (CNC), and Invincible (CND). Although the intelligence contained in it was not particularly important, Mr. Tenney began to decode and translate the Ming traffic. This effort to find frequency characteristics in telegraphic Chinese which would assist in entering the unknown codes was somewhat disappointing, for the secret codes, unlike the single-character Ming code, were phrase books and lacked marked frequency characteristics. But CND was soon entered. A one-part code in English, it was studied only for the purpose of training. It became readable in July or August 1943. This

3. Captain Russell had meanwhile been succeeded, at first by Lieutenant Haynes, and then by Lieutenant Culver C. Chamberlain. By June 1943 Lieutenant Roberts assumed direction of the unit, a post which he still holds.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

date also marks the end of preliminary examination and experimentation in method and the beginning of serious solution and steady production.

At this time GCCS gave considerable help. Early in the summer a photograph of the British reconstruction of CNB soon made current traffic readable. A reconstruction of CNC was received at about the same time, and some two months later it became readable. Towards the end of the summer another Chinese code (CNF), partially reconstructed, was supplied by GCCS and additional identifications were exchanged from time to time until, at the end of the year, the code was readable.

Many Chinese encipherments used on the codes then being read had been explained in various communications from GCCS, and once their pattern and method was understood, others could be solved in most instances by the linguistic staff, but there were still other enciphered-code systems of which nothing was known. Two of the largest (CNG and CNH), used mainly by Dr. T. V. Soong in his correspondence with the Chinese Mission in Washington (SINODEFENS), had been isolated in the first sorting of the traffic and given to the Research Unit of B-III for study. Some suggestions made by Lieutenant (now Major) Charles J. Donahue of the Cipher Section for an attack on CNH were carried out during April by Miss Nellie F. Wood and Miss Edna Waldeck. In May Lieutenant William S. Smith directed a re-examination of both systems and set up elaborate logging and charting techniques; he also

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

planned a more exhaustive indexing procedure for CNH.

In June 1943 Dr. Leslie A. Rutledge was made supervisor of Chinese cryptanalytic problems,[4] coming to this new work from extensive experience on a variety of cipher systems, and Lieutenant Elwood Hill joined the staff after some successful work on two Swiss systems (SZM, SZN), contributing to the analysis and decrypting of CNH.

By September 1943 the 70 digraphic substitution tables used in CNH had all been recovered, and two (later three) IBM message prints and indexes to 30 odd underlying codes (presumably different paginations of one basic code) had been given to Lieutenant Robert's staff for study. The Far Eastern Subsection determined that the codes were actually in Chinese and made a few identifications. But when the cryptanalysts discovered that the underlying codes had no arithmetical relationship to each other and had in fact to be considered as more than 30 separate problems, and that in some cases even a third encipherment had been superimposed on messages of special importance, the system was laid aside as unrewarding.

Facing this impasse, the Subsection turned in the autumn of 1943 to what seemed a still more highly enciphered Chinese code system (CNG), and made a fresh attempt at solution. Some earlier forms of this

---

4. This new unit, which eventually grew to about eight persons, included Dr. Aubrey Diller; Miss Virginia Alderson, who had collaborated with Lieutenant Hill on the Swiss systems; Misses Wood and Waldeck; Mr. Max Lechter, Miss Abbie Cole, and Miss Catherine Snodgrass.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

system were solved[5] during the next two months. It was determined that the basic code was Bentley's Second Phrase Code, but encipherments were frequently changed. Three hundred messages dating from 1932 were decryptographed, which, however, had little value as intelligence.

When the language and cryptanalytic units were given contiguous quarters in January 1944, genuine cooperation on the CNH problems could begin. A still better arrangement was the amalgamation later in the year of the two units, with Lieutenant Roberts and Dr. Rutledge exercising joint supervision. The opportunity afforded members of the units to consult Mr. Tenney and the others on the background of the traffic in CNG, and to assist in the code recovery of CNH by solving spelling encipherments, for example, was gratifying in point of results obtained. The most profitable period of collaboration among the experts in Chinese and the experts in cryptanalysis now began. The cryptanalytic staff had become more experienced and resourceful and once more attacked CNG, which, however, still proved unyielding. The CNL encipherments were quickly solved, and the cryptanalysts then turned their attention to the traffic of the Nanking government (CPA). Among a great many unknown systems, three (CPB, CPC, CPD) were isolated. They were extensive repaginations of the Chinese Ming Code, but sufficient traffic was not available to make them readable until the middle of 1944. Much of the rest of what was at first designated CPA

5. See the paper on CNG prepared by the Recorder's Section.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

was proved in that period to be Japanese commercial traffic and turned over to the Japanese Diplomatic Section (B-III-f).

By the spring of 1944, CNB, CNC, CND, and CNF were easily readable. It was then possible for the staff to undertake the cryptanalysis of other unknown codes. The attack on CNJ, a modified one-part code in Chinese, was immediately successful, and--this time without assistance from GCCS--messages were regularly read within three months. In March 1944 the cryptanalysts had solved the polyalphabetic encipherment of messages in CNL, which was, according to the statements of the Chinese themselves, their most secret system. An attempt on code recovery showed this to be a large two-part code, but the staff was now experienced and confident, and 600 identifications had been made by the time the first exchange with GCCS took place. After two months, a few messages were partially readable, and by the end of summer, the major part of current traffic could be read.

After a short period in which Lieutenant Roberts shared with Dr. Rutledge joint supervision over the amalgamated unit, the latter assumed sole responsibility, while Lieutenant Roberts continued to supervise the Chinese language problems. Now began at once the exploration of all unknown Chungking systems, of which there appeared to be many. A number of air attaché systems (CNM) were investigated and eventually there was accomplished the removal of the encipherments from six of these codes, of which only two remained current. The deciphering was greatly facilitated by a machine devised and built by Dr. Martin Joos

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

of the Research Unit. Several of the financial systems used by the Bank of China were studied, and the encipherment of Bentley's Second Phrase Code (CNK) was solved. Several unknown Chinese digit systems (CNQ), were examined. Another financial and diplomatic system based on an English code (CNN) was studied and solved. Some interesting solutions of transposed Chinese code (CNP, CNT) were made during the summer of 1944.

At this time all codes currently used by the Chinese Foreign Office (seven in Chinese and one in English) were readable, and current traffic in them was regularly processed. Besides those mentioned specifically, another (CNS), supplied by the British in a reconstruction, had then advanced to the point of being almost readable. During 1944 the cryptanalytic staff removed the encipherments from four Chinese government codes used for military traffic (two called CNM, CNO, and CNP), and a beginning was made on the recovery of all of them. CNP is rapidly approaching readability, and the reading of this military attaché system will no doubt facilitate the reading of the others, which have a vocabulary unlike that of the diplomatic codes. Sufficient transposition encipherment has been removed from CNT, another military attaché code, to make it ready for recovery.

Progress during the past year has continued in the Far Eastern field. Complete or partial solutions of four major Chungking systems were effected, and translations have been submitted in all of them.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Of these four, CNL is one of the principal Chinese Foreign Office systems; it is a code enciphered by substitution and is the first two-part Chinese code to be solved in the Signal Security Agency. The other three, CNM (an Air Force code), CNP (a General Staff code), and CNT (a military and naval attaché system) are codes enciphered by digraphic substitution or by keyed columnar transposition. CNT, used by attachés throughout the world, employs a total of about 400 transposition sequences and at least 18 paginations of the basic code; most of the traffic is now fully readable as a result of the year's work. One minor system, CNX, was completely solved during the past year, and a special system, introduced for the United Nations Conference on International Organization and made up of transposition encipherments of several known codes, was partially read.

Entry was also made into the following major systems, the complete solution of which is progressing: CNG, a new additive encipherment which replaced the substitution encipherment of CNG solved last year; CNQ, an additive encipherment of several basic codes used by the National Military Council in Chungking; CNW, a running-key substitution of a new trigraphic Foreign Office code; and CNY, an additive and substitution encipherment of what is thought to be General Tai Li's code. In CNY, the solution of the old code, which apparently became obsolete in 1944, was undertaken by OP-20-G and that of the new code by the Signal Security Agency.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Of the enciphered code systems used by the Nanking Government, the majority were entered or completely solved. The following systems were brought to readability during the past year: CPB, CPC, CPD, CPI, and CPJ. Translations were made in all except CPJ.

B. The Thai Systems

Not long after the first study of Chinese systems, plans were laid to begin the study of the messages sent by the government of Thailand. To hope for solution without the assistance of an expert in the Thai language was thought impossible, and for this purpose the services of Mrs. George B. McFarland were secured.[6] Cryptanalytic research was performed by Mr. A. Ferdinand Engel, then Technical Director of B-III-a, of which this unit was at the time a part, and by Lieutenant Karl Elmquist and Mr. John W. Little.[7] It was soon discovered that the Thai were using English rather than their own language--hence the linguistic difficulty which had been envisaged proved to be illusory, but the intimate acquaintance of Mrs. McFarland with the leading Thai officials proved to be extremely valuable in interpreting the Thai messages.

The Thai code, a relatively large one containing about 100,000 groups, was made readable by the end of 1943.[8] The constantly changing

---

6. Mrs. McFarland had lived in Bangkok from 1908 to 1942 and had collaborated with her late husband on a monumental dictionary of the Thai language.

7. Mr. Little's close contact with the Thai problem was broken when he was inducted into the Army. Though his services were repeatedly requested after that time, he was ultimately sent overseas.

8. Miss Martha Stifler (Mrs. Waller) and Mr. David Kinney worked on code recovery after Mrs. McFarland's departure in January 1944.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

encipherments of Thai, which presented no great difficulty, finally could be removed as promptly as they appeared. The encipherment of a new code system used by the same government was solved in 1945, but the language of the basic code has not yet been determined. The intelligence recovered from Thai messages continued to be of interest; many of the messages were sent through German channels, one of the last to be sent before the surrender being in a new system (THC).

C. The Middle European Systems

In April 1944, shortly after the amalgamation of the Chinese language and the Chinese cryptanalytic units, the functions of the new subsection were extended to cover the traffic of seven minor European governments, both Axis satellite and Allied. Greek traffic was first examined because the subsection possessed a classical scholar who also knew modern Greek.[9]

The Slavic languages were at first represented by Captain Ferdinand W. Coudert, who did much of the preliminary research. The Polish group consisted of four persons,[10] while other Slavic languages were cared

9. Dr. Aubrey Diller. Later Miss Mary Fennel, who had studied ancient Greek, and Lieutenant Praxythea M. Coroneos (Mrs. L. A. Rutledge), and Miss Elaine Pulakos, who were of Greek descent, contributed to the new effort.

10. Privates Marcella Gwiazdzinska and Ruth Lowenthal, and Misses Sophie Shaffer and Phyllis Krus.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

for by another group of five.[11] Captain Coudert devised linguistic tests to determine the fitness of the personnel for this sort of work and began a training program in the minor Slavic languages so that those who possessed a knowledge of one of the languages might communicate this knowledge, if possible, to the others.[12] In addition to these persons, an enlarged staff of clerks and typists to carry on the heavy burden of indexing, filing, and typing, was necessary, with the result that the strength of the subsection (supervisors, linguists, cryptanalysts, and clerks) was and remained about 50 persons, who, in December 1944 were responsible for the cryptanalysis and processing of 4 Bulgarian, 2 Croatian, 4 Czech, 4 Greek, 1 Philippine (not studied), 7 Polish, 1 Slovakian, and 3 Yugoslavian systems in addition to the Chinese and Thai systems. In June 1945 these figures were 2 Bulgarian, 28 Chinese, 4 Czech, 5 Greek, 6 Polish, 1 Slovak, and 2 Yugoslavian systems in addition to plain text in 8 different languages.

As work began on new traffic, Lieutenant Coroneos took over the Greek problem as soon as it was discovered that one of the systems (GRB) could be read from a compromised code. Shortly afterward, regular

---

11. Mr. Luther Meyer, Misses Regina Badnerosky, Viola Riegl and Julia Lovas, and Private Rosalie Goveker. Mrs. Anne M. Elmquist supplied a knowledge of both Czech and Slovak. Miss Nina Pleshkova applied a knowledge of Russian to the related languages of Bulgaria and Yugoslavia.

12. Somewhat later Lieutenant (now Captain) John Libera, who possessed a knowledge of Polish and also experience as a cryptanalyst, returned from overseas. Others who worked on cryptanalytic problems included Lieutenant E. G. Mann, Miss Charlotte McReynolds, and Miss Cordelia Greene.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

production of translations began. Most of the Greek systems seemed unimportant except for the highly enciphered GRA. A new system (GRE), however, introduced for the San Francisco Conference, was entered, and two of the digraphic substitution tables were solved. An isolog helped to identify several hundred groups in the new code. Traffic in Greek systems lapsed for approximately a month in October 1944 when the Papandreou government moved to Athens, but during the period of the San Francisco Conference 122 messages were received.

Lieutenant Coroneos was then put in charge of a new subunit assigned to the Balkan systems and to the traffic problems in general which were created largely by the new Balkan systems. A group of the newer linguistic personnel (eventually six) worked on the Yugoslavian (YOA) and Bulgarian (BUA) codes, and the Bulgarian military attaché ciphers (BUB, BUC, BUD). Some of the repaginations of the codes, together with deciphering tables and most of the cryptographic details of the military ciphers, were supplied by GCCS. YOA was fairly well recovered, but the photograph thereof was very difficult to read, and the typing of it required nearly a month. More time was needed, also, before any of the new personnel could independently translate a message. BUA was much more discouraging since the book was used with many paginations, of which only a few very scantily recovered ones came from GCCS. The amount of Bulgarian traffic intercepted was inadequate since normal communication was by land line rather than by radio, and the intercepts were often defective. Nevertheless, production gradually got under way.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Several important messages in the military cipher (BUC) were deciphered and translated before the British translations arrived, and a few translations were finally achieved in the code systems. About the time (August 1944), when YOA was approaching regular production, the cipher tables changed, but constant key recovery kept most of the current messages readable. Progress was made also in BUA in filling in new values and in assimilating and processing additional paginations received from GCCS. An innovation in the principal Bulgarian cipher (BUC) was also solved. With the surrender of Bulgaria, this traffic decreased sharply in volume and in interest and the ciphers disappeared altogether. Work, however, is continuing on a large backlog.

The problems of the other systems were mainly cryptanalytic. SLA, the Slovakian cipher, was analyzed and partly solved by members of the B-III Research Unit, but too few messages were available in the same key for solution. The encipherments CTA and CTB, two forms of the code used by the puppet Croatian government, had already been solved by the B-III Research Unit, but it was felt at that time that insufficient linguistic personnel was available to make a successful attempt at code recovery.

The principal problem produced by the various Balkan systems at the beginning was the sorting, logging, and filing of the traffic in all the new systems and establishing the records necessary for handling translations, whether produced in the Research Unit or at GCCS. Experienced

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

traffic personnel was temporarily assigned or lent by other units, and eventually the task was accomplished, although the difficulties created by the fact that messages bore numbers not taken from consecutive series, were considerable. When the traffic in partially readable systems was finally in shape, the new Traffic Unit attacked the Polish traffic, which it has logged for the past year and in some cases for the past two years.

The Yugoslavian system YOB and all the Czech and Polish systems were given to the members of the Cryptanalytic Unit for study. The plan was to transfer any systems which became readable back to the Processing Unit and to lend members of the cryptanalytic staff to that Unit when further cryptanalytic development was necessary. The major part of the work on Chinese encipherments was now done, and investigation of any further unknown Chinese systems was postponed until the growing interest in the Balkan situation had diminished sufficiently to permit a return to Chinese problems.

In June the B-III Research Unit attacked a cipher used by Mihailovic in occupied Yugoslavia (YOA), but the system appeared to be double transposition and insolvable with the traffic on hand. Meanwhile, Miss Virginia Alderson was put in charge of a unit devoted mainly to the analysis of the Czech systems, all of which were ciphers. Sergeant Jack Levine of B-III Research gave much time to this problem and established the period of a key in CZB which led eventually to solution. The first solution was that of monoalaphabetic substitution with variants

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

(CZD), and in the deciphered material was an isolog which made possible the entering of CZB, a complicated polyalphabetic substitution system with a long running key. With things well under way, Mrs. Elmquist then took over the solution and production of CZB, her staff of three becoming another subunit in Lieutenant Coroneos's unit.

Sergeant Levine continued his researches on Czech systems and discovered that the alphabets used at Bern, recovered by GCCS in a companion system, were only a different form of those recovered here, and that 24 other variant forms could be postulated. This discovery made possible further advance with CZA.

The Polish systems were first attacked by a staff of about eight persons. The initial analysis led to additive recovery which was directed to successful conclusion in November by producing an index and message print of the first Polish code to be cleared of encipherment (PLF). The basis of the substitution encipherment in PLB had been discovered and recovery of the additive beneath the substitution began.

[redacted]

The indicator pattern of the largest of the Polish diplomatic systems, an enciphered code with digraphic substitution tables (PLC), has been solved.

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

To recapitulate, the achievements of the Research Unit include the independent solution of four codes used by the Chinese government and one by the Thai government; the completion of four other Chinese codes, one Yugoslavian, and one Bulgarian code partially reconstructed by GCCS; and the reconstruction of a large number of cryptographic systems and four complete cipher systems. This represents only work that has been completed to the point of full readability: many other systems have been partially solved.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XII. MISCELLANEOUS SYSTEMS

The systems (all of minor importance) of several governments have been studied in the Signal Security Agency either in conjunction with those of some other government or in an independent unit of small size.

[redacted]

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

A. The Belgian Systems[1]

Initial study of Belgian traffic began in the months of February and March 1943 in the Commercial Section as then constituted.[2] This arrangement continued in force until 18 April 1943 when Belgian traffic was sent to the French Code Recovery Unit (B-II-a-1 at that time).

---

1. The statements made concerning Belgian systems are based on interviews with Dr. Caleb Bevans, Miss Helen J. Bradley, and Miss Charlotte Morris. Incidental references to Belgian systems are made in the progress reports of the French Section (22 February 1943--29 January 1944), now on file in the French Section.

2. The reason for this study of diplomatic traffic in a commercial section was the fact that the head of the Section (then Captain William F. Edgerton) was formerly the head of the French Section, to which he ultimately returned at a later date. It has often happened in the Signal Security Agency that new projects have been initiated by those who were competent to undertake them. Later, when greater activity was involved, special organizations are set up to carry on.

Doc ID: 6554247

TOP SECRET CREAM

Code recovery of an unenciphered code (BEA) proceeded with success, but in September 1943 an enciphered form of the same code (BEB) was encountered and four days after study began was solved sufficiently to permit two translations to be made.

Belgian traffic continued to be received and read wherever possible in this same unit until 24 August 1944. In this period such traffic was received into the two categories BEA and BEB; but much of the traffic filed as BEB was unreadable, since actually a third system (BEC), which had not been isolated as yet, was confused with it. After the reorganization of 24 August 1944, a new unit was set up to process Belgian and Haitian traffic (Luxembourg traffic has since been added to the assignment) and as soon as the unit was organized BEC was isolated from BEB and machine indexes prepared for it, making code recovery possible.

In March 1945 these problems were turned over to the section known as B-III-b, which was organized to process commercial traffic. Thus, the story of Belgian solution begins and ends with a commercial section.

B. Haitian Systems[3]

The first traffic in HTA, the only system known to be used by the government of Haiti, was examined by the French Code Recovery Unit on 2 January 1943 and was then given a preliminary sorting, but nothing

3. The sources are the same as those for the Belgian systems.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

more was done apparently until, on 2 December 1943, an IBM index was prepared. It was discovered, however, on 9 December 1943, that the Haitian government was using a slight modification of the Sittler Commercial Code. All Haitian traffic has since then been completely readable. When on 24 August 1944 Belgian traffic was separated from the French, Haitian traffic was included in the assignment of the new unit, and still later (March 1945) was also turned over to B-III-b.

C. Luxembourg Systems[4]

Only a single system (LUA) is known to be used by the government of the Grand Duchy of Luxembourg. No study of this system was made until September 1944, when a copy of the code, not quite complete, was made available by capture.

[redacted]

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

D. Irish Systems[5]

Irish traffic was first studied in the Traffic Section by Lieutenant (now Captain) Stanley H. Simonds. In the early autumn of 1944 the traffic was assigned for study to two members of the Near and Middle Eastern Section. Solution of this traffic has, however, not advanced

4. On Luxembourg traffic the source of information is an interview with Miss Charlotte Morris.

5. These statements are based on interviews with Mrs. Flobeth Ehninger and Miss Sally Peebles.

TOP SECRET CREAM

Doc ID: 6554247

beyond the stage of cryptanalytic research, since only part of their time is spent on Irish traffic.

E. Hungarian Systems[6]

In April 1944 Hungarian traffic was assigned for study to members of the German Section.[7] Mrs. Anne Henry Stallknecht worked on the problem for several weeks in May. Corporal James Bunting was assigned to the unit during May and June and again after his return from Officer Candidate School in November and December. Miss Mary Evalyn Hampton and Miss Mary Margaret Tenneis were added to the group as cryptanalytic aides, and Miss Bertha Pekare in July as translator.

As the traffic was indexed and studied, it revealed characteristics which augured well for its possible solution. Repetitions were well above random, with slightly over 50 per cent [redacted] yet it did not yield to the usual methods of additive recovery. The entering wedge was provided by the discovery in July that at least 12 long messages sent from Budapest to Tokyo in one encipherment had been sent as circulars to European points in a second encipherment.

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

. . . . [redacted]

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

6. These statements are based on an interview with Miss Margaret Tribble.

7. Miss Margaret Tribble, Mrs. Anne H. Stallkneckt, Mrs. Dorothy K. Watson, and Private Margaret Missko. Miss Bertha Pekare served as translator.

Doc ID: 6554247

TOP SECRET CREAM

compared, revealing their interrelationship. The Research Section of B-III was asked to interpret this, and Corporal Walter Jacobs worked out the exact mathematical relationship of the two encipherments of one message. About this time GCCS sent photographs of four different captured code books. Sergeant Daniel M. Dribin, also of the Research staff, reduced the first message to terms of the 1932 code book, since both the code limitations and key limitations indicated that this code was being used, and early in September the first message was readable.

Because the Tokyo system (HUA) derives its keys from the code book itself, solution was complete, and all traffic in this system has since been read. The second system (HUD) is in the key recovery stage. To assist in its solution four more persons were added in October.[8] IBM and RAM studies were made, as well as indexes, listings of differences, and other cryptanalytic devices; about 50 different overlaps provided material for key recovery. To date 51 key blocks and many individual keys have been recovered.

F. Rumanian Systems[9]

The study of Rumanian systems was carried on from February 1943 to October 1944, when, for the most part, Rumanian traffic ceased.

---

8. Miss Ursula Kennedy, Miss Rachel Hoffman, Miss Mary Lou Coury, and Miss Pauline Miller. They worked under the direction of Sergeant Dribin and Miss Olivia Fulghum.

9. The statements made in this paragraph are based on interviews with Drs. James V. Rice, Caleb Bevans, and Calvin Brown.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

This period may be divided into two parts by the month of June 1944. Before June, Rumanian traffic was studied on a part-time basis by members of Romance language Code Recovery Units.[10] They had to begin a file of traffic in some instances dating back to 1937. This they sorted into two groups, one of which was clearly an unenciphered code designated as ROA and the other the remainder of the material. About 20 groups had been recovered when the system was laid aside and not taken up again until GCCS furnished a reconstruction, about five per cent complete, and some information concerning an enciphered form of the same code. With this assistance, code recovery was continued from time to time and a few translations were made.

In June 1944 the Rumanian problems were turned over to other cryptanalysts in the Romance Language Section.[11] They began the problem anew. The Rumanians appeared to be using a number of systems but chiefly two large five-digit codes, which were employed in both unenciphered forms (ROD and ROF) and in enciphered forms (ROE and ROG). Shortly before traffic ceased, another code of similar type was introduced and considerable work was done on solving the encipherment of the second type. Much work was also done on ROC, a monoalphabetic substitution of two digits for one letter applied to a combination of plain text and code groups of two and three letters each with many variants.

---

10. Dr. James V. Rice and Lieutenant Seymour Bloom.

11. Drs. Caleb Bevans and Calvin S. Brown.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

When Bucharest fell to the Russians late in August 1944, Rumanian traffic ceased abruptly except for occasional traffic between points outside Rumania and for plain text. Such traffic as is intercepted is processed; plain text is translated and code recovery is carried on to some extent in the older traffic and in the new, since the systems were not changed with the new government.

G. Liberian Systems[12]

Traffic in the Liberian systems LBA, LBB, and LBC was intercepted as early as January 1942. Early in 1945 it was analyzed[13] and on 29 April the first entry was made into the diplomatic cipher system LBA. On 3 May the first message was read. Analysis of the traffic had revealed the fact that a polyalphabetic encipherment, consisting of 31 alphabets, was used for this system. The encipherment of the enciphered-code system LBB was also partly solved; but it is still unreadable and is believed to contain both diplomatic and commercial intelligence. The LBC system, identified as employing a commercial code book, was being used frequently for personal messages, rarely for diplomatic. Since the study of Liberian messages began, about 50 per cent of the decoded messages have been published in the Bulletin. The exploitation and development of the three systems has been carried on in B-III-b since their first solution.

---

12. These statements are based on an interview with Miss Naomi McElwaine.

13. By Lieutenant Colonel Frank B. Rowlett and Master Sergeant Daniel M. Dribin.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

CHAPTER XIII. THE SOLUTION OF METEOROLOGICAL SYSTEMS[1]

A. The Problem

Accurate forecasting of weather conditions is, in peace time, highly important to many classes of people, especially to agriculturists, mariners, and aviators. For this reason nations in peace time broadcast weather reports from all parts of the world. In order to make these reports intelligible to those who need them, regardless of their language, the International Meteorological Code (IMC) is used, which consists of a synoptic, or succession of digits, indicating the state of various elements of the weather at the point when and where the weather observations were made. A scale of 1 to 10 is used to represent degrees of visibility, etc. As the eighth digit of a normal synoptic indicates visibility at ground level, an "8" or a "9" in this position in the sequence would indicate very good visibility at the time and place of the report. Single observations are broadcast separately, or several are combined in a bulletin known as a collective.

When war breaks out this broadcasting of weather reports and other meteorological information is needed all the more for efficient planning of military, naval, and aeronautical operations. Such reports, must, however, be sent in a form unintelligible to the

---

1. The statements made in this section are based upon interviews with Major Edward J. Wrigley, Major Clinton C. Swears, and Captain William H. Hezlep, and upon the file of progress reports made by Major Wrigley and Captain Hezlep, dating from 15 August 1942 to the present. No progress reports are available for the period of Captain Lyons' supervision.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

enemy. For this reason the various governments have adopted procedures for enciphering the International Meteorological Code or similar systems.

To be useful, weather information must be current,and, since information derived from such reports declines in value very rapidly after the moment of transmission, and after a few hours becomes completely useless, except for historical purposes, the encipherment must be removed with the highest possible speed.

Removal of the encipherment, however, is of little use unless the location of the observer is known. The time is usually in the clear. Since the location is indicated normally by a number which may frequently be changed, its identity is determined from the continuity of weather types and by cryptanalytic means. Radiogoniometry has not proved satisfactory for this purpose, particularly when, in dealing with a collective, its use could reveal at most the location of the central bureau transmitting the collective. Solution of the reports requires a much higher percentage of intercept coverage than is necessary for ordinary diplomatic traffic, and the coverage must represent not a single station but all stations. Because these reports are broadcast at regular intervals rather than throughout the day, it is necessary that many intercept facilities be assigned weather missions at the proper times. A further difficulty is that the reports are broadcast without regard for atmospheric disturbances, and the text

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

of the intercepts is frequently imperfect. Diplomatic traffic, on the other hand, may be broadcast when the operators find conditions satisfactory.

B. The Organization

On 7 May 1942 the Weather Unit was formed for the solution of enemy meteorological traffic and weather reports and placed under the direction of a Reserve officer, Captain Ulrich S. Lyons, who, in civilian life, had been an astronomer attached for many years to the Naval Observatory in Washington. He was, however, transferred to other duties on 15 August 1942 and was succeeded by Captain Edward J. Wrigley, who in turn was replaced in July 1943 by the present Officer in Charge of the solution of weather reports, Captain William H. Hezlep.

As technical expert Captain Lyons had with him Mr. John Hyman, and Lieutenants Clinton C. Swears and James R. Thompson. During the first week, which, for purposes of orientation, was spent at the Weather Bureau in Washington, the Unit was joined by Captain Wrigley, and on 5 July 1942 it was moved from the Munitions Building to Arlington Hall Station. Shortly afterward several young women were added who soon made substantial contributions to the work of the group.[2]

On 1 September 1942, the staff was further enlarged by seven

---

2. Misses Keturah McDonald, Mildred Erskine, Virginia Brainerd, Mary Donahue, and Louise Gordon.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

enlisted men.[3] All of these men afterwards became expert at the solution of weather traffic, and five of them were assigned to units operating in two different theaters, one in the charge of Lieutenant Pfeiffer, the other under Sergeant Myers. The same month also brought to the Weather Unit two other persons who did exceptionally fine work on the cryptanalysis of weather traffic. Miss Belinda Snow was responsible, without assistance, for the solution of the Vichy French traffic. Miss Marcella Davis remained with the unit until the summer of 1944, when she was transferred to another section. Somewhat later Lieutenant Richard W. Stowbridge, who was the first to examine the Japanese weather reports, joined the unit but left for the China-Burma-India Theater in January 1945. Captain Hezlep became a part of the unit on 13 December 1942. In 1943 three other persons were added: Lieutenant William Fleischman, who remained for a year beginning in July 1943; Lieutenant Clifford J. Maloney, who came shortly after Lieutenant Fleischman and still remains; and Mr. Hyman Shapiro, who remained until February 1944. The last named had previously served with the Air Corps as a meteorologist at Tyndall Field, Florida. Mr. Shapiro's extensive experience as a meteorological observer proved invaluable in the cryptanalysis of the Japanese problems.

In addition to the persons named, the Weather Unit made use of

---

3. Paul N. Pfeiffer, Edwin Marton, Hugh Myers, Richard Friendlich, William Morris, Robert Y. Austin, and George Northern.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the services of a large number of clerks. By 21 December 1942 the original strength of four had grown to 16; the maximum strength of 80 persons was reached on 23 July 1943. There was a general decline in number of personnel in 1944. Captain Hezlep now spends part of his time on research and liaison with the field, in addition to serving as Officer in Charge of the Miscellaneous Diplomatic Section, while Lieutenant Maloney carries the now extensive liaison with the Navy. Other than the work done by these two officers, all activity on weather traffic is now being carried on in the field.

C. Training

In connection with the training program of the Unit, three groups of enlisted men as well as one group of officers were trained for the field.[4] These officers never reached the field, however, as the plan was changed. The first group of enlisted men was trained in September and October 1943 and consisted of seven men assigned to the Weather Unit for training and three of the enlisted men already named, Sergeants Friendlich, Marton, and Northern. They were sent first to the North African Theater, later to the Mediterranean Theater, where they were under the charge of Captain Pfeiffer. The second group, under the charge of Sergeant Myers, was trained in the fall of 1943 and is now in the India-Burma Theater. The third group, trained in the summer

4. Lieutenants Joseph R. Salem, Theodore F. DeGomar, Benson K. Buffham, Edward C. Kalb, and Sidney Jaffe.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

and autumn of 1944, consisted of 17 enlisted men destined for overseas. This last group was trained partly at Arlington Hall Station and partly at Vint Hill Farms Station; the instructors were Captain Hezlep, Lieutenant Kalb, and Lieutenant Buffham.

D. Coverage and Traffic Handling

At first coverage was far from satisfactory and frequent liaison with the intercept units of the Communications Branch was necessary. In 1942 and in early 1943 adequate facilities for interception were not assigned to this traffic. For example, on 2 May 1943 a report stated that at that time the British had 40 receivers and 176 operators at work on the weather problem, while for the same period the Signal Security Agency had only four receivers in operation, and these were not used exclusively for the purpose. Furthermore, intercepts were at times received with no indication of the time or station and were consequently of no value.

In addition, the location of the Weather Unit created problems which gradually had to be overcome. In the first period, when the Unit worked in the Munitions Building, and even later, when it had moved to Arlington Hall, traffic had to be obtained first at the Weather Bureau in Washington and later at the Army Weather Central in the Pentagon, by members of the Unit, using private automobiles, and after the encipherment had been removed, the unenciphered traffic had to be delivered by the same means to the Army Weather Central.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Later, teletype facilities were made available, but still not all the problems were solved. When in May 1943 the Unit was moved from Operations A Building to Operations B Building, a serious time lag took place. Traffic had to be carried from the teletype machines in A Building to the Weather Unit in B Building, and, in the case of the German traffic, after rapid editing, it had to be taken once more to A Building for punching by IBM; finally the cards had to be taken once more to B Building for sorting and printing. The problem was further complicated by the fact that at this time Post Regulations made it necessary to use only commissioned officers for carrying this classified material from one building to another. In the early period the problem of transportation was so acute that current traffic was not received during the first hour of business and work on the analysis had to be stopped an hour before the close of business so that the results could be transported to the Army Weather Central in time to be of use. The result was that the working day was in effect shortened to six hours of intensive activity.

E. Solutions

The constantly increasing need for personnel to process the growing amount of traffic impeded the work in the early period. The fact that the traffic of five different governments was studied, however, did not necessitate experts in the languages of those governments, since the International Meteorological Code or its Japanese counterpart was used.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

At the outset, through the study of text books on the subject and of plain-text weather reports which had been intercepted, Captain Lyons gave his group an acquaintance with the basic science of climatology. A week was spent in a course of training given at the United States Weather Bureau in Washington. No traffic, however, was received until about 9 June 1942, when some Russian weather reports became available. The problem was attacked both by the probable word method (that is, likely weather conditions at the time and place of the message) and by frequencies and superimposition of messages. When German traffic was being studied, arrangements were made to use IBM methods for computing the frequencies. These methods could be used in the case of weather reports on the traffic of a single day. For successful solution, about 250 collectives were needed.

During the summer of 1942 chief emphasis was on Russian traffic, studied for training purposes, but early in September French traffic was also received. Miss Snow turned her attention to the new problem and by the end of the month had solved some messages. French traffic continued to be received until the day of the North African landings, when it stopped at all stations except Dakar. The danger to Allied security was at once apparent, and, at the initiative of the Signal Security Agency, diplomatic pressure was brought to bear on the Vichy government to stop the Dakar traffic. After about 10 days the Dakar station ceased broadcasting these reports.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

In September 1942 the Weather Unit was visited by a British cryptanalyst, Dr. George C. McVittie, a distinguished astronomer, who remained at Arlington Hall Station for about two months. The experience of the British on weather traffic was thus made available; Dr. McVittie's chief contribution was the demonstration of the main features of the Italian weather system then current. Italian reports, however, could not be read at once, but with sufficient coverage the additive keys used for messages could, after some study, be recovered.

Italian reports were of all types: land, ship, "raob," and "pibal." The basic synoptic used consisted of 25 digits, but a special 30-digit synoptic was used by coastal stations. Since the numbers indicating the observation stations were not those used in peace times, these numbers were known by the technical term "war indicatives." They changed approximately every 90 days. The code was enciphered by a running additive key, taken from a table valid for periods of 72 hours. Since the key indicators were unenciphered, overlapping was possible to a considerable depth, enabling the first solutions to be effected in December 1942. On the 21st of that month the progress report mentioned that an average of 2,000 lines of weather traffic had been solved and deciphered each day of the preceding week. On 11 January 1943 the corresponding figure was 4,600 lines. From that time on, Italian traffic was readable as long as it was received. For some reason never understood here, this traffic stopped suddenly

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

on 19 July 1943, to be resumed, but in very small volume, for a short time thereafter. In September 1944, with the capitulation of Italy, it ceased entirely.

After the text of the messages was reduced to the basic plain code, it was transmitted to the Army Weather Central in the Pentagon and, from 22 February 1943, directly by teletype from Arlington Hall to Pasadena, California. For a short period the additive keys solved at Arlington Hall were transmitted regularly to the North African Theater, where the Signal Corps personnel were thus able to process new traffic as it appeared. The Weather Unit here functioned as a cryptanalytic staff for operations in North Africa. By 15 March 1943 the strength of the Unit had grown to 50 persons, who worked in three shifts. On 25 April 1943, however, when a decided drop in traffic was reported, it was possible to transfer 10 of the 57 members then in the Unit elsewhere without loss to production.

German traffic was next studied. Although Dr. McVittie during his visit had expressed skepticism concerning the possibilities of solving these messages, Miss Davis spent most of her time on German traffic after September 1942; and in January 1943 Sergeant Friendlich turned his attention to the German problem. At the end of the month progress was reported as very satisfactory. It was found that the Germans were actually broadcasting from their station in Rome reports on weather conditions in Italy which had already been sent out in

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the Italian system. They also were broadcasting reports on Spanish weather conditions which the Spaniards had previously broadcast. Consequently, the Italian messages, which were by this time readable, and the Spanish messages, which were in the clear, supplied cribs for the unreadable German messages. This entering wedge made possible by the end of February 1943 the solution of the German system.

Though the traffic was transmitted in groups of six digits, these were in reality encipherments of five-digit groups. The central digit of the group was enciphered by substitution of two digits which, when added together by non-carrying arithmetic, would equal that digit. This in itself provided no great security, but the group thus expanded was broken into two equal parts, each three digits being enciphered by substitution from a table containing a thousand three-digit groups, valid for a five-day period. There were 12 of these tables, six being reciprocal to the other six. When the six-digit enciphered groups had been reduced to five-digit unenciphered form, a sequence of five of them would constitute a synoptic. The problem of solution was rendered somewhat easier because the Germans used the basic IMC synoptic, a practice which they continued, in spite of its insecurity, to the end of the war.

On 21 August 1943 the regular progress report stated that during the preceding week 7,100 lines of weather reports had been processed, of which 661 were current; on 3 September 1943 the corresponding

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

figures were 3,549 as a total and 2,967 current. Both Italian and German traffic was included in these figures. The traffic which was not current represented the work of the historical group, which worked on old messages. Normally, this traffic has no value, but in July 1943 the Army Weather Central in the Pentagon had begun to make extensive efforts to prepare tables of probable weather on the basis of the averages of observed weather over a period of years. For such tables older reports were not only useful but even necessary. German traffic so processed was received mainly from the British, who had a greater coverage (approximately 90 per cent) of all the messages broadcast.

Intercepts of Japanese weather reports had been received from time to time, and on 25 January 1943 Miss Snow began to examine it. Traffic was too light, however, for active work until July 1943, when a group within the Weather Section was organized under Lieutenant Fleischmann to make the first intensive study of the available messages. After that the Japanese systems were emphasized more and more, and during 1944 they formed the bulk of the studies carried on by the Section. In the case of the systems used by the European governments, large quantities of plain-text weather reports and much climatological information were available from the beginning but when the Japanese systems were first studied very little assistance of this kind was to be had. All material available at the Weather Bureau library was secured, but the Japanese had apparently for many years deliberately

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

concealed from other governments their activity in meteorology. At international meteorological conferences the Japanese delegations had proved very uncooperative, giving their main attention to matters of protocol. In one instance they had even tried to get special weather concessions in the Netherlands East Indies.

Furthermore, the Japanese do not use the International Meteorological Code, but employ synoptic forms quite different from those of western nations. This difference is illustrated in the following presentation of the IMC and the Japanese equivalent form:

IMC

$$III\ C_L\ C_M\ w\ w\ V\ h\ N_h\ D\ D\ F\ F\ N\ P\ P\ P\ T\ T\ U\ C_H\ a\ p\ p$$

Japanese Long Form

$$(GG)\ III\ D\ D\ F\ F\ w\ w\ P\ P\ P\ T\ T\ t\ t\ R\ R\ N\ C_{L/M}\ N_h\ C_L\ h\ D_L\ C_l\ C_l\ V$$

$$C_2\ C_2\ f\ (EE)$$

Accordingly, climatological data had to be gathered from many sources. Early in 1942, however, the secret code, weather report forms, and the key book then currently used for encipherment by the Japanese Admiralty were captured, and they proved of great help.

The Japanese were using, when study began, an unknown number of weather systems. One of these, a naval system known as JN-36, was used for reporting weather observations made at outlying points. These were sent to the Japanese Weather Centrals at Tokyo and other necessary points by relays. Some work was done on JN-36, but insufficient

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

coverage and the fact that the Navy was already reading it led to concentration on another system, JN-37, the main inter-service collective system in which the reports already enciphered by JN-36 are repeated, including JN-36 reports which may never have been intercepted because of the difficulty of hearing remote and isolated stations.

Reports sent in JN-37 consist of a collective message containing from 1 to 250 synoptics either in the long form (32 digits) or the short form (14 digits). Broadcasts conform to a regular schedule; in addition certain special reports are broadcast anywhere from two hours to two days late and are designated therefore as "retards" or "delayed reports." Coverage of JN-37 traffic was sufficient in July 1943 to permit the beginning of solution and it improved in 1944 to such an extent that about 400 messages were received daily. The bulk of these intercepts come from United States Army stations; the remainder are derived from United States Naval and Canadian stations. The broadcasting schedules maintained by the Japanese have been fully worked out in the case of 16 transmitters, which supply 60 per cent of the bulk of the traffic broadcast. Coverage of station TOYOHATA is most complete; traffic from certain other stations is intercepted in insufficient volume to permit the reconstruction of the entire schedule. The station ERIKO in Saigon is one such station, the study of which would probably be profitable if intercepts from foreign sources were obtainable.

TOP SECRET CREAM

Doc ID: 6554247

The basic feature of the JN-37 encipherment is additive taken from a key book of 1,000 pages, each containing 100 lines of 36 digits printed in nine four-digit groups. The point at which the key begins is shown by an indicator. Key Books 1 to 5 were captured in 1944 or earlier; Key Book 6 has not been captured; Key Book 7 was never used by the Japanese; Key Book 8 has been captured, and Key Book 9, which is in current use, is now in process of recovery. The point of attack is the use of limitations of plain values in the synoptic and characteristic frequencies. By these means messages can be placed in depth, and solution is therefore possible. IBM methods are not practical for such purposes and have never been used on Japanese traffic. Experiments have been conducted to see whether high-speed RAM methods may be used to locate messages enciphered in the same key. These experiments have not proven very successful, nor have attempts at solution of the indicator system. Recent developments in the study of the indicators have shown that they are vulnerable in the following respects:

1. The starting points in the additive key sequences used with the delayed messages are chosen carelessly.

2. Both the text and indicators of JN-36 messages have been enciphered by the same line of additive taken from the JN-37 key book. This permits the solution of the indicator when the additive key has been previously recovered.

Late in 1943 and in 1944 the Japanese used three other systems for weather reports, though the exact dates of introduction are unknown. These are: JWE-24, a system used for reporting weather ob-

Doc ID: 6554247

TOP SECRET CREAM

servations to Tokyo; JWE-3, an encipherment by simple additive, solved by the British; and JWE-5, a system about which little is known, but which is thought to be enciphered by a one-time pad. Only one or two messages are received each day in JWE-5. In the same period the Japanese have also used language codes for reporting weather observations. A one-part code of the type usually found in diplomatic systems (i.e., a code group of three digits with plain equivalent representing actual Japanese words) has been enciphered by the keys taken from the JN-37 key book. Earlier forms of the code were captured in the field and later editions were recovered here.

Captured material in the form of code books, pro forma sheets, pages of keys for minor systems, complete copies of the JN-36 and JN-37 key books, and other cryptographic material has been received from other agencies at various times. Some of the pro forma sheets had been used, and were therefore valuable in showing the operations performed by the Japanese code clerks. Complete and technical liaison with the Navy is now carried on by Lieutenant Maloney. Traffic in low-echelon systems solved by the field unit in the China-Burma-India Theater is received by mail but, being delayed, the information to be obtained generally is of reduced value. The United States Weather Bureau, the Army Weather Central, and several American universities have been conducting extensive climatological studies covering the Far East.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XIV. THE SPECIAL EXAMINATION UNIT[1]

The Special Examination Unit (now a part of B-III-d-1) has had during its history three distinct functions: (1) the reading and transcribing of stenographic documents; (2) the processing of documents suspected of containing open code; and (3) the transcribing and translation of radiotelephone conversations intercepted by electric means. Work on stenographic documents ceased after September 1943 owing to lack of material, and the volume of open-code problems sharply declined after July 1944, with the result that the processing of the recordings of telephone conversations, which began to be received in July 1943, has now become the chief activity of the Unit. By 31 June 1944 only two persons remained in the Unit, and language specialists were called in for particular jobs. After the surrender of Germany most of the conversations were in Japanese, and the men at Vint Hill Station worked on these.

None of these functions were being carried on at the time the Unit was organized in February 1943, though in an earlier period (January to August 1942) the Office of Censorship had from time to time submitted specimens of intercepted mail in the Spanish language suspected of containing hidden messages. These were then processed

---

1. The statements made in this section are based chiefly on the progress reports of Captain Edward J. Vogel from 5 February 1943 to July 1944, and also on interviews with Mrs. Jean Hitch Banks, Mrs. Dorothy K. Watson, and Lieutenant L. Clark Keating.

Doc ID: 6554247

TOP SECRET CREAM

by the South American Section under the direction of Lieutenant (now Major) Leroy M. Glodell,[2] but after the dissolution of that Section, in August 1942, this feature of the work was dropped.[3]

The first head of the Special Examination Unit was Captain Edward J. Vogel,[4] who was directed to form a new unit (B-I-s) for the processing of two kinds of documents: (1) stenographic documents captured in the field; and (2) documents suspected of containing open codes. Captain Vogel at first worked alone, but after a month was given the assistance of another officer[5] and in the summer of 1943 the staff was enlarged by a number of persons.[6]

---

2. See chapter VIII, page 150.

3. Some time in 1943 Lieutenant (now Major) Raymond R. McCurdy is known to have worked on press dispatches from New York to Madrid to see whether they might contain open code, but the results were negative.

4. Captain Vogel was one of four persons who served in cryptological units in World War I and also in the Signal Security Agency in World War II. He was an Army Field Clerk in the Radio Intelligence Section, General Staff, in France, in 1918. As a civilian he was engaged in the business of court reporting and was one of the country's leading experts in stenography.

5. Lieutenant Charles E. Lloyd, succeeded on 23 July 1943 by Mrs. Marion Hazard. Lieutenant (now Captain) L. Clark Keating assisted Captain Vogel in his spare time from September 1943 to May 1944.

6. Misses Dorothy M. Presnell, Annette K. Robinette (Mrs. Herther), Nell McMillan, Cordelia Greene, Jean Hitch (Mrs. Banks), Jacqueline Fowlkes, Virginia V. Summey, Mary G. Murray, Kathleen Pearce, Eleanor P. Horsay, and Dorothy Jarmon.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

At the outset Captain Vogel familiarized himself with a collection of shorthand text books in English, German, French, Spanish, Italian, Japanese, Greek, Hungarian, Turkish, Serbian, and Croatian, which had been the property of the Shorthand Subsection of MI-8 in World War I, and constructed a file of extracts from these text books to serve in the ready identification of stenographic systems in the major European languages and even in Esperanto. On 11 February 1943 the first material arrived: a quantity of German stenographic documents including three personal diaries, six small notebooks, and 58 loose sheets, captured in North Africa on 7 November 1942. This material, forming the bulk of the stenographic material received by Captain Vogel, proved to contain much intelligence concerning the German occupation of North Africa and French armies and materiel in Morocco. There was the day-by-day diary of a German officer from his induction in Germany to the time when he was a member of the Armistice Commission in North Africa, with such items as information concerning his pay, the morale of the troops, the treatment of the French, and observations on the terrain, the population, and the customs of the country. Two lengthy reports on this material were prepared on 25 March and 3 June 1943. Some idea of the nature and difficulty of the work may be derived from a quotation taken from Captain Vogel's progress reported dated 1 June 1943.

> Reading shorthand notes, especially in a foreign language, is a slow process, and by the time they are translated and typed, and enough gathered together to warrant making a report, a considerable period may elapse. Then it is naturally somewhat

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

> discouraging when that material turns out not to be of any great moment. It should be obvious that any shorthand notes seized from the hands of the enemy, or of a suspicious kind, should be deciphered, because their contents cannot be even surmised until that is done. And once they have been read and translated, even though a great deal of the subject matters appears to be of an irrelevant nature, the translation might as well be forwarded to G-2 for them to get whatever intelligence they can out of it. The reading of an enemy officer's correspondence and diaries certainly ought to produce some information of value, even if only historical.

It was intended from the beginning that the Special Examination Unit should process documents suspected of containing open code, and the first two plain-text messages were received from the Office of Censorship on 23 February 1943. The first successful solution of an open code was reported on 9 March 1943. Not many documents were received, usually not more than five or six a week. The following list, taken from a special report dated 14 May 1943, shows the sort of material upon which the Unit worked:

> letters or documents passing through the Military Censorship;
> suspicious documents found in the baggage of enemy agents;
> suspicious document found in a defense plant;
> suspicious document found near an alien detention camp;
> radio broadcasts;
> press releases;
> cablegrams and telegrams;
> newspaper articles;
> letters of Japanese and Italian prisoners of war; and
> letters from civilians to the War Department with reference to codes and ciphers.

The work on this material was, in Captain Vogel's words, "a court in which many are accused but few are convicted." A huge amount of

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

drudgery is involved in the examination of this material which for the most part produces negative results. Negative reports, however, are not without considerable interest, particularly when they clear the writers of the documents from suspicion; and on those occasions when positive results are obtained, the information derived is often highly useful.

In order to shorten the processes of testing suspected documents for open code, a set of 130 operations was derived and systematically applied to each document. For example, operation No. 98 was to read every eleventh letter starting with the sixth letter. After operations Nos. 1 to 97 had been applied to a certain document, operation No. 98 was applied and produced the following sequence:

RASPIHSOGRACWENROBRAHEDISNI

Since each sequence was read both forwards and backwards, the hidden message appeared:

INSIDE HARBOR NEW CARGO SHIPS, etc.

To apply all of these operations to a message was a laborious task. Accordingly, a method of speeding the process was devised. It was now necessary only to copy the message a few times on cross-section paper of the same scale as especially prepared grilles, which made possible the rapid reading of the text in every position. Using these one person could process from 10 to 12 ordinary plain-text messages in a single day.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

On 16 June 1943 the Unit was presented with its first extensive problem in open code, a task which engaged the major portion of the Unit until January 1944. The suspension of cryptographed communications between Axis governments and their representatives in Buenos Aires made it seem likely that these governments would attempt to use open code in place of the former secret communications. It was therefore planned to route all plain-text messages in the traffic to and from Buenos Aires through Captain Vogel's office. The messages were first read by persons in the appropriate language units, and certain messages were selected for processing: messages not entirely intelligible, messages between suspect correspondents, or messages having any unusual character. Some idea of the magnitude of this task may be gained from the totals of messages received. On three days in July 1943 (the second, third, and fifth), the totals were: English 253; German 282; Spanish 275; Italian 105; French 56; Japanese 2; Portuguese 8. For the week ending 29 October 1943 the totals were English 644; German 275; Spanish 1163; Italian 20; French 121; Japanese 0; Portuguese 6. In January 1944, when this work ended, about 2,000 messages were being processed each week. The results of all this work were entirely negative, as were similar attempts carried on in GCCS. There was, however, a large amount of clandestine traffic. On 8 September 1943 the Germans were reported to have sent 182 permitted messages to Buenos Aires and 58 clandestine; from

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Buenos Aires, the totals were respectively 52 and 438. As long as the transmission of clandestine traffic was possible, the Germans probably did not need to resort to the extensive use of open code. There were, however, in traffic intercepted in other systems a number of indications that open-code messages were being used, for the Japanese referred on one or two occasions to information received "in plain text" from their agents in Argentina. If these statements are bona fide, then the messages referred to were not found by the Signal Security Agency. But it should be pointed out that in one type of open-code message, when, for example, correspondents have previously agreed that they will send a message merely acknowledging receipt of a message, and the addressee will then understand that some totally different plain equivalent is meant, it is practically impossible to detect such a message short of capture of the system. Similar tests were also made in August 1943 on Domei broadcasts suspected of containing open-code messages to Japanese in Argentina, but with negative results.

A second problem, on which work was done between 9 July and 10 September 1943, involved the testing of 840 messages sent by officials of the Philips Export Company. The volume of traffic sent by these officials drew the attention of the FBI to this company. Accordingly, the 840 messages were tested by the Special Examination Unit, and in this case positive results were obtained which were helpful to the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

FBI in handling the case.

Another interesting problem was the so-called Friedman Secret Writing Case. In all, there were 20 letters, dating from the period 17 November 1941 to 13 November 1943, which were sent from the United States to correspondents in South America. Each of the messages contained a cover letter in English and a letter written with secret ink. The secret text was in a variety of languages and consisted of plain text mixed with cipher. The cipher, which was solved in several of the instances by Captain Vogel, was based on a key taken from a pocket volume on the opera and from other books not identified. The Special Examination Unit contributed substantially to the solution of these letters and enabled the FBI to close the case.

The Unit also made substantial contributions to the case of Mrs. Velvalee Dickinson, the proprietress of a doll shop in New York City, who was in 1943 convicted of espionage. Among the more amusing problems was a letter sent on 22 November 1943 by an anonymous citizen of Somerville, Massachusetts, to the "Department of Military Intelligence, Washington, D. C." The writer challenged the experts to decipher a message prepared in what proved to be a fairly simple system. The plain text was: "There comes a time in the life of every intelligent man when he realizes how dumb he is." See Tab 25.

About the first of August 1943 work began on the third function of the Special Examination Unit, the processing of radio-telephonic

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

conversations.[7] By 9 September 1943 the Unit had listened to 377 sides of these recordings, with about 200 more awaiting processing at that date, and 169 reports had been prepared. Each record required about 45 minutes merely to listen to one side, to say nothing of transcribing it on paper. Moreover, since many of these converaations were in foreign languages, personnel peculiarly qualified to listen had to be recruited. For this work Mr. Angus McCoy was assigned on loan by the Language Branch to the Special Examination Unit on 27 August 1943; he has since given his full time to the work. For about two months (December 1943 to February 1944) Mr. Henry Sauerwein worked on the German recordings, and other members of the German Unit helped out from time to time. Late in 1943 two small rooms were prepared as audition chambers. In the early period many technical difficulties were encountered. Different systems of recording were tried out with varying degrees of success, and unsatisfactory methods were discarded.

In July 1944 when Captain Vogel was sent on detached service, the direction of the Unit was turned over to Mrs. Dorothy K. Watson. The Special Examination Unit itself, which began as a part of B-I, had been, since the summer of 1943, one of the subsections of B-III. It was now incorporated for administrative purposes into the German Unit (B-III-d-1). The present activity consists almost exclusively of processing telephone conversations, but occasionally open-code problems are still being received.

---

7. The conversations occasionally took place in offices, hotel-rooms, and the like and were intercepted clandestinely.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XV. TRAFFIC IN COMMERCIAL CODES[1]

The mission of the Agency implies that some attention will be given commercial codes, which are intended chiefly to reduce costs of transmission. Their publication has been extensive: about 300 of them are now available in the files of the Signal Security Agency and presumably there are others not yet on hand.

A large volume of commercial traffic, transmitted by stations in countries over which the United Nations do not exercise full control, is worth processing since, even when the transactions discussed are not hostile to the interests of the Allies, information is found concerning the economic situation in enemy and occupied lands which is frequently of value to the Military Intelligence Service.

The processing of commercial traffic has been performed by two separate units, one successor to the other and composed of entirely different personnel. The history of the earlier unit, organized in February 1943, exhibits many changes in personnel and even more frequent changes in the officers in charge.[2] The initial task of the unit was the isolation of various types of commercial code traffic and the solution of the system indicators, if any, used in the messages. During

---

1. The statements in this section are based on interviews with Mrs. Marvin Prather, Miss Maude Devenney, Mr. William D. Coffee, and Captain Benson K. Buffham.

2. Captain William F. Edgerton was succeeded in May 1943 by Captain Franklin F. Russell. The original staff consisted of four civilians; by May two more had been added.

Doc ID: 6554247

TOP SECRET CREAM

this period the unit read and translated a few German and Spanish texts, but the great bulk of the traffic then being received (more than 91 per cent) was in English codes, in spite of the fact that it originated predominantly in Spanish-speaking countries. Another feature of the work was that from time to time bits of information derived from the commercial traffic would be coordinated with data available from other sources which would lead to solution in the crypt-analytic sections.

For a period of about three weeks in August 1943 the Officer in Charge was Lieutenant John C. Apollony, but when he left, the unit, which had up to this point been a part of the Romance Language Code Recovery Unit (then B-2-a, now B-3-a), was transferred to the Cipher Section.

From August to December 1943 the unit was successively in the charge of three different officers, each of whom spent most of his time with other units, so that the person actually directing operations was Miss Devenny.[3] The strength of the unit in this period, exclusive of the Officer in Charge, was reduced to about four, and by December 1943 so little commercial traffic was being received that the unit was disbanded, and the personnel transferred elsewhere.

After an interval of a few weeks during which nothing was done

---

3. These officers were Captain William S. Smith, next Lieutenant J. C. O'Neill, and finally Lieutenant Walter J. Fried.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

with commercial traffic, it was decided to set up a new unit with the same function but with entirely new personnel, all Negro civilians, including the supervisor. For administrative purposes only, this group was, however, placed under a white officer in charge.[4] The supervisor has, throughout the history of the unit, been Mr. William D. Coffee. Until 15 November 1944 the unit was officially attached to the Administrative offices of the old B Branch and later to the Intelligence Division; it is now B-III-b.

At first Mr. Coffee worked alone, but on 25 February 1944 Mrs. Annie H. Briggs became his assistant, and soon the unit had grown to a strength of 20.[5]

As the work began in January 1944 the greatest problem was to be found in the identification of the code used when the preamble contained no discriminant; but as time passed, it was discovered that of the 300 odd codes on file not more than about 15 were in current use. Procedure now begins with an examination of a new message in comparison with the tables of permutations printed in most of the codes. If the

4. In succession the following officers were in charge: Lieutenant John V. Frank, Lieutenant L. Clark Keating, Captain Francis E. Maloney, and, at present, Captain Benson K. Buffham.

5. Of these, Mr. Herman W. Phynes and Miss Naomi K. McElwaine engaged principally in an attempt to solve encipherments, and Miss Aubrey V. Fox, Mrs. Ethel H. Just, and Miss Eloise E. Daniels do the translating of messages in foreign languages. The others perform the operations of code identification, decoding, transcribing of the text of English messages, typing, and filing.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

first few groups are not to be found in the permutation table of a given code, that code may at once be eliminated from consideration. It is no longer necessary to test the message by actually looking up the groups in the code. Whenever this procedure fails to identify the code, then frequency studies are made of the letters appearing in the different positions of the group and compared with similar frequency studies of the various codes on hand. An elaborate cross-reference filing system has been instituted so that the information derived from previous messages may be immediately available to all personnel.

The mission of B-III-b, since its organization as a separate section of the General Cryptanalytic Branch, has been the exploitation of the commercial codes (all known as QAA) used by commercial houses of Australia, Great Britain, Spain, Portugal, Bulgaria, Turkey, Afghanistan, Russia, China, Indo-China, Thailand, Japan, Egypt, South Africa, and several countries of South America. Germany was included in this list until V-E Day, when all QAA traffic in and out of that country stopped. Of the traffic examined during the past year about ten per cent contained diplomatic and military information. Of the remainder about 40 per cent was sent to the Military Intelligence Service for forwarding to the Foreign Economic Administration.

Since 14 November 1944 the Commercial Traffic Section has had the additional assignment of sorting and routing all plain-text

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

traffic (QAZ), a task formerly performed by the Traffic Coordination Section. The traffic, which in a given month may range from 175,000 to 200,000 messages, is sorted into the following categories:

1. Commercial plain text (identified by the address or signature);
2. Plain text dealing with commercial matters but bearing a diplomatic heading;
3. Plain text in the Romance languages and German;
4. Plain text in other languages;
5. Diplomatic plain text;
6. Red Cross plain text (QGA);
7. Commercial Code traffic (QAA).

The languages of the Commercial traffic may be classified as follows:

English	75 per cent
French	10 per cent
German	10 per cent
Spanish	2 per cent approximately
Portuguese	2 per cent approximately

In April 1945 the government systems of four countries were transferred to the Commercial Traffic Section from B-III-a for exploitation. They are those of Belgium (BEA, BEB, BEC, BED, BEE, and BEZ), Haiti (HTA, HTB, and HTZ), Liberia (LBA, LBB, and LBZ), and Luxembourg (LUA and LUZ). Several of these diplomatic systems are now in research. The Section has had considerable success in solving such systems as BED and HTB, and has contributed much to the exploitation of JAH, a Japanese commercial system.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XVI. THE MACHINE CIPHER SECTION[1]

Until the spring of 1942 the Japanese diplomatic Red and Purple machines[2] were the only cipher machines studied by Army cryptanalysts.[3] In that year, however, lectures were given by Lieutenant (now Lieutenant Colonel) Frank B. Rowlett on the IT&T machine and on the Commercial Enigma machine. Captain (now Colonel)Solomon Kullback, upon his return from a visit to GCCS in the summer of 1942, gave lectures to a small group of experienced cryptanalysts on the German Abwehr Enigma (GEQ), German Military Enigma (GEU), and the German Teleprinter ciphers (GES, GET). Research and some work on solution was then done on GEQ.[4] Methods of solution for the Analin Fabrik Commercial Enigma traffic and the

---

1. The statements in this chapter are based on interviews with Major E. Dale Marston, Miss Gertrude Ullman, Mr. Alfred Hesse, and Miss Nancy McWhorter, and on the following documents: Cipher Teleprinter Regulations (SFV) for the Wehrmacht after 1 December 1942 (IL 4040); Major Roy D. Johnson, Cryptanalytic Report Number Two; German Permutation Cipher Teleprinter, Type 52b (IL 3883); A Method for the Solution of the GEQ Indicator System (IL 3296); William F. Friedman, Preliminary Historical Report on the Solution of the "B" Machine; An RAM Procedure for Placing Cribs in a De-Chi; A Statistical Method for Analyzing Certain Types of Flags Applicable to Tunny and Hagelin; Statistical Solution of Messages Enciphered by the Tunny Machine; Synopsis of Cryptanalytic Machines (IL 3988); SZD, A Swiss Machine Cipher (IL 3846). Discussion of Hagelin problems will be discussed in a later chapter.

2. On these machines, see chapter II. Also see volume IX.

3. The SIS had studied other machines but only in test messages.

4. By Lieutenant Herbert H. Maass and Sergeant Arthur Lewis.

Doc ID: 6554247

TOP SECRET CREAM

German Kryha machine were developed.[5] A portion of this traffic was subjected to solution and processed for translations.[6] At this time analysis of the Finnish Hagelin machine was in progress and a separate section was formed to handle all Hagelin problems.

In November 1942, when the cryptanalytic units then known as B Branch, were moved from Headquarters Building, Arlington Hall Station, to the new Operations A Building, there was only one section which concentrated on the cryptanalysis of machine ciphers other than the Hagelin machine. This section, directed by Lieutenant (now Major) E. Dale Marston, consisted of a small group who confined their activities to the solution and reading of messages enciphered by the Japanese Purple machine (JAA).[7] At this time, however, attempts were being made to intercept German Army and Air Force traffic, and it was decided that an intensive course in machine cryptanalysis should be given to a group of cryptanalysts who would ultimately be assigned to the German Enigma problem. The instructors were Mr. Ferner, Miss Grotjan, Mr. Small, Mr. Levine, Lieutenant Maass, Lieutenant Morris R. Collins, Sergeant Lewis, Mr. Maurice Waltz, and Sergeant Hyman. The students in this course, selected from the various units in the Cipher Section

---

5. By Miss Genevieve Grotjahn (Mrs. Feinstein), and Messrs Robert O. Ferner, Albert W. Small, and John Hyman.

6. By Mr. Jack Levine and Mr. Frank Lewis.

7. See chapter II, section C.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

(B-III), were given the instruction in two groups.[8]

After all students in the first group had completed the courses in Military Cryptanalysis, they studied some machine ciphers: Wheatstone, ITT, Commercial Enigma, Swiss (SZD), German Abwehr Enigma (GEQ), German Military Enigma (GEU), German Teleprinter ciphers (GES, GET), Japanese Red and Purple machines (JAA), Hebern machine, Hagelin machine, and the German Kryha (GEH). When Major Roy D. Johnson returned from England in April 1943, he gave a series of lectures on cryptanalytic procedures used at GCCS in connection with the German Military Enigma machine. Until his arrival, the Section was under the direction of Captain (now Major) John N. Seaman, Officer in Charge of the Cipher Section (B-III), and Mr. Robert O. Ferner, who were sent to GCCS in April to study procedures in Enigma cryptanalysis. Two identical electromechanical machines ("003") of great size and complexity were being installed in the basement of Operations B Building for this purpose. (Tab 28). These machines were officially turned over to B Branch on 16 October 1943.[9] Unfortunately,

8. The first group: Miss (now Lieutenant) Mary Charlotte Lane, Misses Betty Scherer, Jeanette Early, Marjorie MacLeod (Mrs. Max-Muller), Isabel Murdock, Sergeants Frederick McComas and Everett R. Dawson, and Lieutenant (now Major) William P. Bundy. The second group: Misses Gertrude Ullman, Nancy McWhorter, Alice Joys, Dr. Albert H. Carter, Lieutenant (now Major) Charles J. Donahue, Dr. Martin Joos, Dr. Ray W. Pettengill, Sergeant (now Lieutenant) Burrows Hunt, Mr. Alfred Hesse, Dr. Frederick Klemm, Dr. Robert Weidman, Dr. Karl Klitzke, Mrs. Hunt, Lieutenant Richard Hallock, Sergeant George Vergine, Sergeant Ernest Goldstein, Sergeant George Hurley, and Sergeant Daniel M. Dribin.

9. For further details and illustration of the 003, see volume IX.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

efforts to obtain traffic and procedure data for this project were entirely unsuccessful, so that use of the equipment has been confined to research and the solution of special jobs sent from GCCS. For further details, see chapter XVIII.

During the summer of 1943 a large number of personnel were assigned to the operation of the 003 to establish procedures for clerical personnel as soon as they could be procured. Maintenance of the 003 was undertaken by the Development Branch. In September 1943 two sections under Captain Marston were established to carry out these functions: B-III-c-4 (Operation and Control of the 003) under Lieutenant (now Captain) C. P. Collins; B-III-c-5 (Maintenance and Repair of the 003) under Lieutenant (now Captain) J. E. Bates. The cryptanalytic personnel were then returned to the Machine Cipher Section (B-III-c-2) for work on problems other than the German Military Enigma. During the summer cryptanalytic personnel of the Machine Cipher Section, except those assigned to the 003, concentrated on other cipher machine problems. Messages enciphered by the Swiss Enigma (SZD), which differs from the Military Enigma in that it has no endplate plugging, were currently read. Work on this system first began in December 1942, and the first translation was processed in July 1943. The stations using this system include: Bern, Washington, London, and Rome. The purpose of exploitation was not primarily the intelligence value of the decipherments but the maintenance of cryptanalytic continuity and the training of new personnel

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

in methods of Enigma cryptanalysis.

Also during the summer the German Abwehr (GEQ) Enigma was studied, but no solutions were obtained because of faulty intercept copies and out-of-date cribs. This Enigma machine differs from other German models in that it has no endplate plugging and from the Swiss Enigma in having a different wheel-turnover pattern. Each wheel has a number of notches which govern the turnover of adjacent wheels. The number of notches varies with each wheel so that the turnover is irregular.

At this time work was resumed on the Commercial Enigma machine, which has none of the complexities of the other Enigma types. Traffic between the Chemnyco Company in New York, which had been forced to close, and the Analin Fabrik, Ludwigshafen, Germany, was seized in New York by the FBI and forwarded to the Signal Security Agency for cryptanalysis.[10]

An extensive study of the German high-grade teleprinter cipher (GET) was initiated under Captain Maass. This system, called Tunny by the British, is entirely different from the Enigma machines. It involves a complex teleprinter machine using non-Morse transmission in the Baudot alphabet. As this traffic was not intercepted by the Signal Security Agency, material was sent from GCCS for research purposes. New methods of solution were devised and special emphasis was placed upon the

---

10. The remaining traffic on hand was read by Miss Gertrude Ullman, Miss Nancy McWhorter, Sergeant George Hurley, Mr. Alfred Hesse, and Lieutenant Richard Hallock.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the application of RAM[11] to this problem. A new method of flag analysis was developed for the solution of this traffic, and many technical reports were written on the basis of research conducted at the Signal Security Agency. In the autumn of 1943 all members of the Section were given training in this problem under the direction of Captain Maass and Sergeant Jack Levine. More advanced courses were planned, and new cryptanalytic attacks were tried out. The Dragon machine, (Tab 31) a mechanical means of sliding a crib against intermediate cipher text to determine [redacted] was constructed and delivered to GCCS in the autumn of 1944, where it has been used operationally with considerable success and has been the prototype of new machines. Concentrating principally on research, the Section was currently informed of operational procedures developed at GCCS by the American Liaison Officer stationed there. At that time, another machine (later known as the 5202) was designed for the purpose of setting certain other wheels (those not set by the Dragon machine) in Tunny machine problems. Certain units of the machine were designed to photograph data on specially prepared films, which were later subjected to a rapid comparison. The entire process was similar to the operation performed by the British machine known as the Colossus.

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

After Major Johnson left the Machine Cipher Section for GCCS,

11. See chapter XVIII.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Captain William S. Smith became head of B-III-c-2 for a short time. Captain Walter Fried then took over the Section until he was appointed Liaison Officer at GCCS. Captain Herbert Maass succeeded him until he too was ordered overseas in the autumn of 1944. Since then the Section has been directed by Mr. Alfred Hesse.

In the early spring of 1944, the space allotted to B-III-c-2 was taken over for the exhibition of B-III cryptanalytic activities. See Tabs 18 to 25. During the two weeks that the exhibition was in progress, members of the Machine Cipher Section were assigned to other sections. Miss Ullman, Miss McWhorter, and Miss Rosebro studied in the Hagelin Section. Mr. Alfred Hesse, Sergeant Goldstein, and Mrs. Max-Muller wrote a report on the solution of the GEQ indicator system and studied the German Teleprinter ciphers GES and GET. Mrs. Dora Ralph and Miss Virginia Roberts maintained current solution of SZD traffic, and the remainder of the Section analyzed the "19 Kana Nigori" (the machine-cipher system employed by the Japanese Army) for B-II. Solution was not possible at this time because of lack of sufficient traffic.

One of the contributions of the Machine Cipher Section has been the extensive analysis of the German Abwehr Enigma (CEQ, formerly called Orange). Attention was first directed to this system in July 1942 upon the return of Captain Kullback from England. Captain Kullback brought with him messages, cribs, and work sheets, and organized a class of 12 cryptanalysts to study this among other machine ciphers.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

No solution work was carried on by this group, but they in turn instructed others in the methods of Enigma cryptanalysis. Interest in the system was revived in the summer of 1943, when Major Johnson brought back additional material from England. A unit of four people (later expanded to nine) was formed to study the GEQ traffic on hand. Reference catalogs were compiled and processed by IBM, and statistical studies were made. Because of the faulty intercept copies and inadequate cribs, little progress was made on the actual solution of the system; but the work did provide excellent training for a large number of people, who later were able to solve the traffic currently. In October 1943 a complete list of keys was received from the British for the traffic of April to September 1943. The back traffic was then deciphered, and crib sheets were prepared and studied for the best points of attack. Work was concentrated on the "A" net (Berlin, Madrid, Bordeaux, Paris, Rome, Merano, Lake Garda, Lisbon), which had much the best coverage. About 60 per cent of the Berlin-Lisbon traffic was covered at this time. The unit, which had shrunk to two people (Lieutenant Hunt and Sergeant Goldstein), was increased to four by the addition of Mr. Alfred Hesse and Miss Betty Scherer on 2 November 1943. Miss Ullman and Miss McWhorter followed within a week. The first solution of current traffic was effected on 12 November 1943. From then on, with the improvement in interception and the training of additional personnel (the unit numbered 21 at its peak), key recovery progressed

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

to the point where 24 of the 31 daily keys for December were solved and messages were processed upon receipt. Methods of analysis using the 003 were developed for these messages so that very rapid solution was possible. The first "D" net (Berlin, Istanbul, Ankara) message was solved on 1 January 1944. On 15 January 1944 cryptographic changes were introduced into the system which prevented further key recovery with the methods in use. The unit was working on a new method of solution when new keys and a description of the changes which were already known in the unit arrived from the British. A method of solving the indicator system was devised,[12] and an elaborate catalog, consisting of an index of the development produced by the reflector and two adjacent wheels for all possible wheel motions, was compiled. The index, a new type of Eggs Catalog, was constructed by IBM methods. Attempts were made to record the data on IC plates and also on RAM tape, but IBM proved to be the most convenient medium. Solution, however, of the current messages was considered impractical because of inadequate interception and lack of cribs. But because the system was used on clandestine circuits which were covered by the United States Coast Guard, all cryptanalytic materials were turned over to the Coast Guard in June 1944 for further analysis.

When, during the spring of 1944, the use of the pluggable

12. See A Method for the Solution of the GEQ Indicator System, IL 3296.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

reflector threatened to become widespread in the Enigma communications of the German Army and Air Force (GEU), the Signal Security Agency was asked to assist GCCS in the hand recovery of the reflector and the endplate plugging by a method known as scritching. Traffic and cribs for this purpose were received from GCCS, and the efforts of the entire Cipher Section were devoted for several weeks to scritching. Many shortcuts and minor improvements on the procedures were developed; but the hand method of solution, impractical because of the time and number of high-grade personnel involved, was afterwards superseded by an electrical means of scritching developed in connection with the 003 to handle this problem. This machine, known as the Autoscritcher (Tab 30), was designed by members of the Research Group and the Machine Cipher Section and constructed by the Development Branch.

On several occasions the Section has contributed to cryptanalytic problems located outside of B-III-c. In the spring and summer of 1944 a small group, under the direction of Captain Herbert Maass and Mr. Samuel S. Snyder, undertook the cryptanalysis of JBH, a Japanese commercial system. Solution was accomplished with the cooperation of GCCS, and the messages were found to contain important economic information. The system proved to be a complex kana transposition and substitution with auto-key. In November 1944 the recovery was attempted of the current JEV (Japanese Army) conversion squares. Solution of the first set of squares was completed on 23 January 1945. At the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

same time other members of the Machine Cipher Section were assigned to the GEE (German one-time pad) system[13] in B-III-d. Cryptanalytic activities there were directed by Mr. Robert Ferner, Captain Walter Fried, and other members of the Research Group. After the nature of the machine which generated the additives was determined, the problem was returned to B-III-d for further exploitation. Problems relating to the security of our own communications have been analyzed from time to time by this group. Other systems which have been studied by the Machine Cipher Section during the winter 1944-45 are: GEV (German Military Attaché); GEX (Tokyo-Berlin German letter traffic); GEW (German Shanghai letter traffic); and FWA (French military B211).

Research of the GEV system was carried out by Miss Wilma J. Lambert and Miss Mary Neely Rosebro. From frequency distributions it was determined that an Enigma machine had been used in encipherment. Messages as far back as 1939 found to be in possible depth with current traffic indicated that no basic change in the machine had taken place since that time. Current cribs from Naval attaché systems were tested without success. Several attempts with the 003 were made, assuming the wheel wiring of the military Enigma. The exact nature of the machine (number of wheels, presence of endplate plugging, wheel break pattern) is not known. The six-letter indicator,

---

13. See chapter IV, section C, page 88. See also volume IX.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

as in the German Abwehr and Armistice Commission Enigmas, points to a setting of three wheels, but since no mention of the nature of the machine has been made in other German systems, no other proof has been found. Work on GEV was continued, and results of the research were sent to GCCS, where a section was organized to continue the work on this problem.

Analysis of GEX (Tokyo-Berlin German letter traffic) has progressed under the direction of Major Marston, Mr. Alfred Hesse, and Dr. Ray Pettengill; but only about 75 messages were received, and traffic ceased entirely at the end of December 1944. The nature of the machine has not yet been determined, but frequencies show that an Enigma machine is probably not involved. Several long messages have been tested statistically for Hagelin characteristics but without success.

The French military machine cipher, FWA, has been analyzed recently by members of B-III-c-2. It is a fractionating cipher and the basic machine is the Swedish Hagelin B-211, which was fully described by Colonels Rowlett, Kullback, and Sinkov in 1939, under the direction of Mr. William F. Friedman. The French, however, have further complicated the action of the machine by the addition of four wheels between the original fractionating device and the printing mechanism. The indicator system has been solved, but the wiring and exact function of the wheels are still unknown.

Traffic for 1943 and 1944 in the GEW system, letter traffic between the Berlin Foreign Office and the German Consulate in Shanghai,

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

was available for study. A cipher-text frequency was made on approximately 24,000 letters taken from messages after 12 July 1944. This distribution revealed that some type of Enigma machine had been used. Some compromised plain texts of messages were available, and although the corresponding cipher text was not on hand, cribs from these messages were tried on at least 18 cipher messages with no success. It was assumed that the wheel wiring was identical with that used in GEQ (German Abwehr Enigma) but several jobs were tried on the 003 without obtaining a solution. Some of the messages had sections of transposed plain text which were studied in the Machine Cipher Section. The traffic from Berlin was sent over clandestine channels and the intelligence was the same as that found in systems analyzed by the United States Coast Guard. Accordingly, work was abandoned on GEW at the Signal Security Agency and the traffic and work sheets were turned over to the Coast Guard.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XVII. THE HAGELIN SECTION[1]

No date for the establishment of the Hagelin Section (now B-III-c-3) can be given. At first this machine was studied in connection with exploratory work carried on by the Administrative Office of B Branch. Considerable time was given to the problem in the spring of 1942 by Lieutenant (later Major) John N. Seaman, who had been a member of the French Section, but, because of his knowledge of Swedish and Finnish, was directed in May 1942 to study the solution of the Hagelin C-38 and Finnish and Swedish plain-text messages. The state of Hagelin studies at this time was hardly more than that presented in a manual prepared by Captain (now Major) G. W. Morgan of GCCS on the Theory and Analysis of a Letter-Subtractor Machine.[2] Techniques

---

1. The name "Hagelin Section" relates to the fact that the cipher machine in question was invented, developed, and produced for commercial sale by the Swedish engineer, Boris C. W. Hagelin, of Stockholm. His original five-wheel model (C-36) was improved by him as a result of certain suggestions by the Signal Intelligence Service in its studies of the possibilities of the C-36 as a small cipher machine for field use. The Hagelin Model C-38 was the result. The United States Army Converter M-209 is a C-38 Hagelin machine without the "slide" and with certain other minor changes. The C-38 machine was sold by Hagelin to a number of governments, the Swedish, Finnish, Dutch, French, Italian, and Portuguese. Hagelin was not, however, successful in interesting the German or British Governments in his machine, although the Germans copied certain features of it in one of their later developments (C-41). See chapter XXI, page 303. Throughout this chapter the name "Hagelin Machine" will refer to the C-38 model. It must not be confused with another Hagelin machine, Model B-211, altogether different in nature. An extensive bibliography on Hagelin solution now exists: see appendix at end of this chapter.

2. SSA Document No. 13.

Doc ID: 6554247

subsequently developed in the Signal Security Agency show an enormous advance measurable both by the volume of Hagelin traffic solved and the publication of a number of technical studies.

Lieutenant Seaman began by making a careful study of the Swedish plain text, and to good advantage, for he was able to solve two Swedish messages by means of phrases common in the plain text and ship names, notably the probable word KOOKABURA. Mr. Robert O. Ferner had found these messages and the method of

[redacted] In order to solve the problem presented by this fact, Lieutenant (now Lieutenant Colonel) Frank B. Rowlett examined [redacted]

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

In this period work on the Hagelin problem was advanced by the assistance of a number of other persons,[3] but the group itself possessed

3. Captain (now Lieutenant Colonel) Perry Molstad, Lieutenant (now Major) Charles J. Donahue, Lieutenant (now Captain) Cyrus H. Gordon, Lieutenant (now Major) Stephen Dunwell, Lieutenant (now Lieutenant Colonel) James B. Greene, Mr. Robert O. Ferner, Mr. John Hyman, Miss Genevieve Grotjan (Mrs. Feinstein), and Sergeant Earl M. Ratser.

Doc ID: 6554247

TOP SECRET CREAM

only four persons regularly assigned to it.[4] When the Signal Intelligence Service moved to Arlington Hall Station in July 1942, there was a further increase. About this time a series of Swedish cipher tables was received, and to decryptograph a large body of accumulated traffic a number of clerks were added.[5] A method of extending the compromised Swedish tables to other circuits, based on relationships among them discovered by Captain Rowlett, was evolved.

The first entry into Finnish systems came in September. Only a single fragment of information about the Finnish use of the cryptograph was available,[6] but soon methods of solution were developed.

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

.....

[redacted]

4. Lieutenants Seaman, Donahue, and Gordon, and Captain Molstad.

5. Translations were made by Captain Molstad, Lieutenants Donahue and Gordon, and Dr. Martin Joos. Dr. A. H. Carter was assigned to the task of studying Finnish plain text in order to discover probable words, and to recognize and translate Finnish, should it ever be recovered.

6. This had been learned accidentally during a visit to the Signal Security Agency of Brigadier Tiltman of the British Army. He had used the term "finnery" in a totally different connection, and upon inquiry explained that the British had read a day or so of Finnish traffic and had labeled cyclic interruption there discovered "finnery."

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

On 17 December 1942, when Captain Seaman became Officer in Charge of the Cipher Section (B-III), Dr. A. H. Carter took over the leadership of the Hagelin Section, but continued to concentrate his efforts on the task of translation, for although experts in Finnish were now available,[8] cryptanalytic production, which was by January 1943 on a

---

7. New members of the Hagelin Section included Private (later Lieutenant) Burrowes Hunt, Miss Dudley Scovil (Mrs. Hunt), and Lieutenants Arnold I. Dumey and Walter J. Fried. Lieutenants Dumey and Fried had successfully analyzed the Hagelin machine while engaged in the practice of law.

8. Mr. John Kepke, one of the country's leading experts on Finno-Ugrian languages, and Dr. Reino Virtanen.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

current basis, outran linguistic production.[9] The first language study in Finnish was prepared about this time.[10]

By February the Hagelin Section had grown to some 50 people, and it was regarded as a training ground for machine cryptanalysis. On 12 February the first solution of a Hagelin cryptogram was accomplished.[11] The translation of volumes of correspondence, cryptographic materials, and records of all sorts in a very short time created a task of enormous proportions.

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

9. At this period Sergeant Vergine was in charge of statistical analysis, Lieutenants Dumey and Fried, Sergeant Goldstein, and Captain C. A. Rupp were in charge of research. Mr. (now Sergeant) Walter Jacobs was added to the staff in March 1943.

10. A "language study" in this sense is a statistical analysis, usually by IBM methods, of the frequencies of individual letters, groups of letters, and words in a representative sample of plain text.

11. In March Dr. Carter was transferred to the Research Group working on special problems and machine ciphers, and Lieutenant (now Major) William P. Bundy took charge.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

messages.[12]

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

Some of these solutions were achieved through adaptations and refinements of the

[redacted] was especially the work of Miss Oriole Gidlof, who worked out many methods for the speedy

12. At the time of the final negotiations between the two countries the Section was on a 24-hour basis, and several members were more than once summoned from bed.

TOP SECRET CREAM

Doc ID: 6554247

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

..... [redacted] As for the non-Hagelin systems,[13] Mr. (now Sergeant) Robert Brumbaugh, and Lieutenant Vilar Kelley solved the transposition system FIG. Dr. Reino Virtanen, Dr. Leslie Rutledge, Lieutenant Richard Hallock, and Dr. Carter were responsible for the entry into FIB. Dr. Virtanen, Captain Paavo Carlson, and Mr. Kepke are to be credited for their work on the running-key system. Reconstruction of the FIE system (substitution with disguised running key) is one of the landmarks in cryptanalytic history in B-III: the plain text was known but not the relationship of plain to cipher text. Once this was found after many tedious hours, it could be tested only by examining the resultant key, which had approximately the same frequency characteristics as English. This key in turn had to be anagrammed in such a way that fragments of English plain text appeared. From such a fragment "---isati---" it was believed that the key book was an English book published on the Continent: the spelling "(civil)isati(on)" was the clue. From such reconstructions the key book was located in a single day's search. When the key book changed and the supply of captured plain text was exhausted, by dint of sustained patience and effort two fragments of running key were reconstructed--a sequence of trigraphs and one of pentagraphs taken from the margin of a book by a route transposition--which made possible

13. The Hagelin Section also studied systems not using the C-38 machine because it had the personnel qualified to work in Finnish and Scandinavian languages, who were required for this work.

Doc ID: 6554247

TOP SECRET CREAM

the discovery of the key book after a search of five days in libraries in the New York area. The key book for FIF also gave an exciting chase. At one point, through an unfortunate slip in liaison, the Library of Congress actually requested it of the Finnish Legation! But it was found in the New York Public Library after a series of searches by several agencies here and abroad. Later, Dr. Virtanen inspected the libraries in the foremost Finnish-speaking communities in the United States, where he obtained[14] the key book used in the Buenos Aires version of the FIA systems.

Lieutenant Bundy was relieved by Lieutenant Fried in June 1943, and he by Lieutenant Dumey in December 1943. At about the same time, the exploitation of the Portuguese Hagelin (POV and POW) systems was undertaken, based on keys supplied by GCCS. In February 1944 the problem of the Netherlands Hagelin NEA system arose. The current solution of most of this traffic owes much to new techniques of aligning messages.

Among the major achievements of B-III-c-3, aside from the great production maintained in the Section, must be counted: recommendations to the Cryptographic Branch for the protection of our own systems,

---

14. Search in public libraries and Finnish book stores was unavailing, but Dr. Virtanen read in the files of a Finnish newspaper in New York that the publisher of the book (assumed but not known to be the key book desired) had donated copies of books to the library of a Finnish college in Michigan. Dr. Virtanen went to this college and found and surreptitiously appropriated the book, which proved to be the correct one.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the justification of warnings issued by the cryptanalysts after the reading of a message picked up by the Security Branch on a routine inspection of the Code Room of the Office of War Information, the several technical papers, and the interchange of technical information with GCCS and OP-20-G.

BIBLIOGRAPHY

FIA, FIF, and others. Second addendum (dated 29 January 1944) to Memorandum concerning Finnish traffic (dated 6 August 1943) covering events since 6 November 1943. [By Arnold I. Dumey and Albert Howard Carter.] 14 February 1944. IL 1201.

FIB. [Prepared by Willie J. Firestone.] 4 January 1945. IR 4097.

Final report on the FIB system. 8 July 1943. IL 1201.

Finnish language notes. [By John Kepke.] n.d.

First addendum (dated 6 November 1943) to Memorandums re Finnish traffic (dated 6 August 1943). [By Walter Fried.] IL 1201.

Hagelin report No. 2. January 1943. Compiled by Captain John N. Seaman, Sergeant [George] Vergine, and Miss [Dudley] Scovil [Mrs. B. Hunt]. IL 480.

Hagelin report No. 3. Statistical solution. Compiled by Sergeant [George] Vergine. n.d. Part II. A statistical approach to the Hagelin machine. [By Martin Joos.] n.d.

Hagelin report No. 4. The estimation of the key distribution. [By Walter Jacobs.] n.d. IL 751.

An insecure use of the Hagelin cryptograph leading to the discovery of messages in depth and the reconstruction of base settings—NEA. [By Arnold I. Dumey and Albert Howard Carter.] 20 November 1944.

Memorandum re Finnish traffic. [By Walter Fried. 6 August 1943.] IL 1201.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

[redacted] [By Arnold I. Dumey. 14 November 1944.]

The modified horizontal-vertical method. [By Walter Jacobs and Albert Howard Carter.] [30] May 1944. IL 3491.

Report on the solution of the Finnish 0000 and 17 systems. [By Leslie A. Rutledge.] 17 June 1943.

Report on solution of the Swedish Hagelin traffic [Hagelin report No. 1]. By Lieutenant John N. Seaman. n.d. IL 479-A.

The solution and analysis of the Hagelin letter-subtractor machine [By George Vergine and Albert Howard Carter.] [14 April] 1944.

Solution of FIE. [By Arnold I. Dumey.] n.d.

Solution of the Finnish transposition system (Rio de Janeiro-Helsinki circuit). [By Lieutenant Wilar F. Kelly and Private First Class Robert S. Brumbaugh. Ca 10 February 1944.] B 286.

Solution of FIR-2. [By Arnold I. Dumey. Ca 8 June 1944.]

[redacted] [By Arnold I. Dumey and Albert Howard Carter.] 31 March 1944.

The solution of the Netherlands Nagelin-enciphered traffic between Curacao and London (NEA). [By Arnold I. Dumey and Albert Howard Carter.] 3 March 1944.

Some NEA keys. [By Arnold I. Dumey and Albert Howard Carter.] 22 Ap. 1944.

[redacted] [By Jack Levine.] March 1944.

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XVIII. THE YELLOW PROJECT[1]

Knowledge of the German Enigma problem and some details of operational procedure were first brought to the United States by Captain (now Colonel) Abraham Sinkov and Lieutenant (now Lieutenant Colonel) Leo Rosen in the spring of 1941 when they returned from a study of the problem at GCCS.

The cryptanalysis of the German Army and Air Force traffic was first considered by the Signal Intelligence Service in the early spring of 1942. The methods of Enigma cryptanalysis used by the Navy (OP-20-G) and at GCCS had been examined, and it was decided to abandon the rotary type Bombe used at these centers in favor of a relay switching system which could be developed at the Bell Telephone Laboratories in New York. It was felt that research could be undertaken with more profitable results with this type of equipment. Accordingly, a meeting was held at the Bell Laboratories in New York on 30 September 1942.[2] The

---

1. The statements in this chapter are based on interviews with Mr. William F. Friedman, Lieutenant Colonel Frank B. Rowlett, Colonel Earle F. Cook, Major Lewis W. Gammell, Captain C. P. Collins, Major E. Dale Marston, Captain Joseph E. Bates, and Lieutenant Margaret Baker, and upon the following documents: The Arlington Dudbuster (IL 4099); Bell Laboratories Project File (Secret Switching System Project X68003); Contract File (SPSIF); File on the 003 in SPSIB-3; Semimonthly reports of B-III-c-4; Cryptanalytic report No. 2, by Major Roy D. Johnson.

2. Those present were Colonel Frank W. Bullock, then Officer in Charge of the Signal Intelligence Service; Captain Leo Rosen, now Chief, Equipment Branch, SSA, who was charged with the responsibility of the engineering on this problem; Mr. William F. Friedman, Director of Communications Research, SSA; Messrs Williams, Mertz and Stibitz, who originally designed the switching system, and Mr. A. B. Clarke, all of the Bell Laboratories.

Doc ID: 6554247

TOP SECRET CREAM

details of the cryptanalytic problem were presented by the representatives of the Signal Intelligence Service, and the discussions resulted in the decision to construct, at the Bell Laboratories, an experimental Enigma frame which would duplicate in effect the motion of a three-wheel Enigma machine with fixed reflector and pluggable end-plate. A letter of intent was sent to the Bell Laboratories on 16 October 1942 authorizing the expenditure of $30,000 for the construction of one Enigma frame to be known as Secret Project X68009. On 3 November plans were drawn up for the development of an electronic model. An engineering survey was made (X68007), but after the expenditure of $2,000 in experimentation, this project was abandoned because the time and cost involved did not warrant further development. The original experimental relay frame was completed and demonstrated to Mr. Friedman and Captain Rosen on 22 November 1942. Another successful demonstration was given on 9 December in the presence of Captain (now Lieutenant Colonel) Frank B. Rowlett, present Chief, General Cryptanalytic Branch, Signal Security Agency, then attached to the Office of Director of Communications Research, and Captain (now Major) L. W. Gammell, who, under Captain Rosen, was to be responsible for the maintenance and mechanical functions of the Bombe. Since the performance of X68009 was excellent, plans were made for the construction of a unit containing 144 frames and a recording apparatus, to be installed at the Signal Intelligence Service. Half of the frames were scheduled for completion by 1 April 1943 and the remainder by the following August.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Developments were made on the recording apparatus and other features. An A-1 priority was placed upon the construction of the first 72 frames, and the project was designated as X68003. On 5 February 1943 representatives of the British Government, Mr. Turing, and Major G. G. Stevens, then British Liaison Officer at the Signal Security Agency, were given a demonstration of the X68009. They were favorably impressed with the departure from the rotary bombe technique, which had been replaced by a new stepping apparatus controlled by switches.

During the early part of February steps were taken to obtain German Army and Air Force traffic and intercept data which were desperately needed for this project. A small amount of traffic was currently received from stations at Vint Hill Farms, Newfoundland, and Iceland, but, because of geographical location, they could never provide adequate intercept material. In addition to intercept data, information on cryptanalytic procedures was extremely important, if not vital, for efficient exploitation of the traffic. This information could be obtained only from GCCS, however, and Brigadier Tiltman had indicated that, for reasons of security, the British Government would be most unwilling to allow such information to leave England. Consequently, liaison concerning this matter had to be conducted on the highest level. A letter to the late Field Marshal Sir John Dill was prepared in February 1943 for the signature of General George C. Marshall, Chief of Staff, requesting all pertinent information needed for the exploitation of German Army and Air Force traffic by the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

United States Government. The reasons for the request were stated as follows:

1. In all probability the Signal Security Agency could make important contributions in respect to the type of machinery employed because of the new design, which gives greater flexibility; but only practical operation on actual traffic could establish this point.

2. It was desired to supplement British interception of this traffic in order that as complete coverage as possible of German cryptonets could be maintained.

3. American coverage of areas applicable to Allied operations in North Africa would release British intercept sets and personnel for other assignments pertinent to British rather than to American operations.

4. If the Germans should introduce a fourth wheel into the Army and Air Force Traffic, as they had done in the Naval Enigma, the Signal Security Agency would be in a position to assist materially in solution.

5. It was felt that actual operation of the relay bombe would afford the best training for cryptanalytic personnel, so that, in the event that American forces should operate in areas of primary interest to the United States, exploitation of the traffic might be carried on by the Signal Security Agency personnel without burdening GCCS.

6. Indications that the Japanese might adopt the Enigma machine had been noticed in Japanese Military Attache messages. If this should happen, the Signal Security Agency had to be in a position to solve the traffic.

7. It seemed wise to provide against the contingency of the wholesale destruction of equipment and specially qualified personnel in England, which at that time, shortly after the Battle of Britain, was entirely possible.

Whether this letter ever reached General Marshall or Sir John Dill is not known, but Mr. W. G. Welchman, in charge of Enigma operations at GCCS, came to the Signal Security Agency in April 1943 to

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

present the British point of view and to arrange a working plan of operation between the Signal Security Agency and GCCS on this problem. Agreement was reached on 17 May 1943.

During January 1943 personnel were selected from various sections of B Branch for special training on machine ciphers in preparation for Enigma cryptanalysis, as has been described in chapter XVI, page 235.

In April Major Roy D. Johnson, who had spent several months in the Engima Section of GCCS, returned to the Signal Security Agency to organize, under Lieutenant Colonel Rowlett, the Enigma Cryptanalytic Section here. Lectures on methods and procedures employed at GCCS were given to the personnel of the Machine Cipher Section (B-III-b), and its subsections were planned according to the British method of operation. None of these subsections functioned according to the original plan, except the Translation and Intelligence Unit under Captain (now Major) Charles Donahue, Dr. Ray W. Pettengill, and Dr. A. H. Carter, because sufficient traffic was never available for traffic analysis or cryptanalysis. Several attempts were made to expedite the interception of more traffic during the spring and summer of 1943 without success. Research on discriminants and unsuccessful attempts to isolate crib messages from the available traffic were carried on by Captain Roy D. Solomon and Mrs. Marjory Max-Muller; the remainder of the Section at that time concentrated on other problems, except for the Information Section, under Dr. Carter, which analyzed reports from intercept centers in order to direct

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

intercept activity towards particular cryptonets which would offer crib material. It was soon discovered that the system of allocating discriminants had changed since Major Johnson had studied it at GCCS and that the new system could not be accurately determined from the small amount of traffic at the Signal Security Agency. The few cribs on hand were out of date and could not be applied with any hope of success to current traffic. Jobs on current traffic were submitted to the bombe, and approximately 1000 machine hours were consumed without a single solution. Liaison with B Branch, which then was responsible for the traffic analysis, was conducted with Lieutenant Richard Farricker, who headed the group of traffic analysts assigned to this problem. When all attempts at cryptanalysis were abandoned in October 1943, the Section was disbanded and the personnel were assigned elsewhere. In August 1943 work on current traffic was temporarily abandoned until information regarding cribs and discriminants could be obtained from the British, or the interception of traffic greatly increased.

Installation of the Bombe 003 began 1 April 1943, but it was not until 1 June of that year that test jobs from B Branch could be submitted. These test jobs, actual menus received from the British, proved that considerably more work had to be done on the 003 before any operations could be considered. It was not until 23 July 1943 that the 003 was functioning with a degree of accuracy sufficient to warrant operational work. Enigma cryptanalysis at this time was

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

devoted primarily to research, and all activities connected with it were known as the Yellow Project. By arrangement with Commander Sir Edward Travis and Mr. Welchman, operational jobs were regularly sent to the Signal Security Agency from GCCS. Special communication channels were set up between the two centers to insure speedy exchange of jobs and solutions, and the section at the Signal Security Agency actually functioned as a subsection of the British unit.

Sections to handle these problems were organized so that the cryptanalytic group checking the runs were separated physically from the bombe operators and maintenance crew, because several Bell Telephone personnel were included in the latter group. Three control officers were selected to direct the activities of both groups.[3] After Major Johnson received orders to go to England, Lieutenant Morris Collins was put in charge of all Yellow operations until Major Marston could relieve him. Because of the shortage of clerical personnel, the delayed WAC program, and the security problem involved, it was necessary to assign highly trained cryptanalytic personnel, during the experimental period, to the jobs of turret operation and run checking so that they could train others at a later date.[4]

---

3. At the beginning of operations these officers were Lieutenants (now Captains) C. P. Collins, Robert Masenga, and Vilar Kelley.

4. The personnel then included Misses Gertrude Ullman, Betty Scherer, Jeannette Early, Elizabeth Page, Wilma J. Lambert, Nancy McWhorter, Mary Neely Rosebro, Margaret Smith, Evelyn Burch, Alma Earle Parker, and Marjory Max-Muller.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

The run-checking job consisted of examining all stops from the Bombe with a celluloid mask grille for contradictions in endplate plugging. If no contradiction occurred, the menu had to be further tested on a hand model (Tab 27) of the Enigma machine for a possible solution. Solutions were actually deciphered on a captured machine before the wheel setting and endplate plugging were sent to GCCS. This group developed rapid methods of checking and hand testing as well as methods for making menus, so that less highly trained personnel were able to take over the job later in November when they were made available to the Section. Operations in the turret room included plugging menus to the Bombe, adjusting wheel-setting keys, operating and adjusting the recording apparatus, and routing maintenance of the frames. This is now done largely by enlisted personnel.

In October 1943 Major Johnson left for England to head the Beechnut Project, and responsibility for the Yellow Project was assumed by Captain E. Dale Marston, effective 15 October 1943. Under him Captain J. E. Bates from the Development Branch took charge of the maintenance of the 003, which was completed and turned over to B Branch on 16 October 1943. Lieutenant Charles P. Collins headed the cryptanalytic group in charge of Bombe operations. The second set of 72 frames was completed on 2 October, and acceptance tests were conducted immediately afterwards, so that the entire unit was functioning on an operational basis by 16 October. Further attempts to work on current traffic were made after the receipt of a discriminant list from Colonel George Bicher

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

at ETOUSA and of information about the solution of the new discriminant allocation system. Traffic could then be sorted according to the various cryptonets, but the lack of cribs, together with the fact that the volume of traffic was decreasing, prevented success in solution. All work on current traffic, including interception of the traffic, was officially abandoned on 15 October 1943 and has not been resumed.

At this time, October 1943, successful tests were made on two attachments to the 003 (projects X68128 and X68129). The first of these attachments (known as "the machine gun" because of its noise) was designed to cut down the number of stops on a run by means of a mechanism which prevents the 003 from recording a stop when there are conflicts in the endplate plugging. Therefore, only the stops which must be hand tested are recorded. The other attachment allows two small related menus to be tested simultaneously (the double input method). The construction of these attachments brought the total cost of the 003 equipment to $944,101.10.

When only 72 frames were functioning, it was possible to handle an average of 10 jobs a week, which made necessary about 30 separate runs on the 003 to cover all possibilities of wheel turnover. After 16 October, when all 144 frames were operating, 12 menus could be handled every 24 hours, using only 75 per cent of the total capacity and leaving 36 frames for research activities. Actual operation time per job ranged from three to 36 hours. Jobs of high priority were processed with all possible speed, and in some cases answers were

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

cabled to GCCS within three hours of the receipt of the message at Arlington Hall Station. The time involved in the case of dud solutions was even less.

Early in September 1943 plans were made for the construction of a machine to solve messages for which all elements of the key except the setting of the wheels at the beginning of the encipherment are known. The first model of such a machine, the Dudbuster, consisted of 36 Enigma frames; this number, one-fourth of the 003 capacity, seriously hampered the production of regular jobs. Dud solution by this method was soon abandoned in favor of a single-frame model (Tab 29), which handled, from the date of its completion in October 1944 to 15 May 1945 when traffic ceased with the cessation of German military activities, an average of 10 dud messages each day. The record number of solutions in any one day was 12, and the maximum daily capacity for the machine was 30. In two cases solutions for high priority duds were sent to the British within one hour after the receipt of the message at Arlington Hall. Often as much as 10 per cent of the total daily traffic, or 40 per cent of the traffic on a single cryptonet, was intercepted with faulty or garbled indicators, and the Arlington Dudbuster was able to contribute to the solution of messages for which British personnel had neither the time nor the equipment to divert from regular solution.

In September 1944 a Dudbuster of a different type was developed. This new machine consisted of a specially designed camera connected to

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

an Enigma frame. The generatrices of high-frequency letters, with a given endplate plugging, generated by an Enigma frame, clip setting, and wheel order, were recorded on film. Films made of cipher texts were then compared, by RAM, with the generatrices, the largest number of coincidences indicating the correct stops.

In January 1944 half of the 003 frames were rewired to make possible the solution of messages enciphered with a new reflector which the Germans had introduced into some cryptonets. At the same time the British recommended that Enigma research be concentrated on three problems:

1. The quick solution of dud messages.
2. The solution of two-period cillies.[5]
3. The simultaneous recovery of endplate plugging and reflector wiring.[6]

Study of all of these problems was undertaken by the Research Group, and the sections concerned with the operation of the 003 (B-III-c-4 and B-III-c-5). The Arlington Dudbuster was the answer to the first problem. As for the second problem, a method was devised

---

5. A cilli occurs when the setting of a message part can be derived from the assumption that the operator has failed to move the wheels since the encipherment of the last message before enciphering the indicator of the next message part; if the wheel setting so derived is recognized by comparison with settings commonly used, deductions as to wheel order can be made and the setting used as an indicator crib.

6. In certain Army cryptonets the Germans had introduced a pluggable reflector on which the plugging changed every 10 days, so that regular Bombe methods of solution were impossible without prior recovery of the reflector wiring.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

for adapting the 003 to the analysis of two-period cillies. The British then sent all problems of this type to the Signal Security Agency for solution. The third problem, simultaneous recovery of two series of plugging, one at the endplate and another at the reflector, at first appeared invulnerable to machine attack. But cryptanalysts at GCCS, OP-20-G, and the Signal Security Agency have, after one year of experimentation, succeeded in finding three different answers to the problem. Hand solution was begun immediately on a large scale at GCCS. It was greatly feared, from the reading of messages dealing with code instructions, that the enemy would soon introduce the pluggable reflector into all cryptonets; therefore rapid methods of solution were badly needed. The Signal Security Agency was asked to assist in hand methods. About 20 persons were trained in this long tedious job which the British termed "scritching" and which the Americans called "Bingo". This method involved the assumption of one pairing in the endplate plugging and the examination by eye of the implications in the reflector for a series of constatations until a contradiction or confirmation was found. Fortunately, the enemy was slow in spreading the use of the pluggable reflector; hence the hand method could be abandoned in favor of the development of machine methods. Plans were drawn up and submitted to the Development Branch for a mechanical means of scritching; these resulted in the construction of the Arlington

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Autoscritcher.[7] First, experiments were made on the 003 by running all of the 144 frames in combination, using only two wires in each reflector. On the strength of this experiment the British constructed a machine similar in theory known as the "Giant." The Navy, working on a different theory, constructed a machine known as the "Duenna," which was successful in later Enigma operations. The Autoscritcher, constructed from 003 equipment by the Development Branch, accomplishes solution according to the same principles as hand scritching but does the job in a fraction of the time. It can test all possible constatations in a problem in about two weeks, depending on the length of the crib. This time is equivalent to that required by the Giant and, with a long crib, half that required by the Duenna; with a short crib the time might be twice that required by the Duenna. Preliminary tests were successful and actual operations began 25 December 1944.

For the most part, the unit working at the Yellow Project functioned as an operational subsection of GCCS, sharing the burden of routine Enigma Solution. From 23 July 1943 to 30 January 1945 the number of jobs received and solutions obtained were:

	Received	Solutions
Jobs	1,375	413
Cillies	71	21
Duds	714	499

7. The problem was outlined by Mr. Albert W. Small and Mr. Robert A. Ferner, and the Autoscritcher, the Army's answer to the problem, was designed by Captain C. R. Deeter and constructed by the engineers of the Development Branch.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Development of the Arlington Dudbuster and the Autoscritcher have been important contributions of the Signal Security Agency. A Superscritcher, suggested by members of the General Cryptanalytic Branch and designed and constructed by the Development Branch, was prepared to go into operation in the summer of 1945. This is an electronic machine, capable of accomplishing in 12 hours an amount of work that required two weeks on the Autoscritcher.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XIX. THE RAM SECTION

Rapid analytical machinery (RAM) was first developed for cryptanalytic purposes by the Navy (OP-20-G). The machinery was designed along general lines and not for specific problems. Thus, the application of existing machinery to actual problems was at first very limited, but it offered a wide field for research and development.

The term RAM, as used within the Signal Security Agency, is limited to high-speed cryptanalytic equipment using the photoelectric principle of evaluation, though it is not impossible that in future other techniques may be developed and then be included within the term. Included in this category are index of coincidence (IC) comparators, the Tetragraph Tester, the 70-mm Comparator, the 5202, and others. Each machine is constructed for certain specific types of tests: the IC will give an index of coincidence between two bodies of text 600 by 26 units maximum with a margin of error of approximately 1 per cent for all positions. The Tetratester will recognize coincidences of predetermined pattern between the messages for a length of 30 letters or the exact number of coincidences in any position of the 30 letters. The 70-mm Comparator will tabulate exactly the number of coincidences (monographic, digraphic, trigraphic, etc.) for two lengths of text up to 1,800 letters, or longer with modification, for all juxtapositions.

A request for this machinery was initiated by B Branch on 7 January 1943. Subsequent negotiations were carried on between the

Doc ID: 6554247

TOP SECRET CREAM

Equipment Branch (then called the Development Branch), which had recently been established, and the Bureau of Ships, Navy Department. Allotments of $100,000 and $77,000 were made to the Bureau of Ships for the purpose of buying RAM equipment. They in turn negotiated research contracts with the Eastman Kodak Company, the National Cash Register Company, the Grey Manufacturing Company, and the International Business Machines Company (IBM). Aside from the RAM, the contracts included certain other items: 6 additive machines, hand operated by the cryptanalyst; 20 robot heads for use in the Development Branch (solenoid banks for remote operation of Electromatic typewriters); Special IBM teletypewriter tape equipment used in connection with RAM.

The complete list of equipment on order and installed by February 1944 was:

1. From the IBM Company: 15 tape readers, 8 tape punches, 7 punch controls (SMFSA),[1] 1 copy machine (SFMSA), 7 regenerating units (SMFSA), and 20 robot heads.

2. From the Eastman Kodak Company: 1 Tetragraph Tester (including projector), 4 IC cameras, and 5 projectors.

3. From the National Cash Register Company: 6 additive machines, 1 70-mm Counter Printer, 1 70-mm Relay Control.

4. From the Grey Manufacturing Company: 1 70-mm Comparator, 2 70-mm punches.

---

1. A Navy term for "Special Machinery for Security Applications."

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

In January 1943 personnel were assigned to special study of RAM equipment. Lieutenants LeRoy Wheatly and William Moran studied the operation and maintenance of the machinery at Rochester, New York under the supervision of the experts at the Eastman Kodak Company. After the delivery of the IC equipment to the Signal Security Agency in July 1943, tests were made on it by using three sample messages from the text of Military Cryptanalysis, Part III. These tests were so successful that, as soon as the personnel became familiar with the operation and theory of the machinery, actual operations were begun 7 July 1943 on Swedish diplomatic Hagelin (SWA) messages. Following that, 124 messages enciphered by the German clandestine Enigma machine (the GEQ system) were compared for coincidences. Special projects for the Equipment Branch for the security of our own communications were also accomplished.

During the summer and autumn of 1943 the RAM Section (then designated B-III-c-1), under Captain E. Dale Marston, included Lieutenant William Sprengle, assisted by 2 enlisted men, 1 enlisted woman, and 14 civilians.

Among the early operational work was an IC count of sample messages submitted to test the security of some American machines, a project that would have taken at least a month by hand methods but which required only two days by RAM. The IC machinery was also used for a study of Japanese meteorological systems by RAM. But on 19 November

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

1943, when the Tetragraph Tester was in operation, the comparison of Japanese meteorological systems was transferred to this equipment. In January 1944 a method was devised to determine the dimensions of a transposition matrix by means of the Tetragraph Tester. The regular jobs done by the RAM Section at this time included pattern searches of JBD (Japanese diplomatic), overlapping of FIR (Finnish) messages, which involved 1800 separate comparisons at all possible positions of each message, and the comparison of JAM (Japanese diplomatic) messages to establish overlaps. To speed up this job one IC projector was remodeled to handle film in place of the glass plates. On 10 November 1943 the first Tetragraph Tester projector and camera were delivered. The IC Projector had measured only the index of coincidence, was hand-operated, and was capable of testing only two messages at a time; but the Tetragraph Tester could search for patterns of any complexity up to 30 positions, was motor-driven, and could compare 40,000 characters in a single position. This was possible because the Tetragraph Tester used 35-mm film rather than plates.

At the same time as the Tetragraph Tester, another piece of RAM equipment, capable of extremely high-speed coincidence counting, was developed and put into operational use. This was the 70-mm Comparator, capable of performing any task in which counting coincidences was necessary and of recording in written form the results of coincidence tests. It was with this unit that the first electronic

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

counter was successfully used. Its weak points were that only 10 characters could be examined at one time, and the difficulty of producing 70-mm punched tape.

The theory of multiple exposures, or the comparison of more than one character at a time, was explored and was applied to a new Tetragraph Tester camera. This proved to be one of the most valuable modifications of RAM equipment because it made possible the comparison of long stretches of key with many variants and the search for repetitions in text using the same key. This modification made possible the first of a long series of successes with Japanese Army problems.

On 14 September 1944 a new Tetragraph Tester camera incorporating many changes in design, including the use of lucite rods, was delivered. At this time an IC Film Projector equipped with an electronic counter to count coincidences was also received. With this equipment the subsection developed methods for solving enciphered messages with the same transposition key of the IC film projector. Techniques for comparing partially recovered lines of enciphering squares for contradictions and confirmations and for comparing long stretches of key with variants with cipher or plain text were developed in a search for repetitions.

With the arrival of the multiple-exposure Tetragraph Tester camera, searches could be made for repetitions within key with variant possibilities. Such a search was first successfully accomplished on

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

JEP (Japanese Army) messages. The RAM Subsection devised methods of using film projectors to search long stretches of cipher text for cribs for which there were multiple possibilities on coincidence and successfully applied them to JEQ and JEM (Japanese Army) traffic.

Upon the arrival of the 70-mm Comparator unit, work was begun on the setting of the patterns of the cyclic wheels in GET (German teletypewriter cipher) messages. This was possible with only a small modification of the equipment and proved that high-speed electronic counting could be done with little difficulty. At this time a 70-mm tape 108 feet long was used operationally for the first time. The tape was over four times as long as that originally designed.

The Index of Coincidence Plate Projector was modified so that it could utilize the film produced by the camera of the Tetragraph Tester. This was accomplished by changing the plate gate of the (IC) projector and substituting double film gates in which as many films as desired could be inserted at one time. A motor-driven version of this modification is planned for the future.[2]

A further development along this line, the 5202 (Tabs 32,33), when tested, was taken to England and installed. Three characteristics set

---

2. On 15 May 1944 Lieutenant Robert Masenga took charge of the Section, replacing Lieutenant Wheatley. The Section continued to expand, and in October it was decided that additions would be limited to enlisted women. On 15 February 1945 Lieutenant George Dixon, a radar and electronics engineer, was added to the staff.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

it apart from other IC machines: it can scan a large body of text (40,000 elements), it can compare two different sets of textual data simultaneously and can thus make use of principles of positive and negative weighting, and it can count the coincidences at specified positions with almost 100 per cent accuracy. Accordingly, though it was designed for a specific cryptanalytic problem it is a general cryptanalytic tool which can be adapted to the solution of many types of ciphers. This machine is a landmark in RAM development.

Another machine, the Dragon, used in the solution of the German teletypewriter cipher, was constructed by the Equipment Branch with the advice of the Subsection. In the autumn of 1944 it too was delivered to GCCS, and it has been used successfully in operations at GCCS since that time.

More recently, RAM proved useful at a time of crisis in the solution of JAA (Japanese diplomatic Purple machine) messages. When, in March 1945, far-reaching changes took place in Japanese cryptography, new machine methods were needed to maintain the important flow of Purple intelligence. An IBM card reproducer was connected in record time to the analog of the Purple machine constructed in the Signal Security Agency, and the reproduction on cards of the entire development of the Purple machine was completed in one day. Thus, the testing of all starting points with a crib for JAA messages in 15 minutes was for the first time possible, whereas hand testing had formerly

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

required about a week. During one two-week period some 50 messages were read by the application of 150 cribs.

Another significant development in the application of RAM was the recovery of the JAS Conversion Square No. 28 in the J-period. This analysis, done on the 70-mm Comparator, provided overlaps which made possible the reconstruction of segments of the square. The limitations of Square No. 28 were ascertained through the juxtaposition of the cipher text of a number of messages and the plain text known to underlie them recovered from messages of the readable I period. The study of these messages by RAM provided a means of attack on Square No. 28 as well as on the indicator keys of the J-period key book.

RAM is at the service of all the sections of the Branch and of other branches with suitable problems. It has not only saved untold hours of work and made feasible projects that otherwise would have been too costly in time, but it has also eliminated the inescapable inaccuracies that void much of the work done by hand. The flexibility of RAM appears in the variety of systems it has analyzed: polyalphabetic substitution, additive encipherment, encipherment with running key and random cipher square, machine ciphers, and unknown systems.

RAM and accessory equipment in use at the Signal Security Agency on 15 March 1945 included the following: IBM letter writing (teletypewriter tape) equipment: 20 readers, 9 punches, 5 punch

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

controls (digit), 2 regeneration machines (32-character), and 5 regeneration machines (standard); 70-mm equipment: 2 comparators, 2 control units, and 2 counting and printing units (each counting unit containing 5 counters); 35-mm film equipment: 2 Tetragraph Tester projectors, 3 IC film projectors, 2 Tetragraph Tester cameras, and 1 special camera (with lucite rods); IC plate equipment: 3 IC plate cameras, and 2 IC plate projectors.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XX. THE TECHNICAL STAFFS AND SERVICE UNITS

The General Cryptanalytic Branch has included in its organization for a large part of the duration of the War a number of small units which are not assigned to the task of cryptanalyzing the traffic of specific countries and types of communication, but which perform a variety of services which are used by most, if not all, of the operating sections of the Branch. These units range in character from the Research Section, which provides expert cryptanalysts for the most difficult problems encountered by the operating sections, to the Document Section, the duty of which is to catalog, distribute, and account for all documents belonging to the Branch. In the present chapter the story of each of these units will be presented in turn.

A. The Research Section

The Research Section was organized on 1 July 1943, with Mr. Albert W. Small serving as acting head until Mr. Robert O. Ferner's return from England. The original personnel of this Section (Mr. Small, Mrs. Genevieve G. Feinstein, Mr. Martin Joos, and Sergeant Walter Jacobs) were all research specialists of the Cipher Machine Section and had indeed had experience with many, if not all, of the systems studied in B-III. These four cryptanalysts had given assistance in the study of the SIGCUM cipher teletypewriter and after a month's study had been able to increase the security of the machine. Upon the conclusion of this special assignment, it was decided to maintain the group to handle other special problems and to assist

Doc ID: 6554247

TOP SECRET CREAM

and advise the operating sections of the Branch on new problems, difficult and time-consuming for the operating sections. From the beginning the policy of the Research Section has been to rotate personnel. New personnel were brought in from time to time and others were on indefinite loan to the operating sections where need for them existed. Thus, specialists in various phases of the work of the Branch were brought together to foster an exchange of ideas and to engage in profitable study. They maintained constant close contact with operations and, for the most part, concentrated on operational activities.

In addition, constant informal liaison was carried on with the Cryptographic Materiel Branch and the Equipment Branch. Members of the Section were consulted regarding the security of systems, including ciphony and cifax. One of the early members of the Section, Dr. Martin Joos, was eventually transferred to F Branch to continue his specialized research.

The personnel for the Section was chosen originally to concentrate on cipher-machine analysis (Mrs. Feinstein; Dr. Joos; Sergeants Dribin, Levine, and Jacobs; and later Dr. Getchell, and Mr. Lipsky). Soon, however, specialists in various other fields, for example, transposition and additive, were brought in (Mr. Bryan, Mrs. Siegel, and Mr. Snyder).

The principal contributions of the Section lay in solutions, advancement of cryptanalytics, especially in the field of machine-cipher analysis, and recommendations for new cryptographic machinery

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

and cryptanalytic mechanized procedures. The activities of the group ranged from the analysis of machines used by the United States to cryptanalytic attacks on high-grade German and Japanese machine-cipher systems.

The lessons learned from attacks upon enemy systems have been applied to the analysis of our own systems in order to increase their security, as in the case of the M-228, M-325, and M-409 machines. As for the M-228, it was recommended, even after improvements had been made by the Research staff, that the device be abandoned for secret communications since it was possible to read any two messages enciphered with the same indicators without any knowledge of the key-generating unit. Pluggable endplates were suggested for the M-325 and M-409, and the vulnerability of machines without such pluggings was demonstrated. A further protection was obtained by the incorporation of additional notches to the rotors, so that all rotors must step more often, eliminating the possibility of solving the rotors one at a time. To the M-409 a second continuously moving wheel was added, which prevented solution even with the use of a long plain-text crib. Moreover, a new type of circuit known as the "reflexing circuit" was designed to repeat a variable number of times the encipherment of individual letters. In conjunction with the Security Division and OP-20-G, the group, after extensive study of a certain combined-operations cipher machine, was able to improve its security by changing the indicator system.

Important contributions in a different field may be noted in the

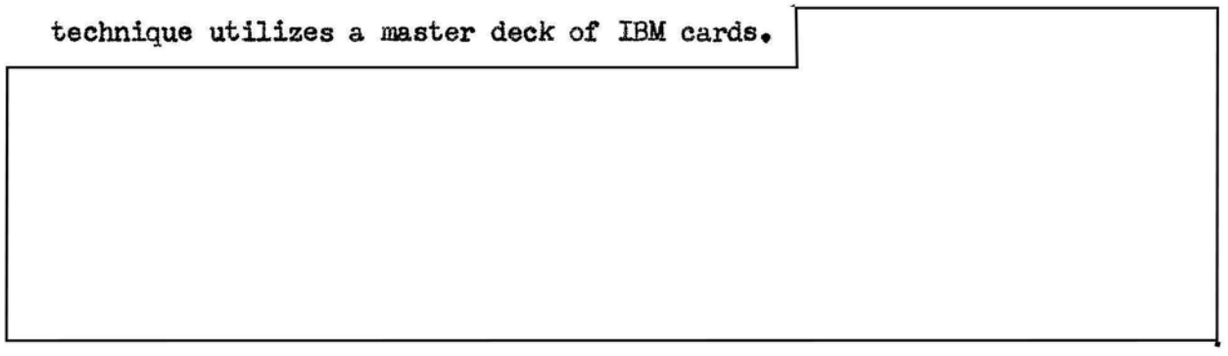
TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

original solutions of certain Japanese diplomatic enciphered code systems. JBA, a transposition system of a degree of security second only to the Purple machine-cipher system (JAA), was solved by statistical methods within six weeks. This solution is believed to be the first instance of the recovery of an unknown transposition of an unknown code by purely statistical means. Beginning groups, and later, code groups within the body of the text were found by matching stretches of cipher text from several messages with the same indicator. Frequent digraphs were recorded, and eventually the transposition patterns and tetragraphic code groups were recovered despite the presence of occasional trigraphic groups, the use of blanks in the matrix, and the use of the letters of the signature as nulls throughout the message.

The Research Section also made contributions to the theory of additive recovery. Studies of the problems of additive recovery led to the development of new techniques, especially statistical approaches to the determination of relative probability involving logarithmic weighting. In addition, the group proposed designs for RAM equipment to effect additive recovery on purely statistical bases. One technique utilizes a master deck of IBM cards.



TOP SECRET CREAM

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

Doc ID: 6554247

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

This method has been successfully applied to several of the Japanese diplomatic systems and has contributed to the exploitation of the JE group of Japanese Army codes.

In the field of enemy machine ciphers the staff has also made contributions, especially in designs for cryptanalytic machinery, such as the Autoscritcher and the 5202, designed to overcome many of the obstacles to solution of such machine ciphers as the Enigma and the teletypewriter systems. The captured Japanese Army Green Machine was examined and analyzed jointly by the Military Cryptanalytic Branch and the Research staff of the General Cryptanalytic Branch. Confronted with the problems of a general solution, they were able to devise a hand method and an IBM method as well as a relay device for the process of solution. In connection with the study of the Green Machine, the principle of the setting rotor was discovered; this principle in addition to providing a comparatively rapid method of solution for the Green Machine, was applicable also to the Purple Machine problem and is expected to provide a much speedier method of solution than the present one. Moreover, the group prepared instructional materials used in courses designed to prepare cryptanalysts against the possibility that the Japanese might use the machine even though it had been captured. In another Japanese military field "The Mathematical Theory

Doc ID: 6554247

TOP SECRET CREAM

of Related Cipher Alphabets," a research paper prepared by Sergeant Jacobs primarily to clarify the analysis of cipher machines with Hebern-type rotors, was unexpectedly applied successfully to the recovery of a basic square used in a Japanese Army double additive encipherment system.

One of the most important problems studied by the Research Section was GEE, the German one-time pad system. After the initial break into the system by the German Diplomatic Section (B-III-d-1), the entire Research staff was assigned for some months to assist in the exploitation of the system and to speed the reconstruction and the reading of the pads. Their assistance made it possible to supply a great amount of useful intelligence before V-E Day as well as afterwards.

Thus, through their original solutions, their recommendations for more effective procedures, their inventions of accurate and time-saving cryptanalytic machines, and their specialized training courses, the Research staff made available a great amount of intelligence from many different sources. Working together as a group, the Section has advanced the science of cryptanalytics and increased the security of our own systems.

B. The Recorder's Group

On 12 August 1943 a committee of the General Cryptanalytic Branch recommended the establishment of the Recorder's Group for the purpose of composing and publishing technical papers dealing with cryptanalysis and various other activities. During the two years of its existence,

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the group expanded in number from one to ten. Dr. Albert Howard Carter, who was in charge of the group from the beginning, conceived the need of permanent records of the valuable cryptanalytic work of the General Cryptanalytic Branch for present and future use.

The Group prepared many kinds of papers. The first category describes the nature of the traffic in various cryptographic systems, the history and methods of the cryptanalysis of the systems, their cryptanalytic relations with other systems, and the cryptanalytic and cryptographic materials necessary to their solution. Papers have been written describing 50 such systems. To a second category belong technical papers dealing with the theory and application of cryptanalytic methods. They are theoretical contributions to cryptanalytics rather than descriptions of specific aspects of the cryptanalysis of a particular system. Since the organization of the group, 12 of these have been printed and several more prepared in typescript. A third category includes miscellaneous writings, such as surveys, summaries of cryptanalytic work done, progress reports, indexes, staff studies, and other such reports for which a need arises in the administration, operation, or liaison of B-III. The progress reports include the Daily Information Bulletin (published since 5 September 1944), which contains a summary of news from all sections of the Branch. This bulletin covers mainly cryptanalytic data, but also intelligence which keeps higher authority and operating sections promptly informed of important developments. The Semimonthly Report

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

comments on the progress of solution and the administrative problems of the Branch. The Annual Report for the Fiscal Year relates to the achievements of B-III and forms the basis of that part of the Summary Annual Report of the Army Security Agency dealing with general cryptanalytic problems. The Branch history presents a report of the achievements and policies of B-III.

In general, such papers were prepared by the Recorder's Group as permanent records of the achievements and failures of the Signal Security Agency. They were sent to the cryptanalysts in the various sections and branches of the Agency for their information and use, to the Navy for the furtherance of their work, to our Allies, and to the Vault for preservation. In the writing of these papers, accuracy, completeness, and clarity, including the use of standard nomenclature, have been the goals.

The Recorder's Group has also been responsible for recording the proceedings of the Committee on Terminology. The preparation of a prescriptive glossary, necessitating constant research in the literature of cryptology and personal contact with key members of the Signal Security Agency and other centers, has also been part of the contributions of the Recorder's Group. One tentative edition of approximately 234 copies has been published by the Post Committee on Terminology. This manual contains definitions of terms dealing with signal security and intelligence. At the request of the Office of the

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Director of Military Training, Army Service Forces, the Committee on Terminology during the past year was engaged in the preparation of a change to A Dictionary of United States Army Terms (TM 20-205) to deal with all terms falling within the province of the Signal Security Agency. In addition, the Recorder appointed the Signal Security Agency member of the working committee of the Army-Navy Communications Intelligence Coordinating Committee on the preparation of a dictionary of cryptographic terms.

Another work of the Recorder's Group is that dealing with the liaison reports between the Signal Security Agency and GCCS and other cooperating centers. These reports have been fully studied and indexed. In 1945, as directed by the Commanding General for his information, a monthly report was prepared on the Status of Liaison between the Signal Security Agency and the London Offices of GCCS.

Through this group a high level of consistency has been maintained in the written production of the Branch and an important body of cryptanalytic literature has been compiled.

C. The Planning and Priorities Unit[1]

The small unit now known as the Planning and Priorities Unit of the General Cryptanalytic Branch came into formal existence on 31 August 1944 but was an outgrowth of an earlier unit known as the

---

1. Statements made in this section are based chiefly on interviews with Captains Francis E. Maloney and Benson K. Buffham, and with Miss Margaret Hancock and Mrs. Nelle Smithson.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Contol Unit of B-III, of which Lieutenant (now Captain) Francis E. Maloney was the Officer in Charge. Lieutenant Maloney also served as Traffic and Systems Coordinator as well as the Executive Officer of B-III. He had one civilian assistant for this work. In October 1944 he was succeeded by Lieutenant (now Captain) Benson K. Buffham.

The principal contribution of the Planning and Priorities Unit has been the daily dissemination of information, usually concerning the description of systems, to the several cryptanalytic units, together with continuous research into the nature of new traffic for the purpose of allocating responsibility and of routing. Its services have covered a wide range of activity from routine affairs to its special projects: contact with cryptanalytic units, liaison with GCCS and EU, assignment of priority to systems, assignment of short titles, maintenance of the list of short titles, and compilation of the System Identification Book.

Constant contact with the cryptanalytic units was maintained in order to find out what intelligence may be of value to them and to bring to the attention of all units any operations performed elsewhere which might help them increase their efficiency. Material collected and sent to the Communications Branch has constituted an important contribution. This work involves informing the Records and Distribution Unit of the external characteristics of systems and the circuits over which they travel and checking the work of the Records and Distribution Unit on this

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

phase of traffic processing. The Planning and Priorities Unit studied all mistakes in routing or identification to determine the probable cause for the error in order to avoid similar mistakes in the future. A report on the relative coverage of traffic sources over point-to-point circuits was submitted monthly to the Military Traffic Analysis Branch.

Exchange of information with GCCS and EU was another profitable phase of the work of the Unit. Requests were prepared by this office both for traffic desired by B-III units and for specific information not of a technical cryptanalytic nature but necessary to the performance of services. Information in response to requests from GCCS and EU was collected from the cryptanalytic sections of B-III and forwarded.

General supervision of the distribution and indexing of traffic in B-III has been another responsibility of the Planning and Priorities Unit, which also assigned priority to intercepted traffic. Such factors as the overall priority of the traffic of a given government, the readability and intelligence value of the system, and the need for speed in handling were examined to provide a basis for the assignment of the priority. Thus, during the San Francisco Conference, the Unit established temporary priorities for the 24-hour working day of some of the units. Further, a month-by-month evaluation of the relative priority of all diplomatic systems has been maintained together with a list showing current priorities of the systems.

A number of miscellaneous services were also performed by this

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

Unit during the past year. One copy of cryptographic information messages concerning all systems except those of the Japanese Army was filed and one copy of all messages dealing with radio communications was sent to the Communications Branch. Radio service messages were examined and the information contained placed at the disposal of the various cryptanalytic units of the Branch.

A special project was the assignment of short titles in the form of trigraphic designations to systems and the preparation and maintenance of a list of short titles for all foreign cryptographic systems except those of the Japanese Army. The list is arranged systematically by short title; two annual lists have been published to date, the first appearing in February 1944 and the most recent in January 1945. The task of compiling this list involved determining the existence of new traffic, assigning new short titles to the traffic, and collecting as much data on each system, together with a sample message, as necessary to make identification possible.

The System Identification Book is a permanent record in convenient form of all types of traffic received in B-III. Containing data used in identifying more than 500 systems, it is arranged alphabetically according to short titles. Material was compiled from study of traffic to determine the identifying characteristics of each system, such as the preamble, call signs, signature, indicators, and the circuits used; sample messages were included for each system.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

D. Documents Section

A rapid accumulation of documentary material concerned mainly with the activities of the representatives of the Signal Security Agency at GCCS, needing immediate methods of identification, prompted the Administrative Office of B-III to create a separate unit for this purpose. In November 1943 Mrs. Julia Martin began setting up a system for indexing and cross-indexing this material. The necessity for routing, accounting for, and expediting such records to the sections of B-III for their information, as well as to other outside branches, made the main purpose of the Documents Section that of identification. Registration of these documents was a laborious assignment, involving a backlog of as many as 58 reports from the American Liaison Officer in GCCS. Well over 7000 cards comprise the files of the liaison reports. Continuous dissemination of material required an elaborate system of handling and checking, so that a record of those signed out to any person in the Branch could be seen at a glance.

E. The Decryptographing Unit[2]

From September 1942 to September 1943, a Decryptographing Unit (B-I-c) contributed to the operations of the Branch. Its function was the decryptographing of all messages sent in systems not involving further cryptanalytic work. Such systems were of three types:

---

2. The statements made in this section are based upon interviews with Miss Katharine L. Swift, Mrs. Betty Moulton Leonard, and Mrs. Olive Mickle, a diary kept by Miss Swift from 16 October 1942 to the present, and a report by Lieutenant James C. Taylor on the personnel of this Unit (11 November 1942).

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

compromised, completely solved, and reconstructed to a point where translations could be prepared with little or no cryptanalysis, although some of the codes required additional recovery. The Unit was organized to relieve the cryptanalytic units of purely mechanical tasks.

For a time Mrs. Jean Reischauer was the supervisor, but by 11 November 1942 Lieutenant James C. Taylor had become Officer in Charge. The latter continued in this post until just before the abandonment of the Unit in 1943, when Captain Carlisle C. Taylor succeeded him temporarily. On 11 November 1942 the 26 civilians and 3 enlisted men under Lieutenant Taylor processed four Japanese systems, three weather systems, four systems using Spanish, and four using French.

As time went on the Unit tended to specialize more and more until it was divided into a French group, a Spanish group, and a Japanese group.[3] The Japanese group, under the direction of Mrs. Evalyn McGee, processed traffic in JAE, JAI, JAH, JAJ, and JAK. The premium on a knowledge of Japanese prevented the assignment to this group of any person who could read the message decoded.

The French group, which at first included only Mrs. Helen Siegel and Mrs. Ruth Cherniss, was expanded on 16 October 1942 by the addition of Miss Katharine L. Swift, who, after December 1942, was the supervisor and continued to supervise French decoding even after her group

3. No group, apparently, was formed for weather traffic, which had ceased to be processed in this Unit before the specialization.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

was absorbed on 21 September 1943 by the French Section (B-III-d). Two French systems (FBT and FBU) and, by September 1943, eight others (FAC, FAD, FAE, FAG, FAH, FAM, FAN, and FAV) were processed. Unlike the Japanese group, the French group was laregly able to read the traffic. Moreover, in this unit certain features of encipherment and some previously unidentified code groups were recovered, so that in actual practice the French group accomplished somewhat more than its assignment. In the spring of 1943 when traffic in one Italian system (ITD) was heavy, this unit assisted the Italian Section in decoding the messages.

The supervisor of the Spanish group was Miss Betty Moulton (Mrs. Leonard). Most of the group could read Spanish, with consequent profit to the work. Systems processed by this group included the following: ARB, CLA, CUA, MXA, MXB, SPB, and VZA. Toward the end of their work, the unit worked on some of the Portuguese systems also.

Because the cryptanalytic units were deprived of data made available by exploitation and the decryptographers were deprived of cryptanalytic aid, the Decryptographing Unit was abandoned and its personnel and functions were reassigned to the respective language units.

TOP SECRET CREAM

Doc ID: 6554247

CHAPTER XXI. ASSISTANCE FROM ESPIONAGE

Before leaving the subject of the cryptanalytic activities of the General Cryptanalytic Branch and passing on (in volume III) to the story of similar activities on a specific class of systems, namely, those of the Japanese Army, it will be well to consider one phase of the work which in the preceding chapters has been mentioned briefly on some occasions but not discussed adequately. This was the assistance given to cryptanalysts by the efforts of espionage agents assigned to the task of obtaining information concerning foreign cryptographic systems.

As will shortly be made clear, much information of this type was received by the Signal Security Agency and was, in most cases, highly valuable in cryptanalytic operations. The reader of the foregoing chapters will have been impressed by the fact that, given the modern techniques of cryptanalysis, it appears to be possible to solve even the most secure cryptographic systems purely as the result of cryptanalysis. An illuminating example of this kind is provided by the solution of the Japanese Purple Machine described above in chapter II, an instance in which no compromised material was received.

Though it may be theoretically possible to solve any type of system without assistance from espionage, it is a fact that even a small amount of information at once greatly increases the probability of successful solution and lessens the expenditure of time, effort, and funds necessary to achieve solution. On many occasions success

Doc ID: 6554247

TOP SECRET CREAM

in reading messages would probably not have been achieved at all had not some ulterior assistance been received, since a cryptographic system involving the principle of a truly random one-time pad would, so far as present knowledge is concerned, be absolutely impregnable to cryptanalytic attack.[1] If, therefore, it is possible to obtain by means of what are colloquially known as "second-story methods" a photograph of the one-time pad itself, the extracting of intelligence becomes possible. Similarly, in the case of less secure systems, the possession, for example, of a photograph of the basic code book used in an enciphered code system greatly reduces the time and effort needed for solution, even though success might be achieved without it.

Furthermore, one of the aims of the more astute cryptographers is to prepare systems in sufficient numbers so that only a small volume of traffic will pass in any one system. For this reason, it is frequently true that very little traffic can be intercepted in systems intrinsically not of the highest security but safe enough when insufficient traffic is available for study. A case in point is the sort of system provided by many governments for temporary use during an international conference: the small volume of traffic passing at such time may be entirely insufficient for solution while the importance of the traffic is even greater than normally.

For these reasons the mature cryptanalyst will be grateful for

---

1. GEE proved not to be a random one-time pad. See chapter IV, section C, pages 89, 90.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

any assistance that comes to him from the outside. Not only this, but he may even himself initiate steps to gain such help. In the case of military systems, particularly those used by echelons low enough to be subject to capture, the receipt of captured cryptographic documents becomes more frequent in proportion to the progress made by the armed forces of the United States and decreases in the same proportion as these forces are thrown back. Naturally, cryptographic personnel attempt to destroy material of this kind to avoid its capture but there will always be instances in which attack is so swift that destruction cannot be accomplished, and, as a result, cryptographic documents are made available for the study of the cryptanalysts.

Diplomatic systems, however, are not subject to this kind of capture. They are normally distributed in sealed diplomatic pouches. They are to be presumed to be kept under lock and key or in combination safes at all times. To photograph them without detection by their holders is a task that obviously requires the most careful and astute work on the part of those assigned to this activity. Only when the work is done without detection is it of any value at all, for, if suspicion is aroused, the presumption is that the users will at once change as many elements in the cryptographic systems that have been compromised as the difficulties of distribution under current conditions permit them to effect. If such changes are possible, it may well be that the value of the compromised documents is much less than the fresh obstacles created by the change. In many instances it is

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

therefore better to continue without such assistance than to run the risk of forcing a change.

For this reason the Signal Security Agency did not initiate extensive operations of this kind. Of the two alternatives, it preferred to depend more upon analysis and less upon ulterior assistance, and this preference rose less from confidence in its powers to perform successful analysis than from fear that clumsy attempts at theft of cryptographic documents might reveal to the government concerned the fact that compromises had been made. Nevertheless, the fact remains that much valuable assistance of this kind was received, together with some useless material.

The earliest example on record of compromise attempts through "second-story work" concerns the photographing of the diplomatic and consular code used by a Spanish official in Panama during World War I.[2] This attempt was actually instigated by the Chief of the Cipher Bureau, Captain Herbert O. Yardley,[3] who sent an agent provided, so it is said, with $20,000 for the purpose. What actually happened was that this agent was so clumsy and indiscreet that his mission became known to representatives of the Intelligence Officer on duty in Panama, and

---

2. See Historical Background of the Signal Security Agency, volume Two, p. 91. The information about what happened in Panama was given by one of the participating agents to Mr. William F. Friedman and is on file in the Office of the Director of Communications Research.

3. This statement is based on Yardley's book, The American Black Chamber, pp. 172-186. The account there differs from that of the agent, and the story of the appropriation of $20,000 for this purpose in particular is seriously open to question.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

he was told that if he would be patient these representatives would obtain what he wanted. The Intelligence agents made use of the fact that the Spaniard had a son whose thirst for strong drink had forced the father to limit his allowance to such a point that the son was easily induced to go on a wild party, the funds for which were supplied by the agents. Choosing a night when it was known that the official himself would be absent from home, the boy was made drunk through the help of two prostitutes. His key ring was abstracted from his trousers and an impression made of the safe key which he carried. Using this impression, another key was at once made, and with this the agents were able to open the safe and remove the code. This was photographed, but a single page failed to be photographed well, and the whole proceedings had to be repeated. Neither the Consul himself nor his son were aware that the code had been compromised, but the photograph became very useful in the solution of all the Spanish government codes, even though it was not the basis for many of the diplomatic systems. This story has been told in detail because it will serve as a useful illustration of the undercover method involved. The Signal Security Agency was not itself informed of the means used in the attempts at compromise which were successful, since the security of espionage agents depends on keeping their methods as secret as possible.

The following review of benefits to the General Cryptanalytic Branch from direct action of the kind described is based on a document

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

in the Branch files dated 17 February 1945:[4]

1. Finnish.—In 1943 the FBI was successful in procuring photographic copies of cryptographic materials in the Finnish Embassy at Washington. While some cryptanalytic success had been attained previously, this effort permitted the exploitation of all Finnish machine cipher systems the traffic of which was then available. Cribs,[5] keys, work sheets, and library references were obtained. Not only was a new source of intelligence developed over night, but insight into the techniques employed by Finnish cryptographers was a tremendous aid to our own research work. It would have been virtually impossible to read these systems through cryptanalysis in their later stages if it had not been for this "break." At the present time little Finnish traffic is being received. The military attaché in Rio is one important source of raw traffic; however, this traffic is sporadic and incomplete. It is extremely doubtful if the traffic could now be read without the background provided by the compromised material. See also footnote 14, page 254.

2. German.—Wolff, a German agent, was intercepted in the Canal Zone by the FBI in 1940, and the Signal Security Agency was provided with cryptographic materials which had been intended for distribution in South America. The immediate value of this compromise[6] can best be understood in relation to the cryptanalysis of GEC.[6] At that time, not only was it necessary for the cryptanalysts to recover the keys and the method of their application to the basic code, but it was also necessary to recover the basic code book of 100,000 possible groups. Among the materials Dr. Wolff carried was a copy of this basic code, and its possession eliminated the complex and infinitely meticulous task of a simultaneous recovery of both related elements, the code book and the additive used with it. Also among these materials were sheets of one-time pad (GEE) which enabled the analysts to determine the pad patterns leading to important discoveries in this system. Without photographic copies of these pads the characteristics of their reconstruction would not have been evident. More recently, the OSS has been able to provide German Foreign Office copies of messages in the latter quarters of 1944 (known as the "Boston Series").

---

4. Lieutenant Colonel Frank B. Rowlett to Colonel Harold G. Hayes, Subject: Assistance to Cryptanalysis, 17 February 1945, filed in WDGAS-90.

5. That is, messages containing wholly or in part the same plain text as that contained in messages sent in other systems or keys.

6. On this, see chapter IV, section B, page 83.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

These have been used to generate provisional additive to determine patterns, which can be correlated with those already produced in GEE. This fact, coupled with translations of GEC messages, has confirmed the authenticity of the "Boston Series." Thus, the value of the "Boston Series" to the cryptanalysts has been considerable. The FBI has several times submitted copies of cipher mail originating from German sources in Argentina, which, in some cases, the German Section has been successful in reading. This traffic would not have been available to the Signal Security Agency through regular channels, and the intelligence contained in it would have been lost.

3. Yugoslav.—An example of the value of the actual code book to cryptanalysis can be demonstrated in a consideration of the Yugoslav YOA book. An old version, picked up by the British[7] and forwarded to the Signal Security Agency, has been subsequently employed through repagination as the basic book in new systems. Despite the difficulties of reconstructing a repagination of a known book, the task of reconstruction without the book would be immeasurably more difficult, especially in considering the scarcity of able linguists in the Balkan Section and the paucity of traffic available for study.

4. Greek.—A copy of the GRB code book was received from the FBI in 1942. This permitted immediate exploitation of the system and saved the time of a number of personnel who would otherwise have been required for code reconstruction. In addition, a study of the format of the book was instrumental in demonstrating Greek cryptographic methods as well as the inflection principle used by the Greeks.[8]

5. Iran.—The British sent photographic copies of the Iranian diplomatic systems IRA, IRB, and IRC. At the time, the Near East Section had been painfully attempting to reconstruct

---

7. The British have had considerable success through the utilization of the direct method: "Photographs or actual copies of such cryptographic devices as keys, cribs, code books, cipher machine and indicator lists received from GCCS speak eloquently for the proficiency of the British Secret Service." (Quoted from the report cited in footnote 4 above).

8. The fact that some foreign languages employ highly inflected forms to express grammatical relationships produces characteristic frequencies which may become useful tools.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

the IRA book and had not even begun to think of further projects.[9] This piece of "practical cryptanalysis" permitted the complete exploitation of Iranian systems with a considerable saving of personnel and time.

6. Turkish.—The same is true of the Turkish systems TUA and TUE, in which actual copies of the code books were received. This aided key recovery considerably and permitted immediate exploitation of the message when the keys were solved. In addition, valuable linguistic personnel was freed from the code-recovery problems and became available both for translation purposes and cryptanalytic requirements.

7. Spanish.—Without direct aid the SPA tape system could not have been read since it is a one-time system. Regularly the keys for various circuits are received through the FBI, permitting direct exploitation of the system without delay. The British are also able to obtain these keys on the Continent, another indication of the development which their organization has attained. The [redacted] in South America have been instrumental in obtaining copies of raw traffic sent out by Spanish emissaries, which has allowed further development of this intelligence source. This traffic is not normally available through our intercept sources since it never goes on the air.

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

8. French.—The French Section has been the recipient of more compromised material than any other language group. The following photographed code books are in the Section: CTX (used in FMH and FMS); PC-148 (FAV); PC-146 (FAH); PC-155 (FAD); CGX (FCB tables); DN-1 (FAP); X-37 (FAM); X-38 (FAN); and PC-152 (FAC). These have been extremely valuable not only for exploitation but also in the research on unknown systems. Since the French frequently make use of variations of formerly used cryptographic materials, it has been possible to achieve solutions where some of the elements (i.e., the old material used in new systems) were available. The linguistic problem of code reconstruction of these codes through cryptanalysis would have required many more translators than have ever been available.

9. Portuguese.—Possession of the "Diccionario do Cifra de Ministerio dos Negocios Estrangeiros," Lisbon, 1910, 4th edition,

---

9. It should be pointed out that no one in the Section had ever had more than a smattering of Persian.

TOP SECRET CREAM

Doc ID: 6554247

TOP SECRET CREAM

has enabled the Section to read POA, POB, and POR; the 6th edition of this same book (1937), gave the basic code for POF, POH, POI, POJ, and POK; the 7th edition made possible the solution of POC, POD, POE, and POL. POM was made readable through the 8th and 10th editions of "Diccionario Cryptographico," while the 2nd edition of the Mascotte commercial code (1930) is used in PPD and BZE. The latter is a commercial code as is "Guedes", the code book used for PON, which was obtained from the Library of Congress. It should be stated that, while most if not all of these systems could have been read by pure analysis alone, to do so would have involved a huge amount of labor and time.

10. South American.--The Peruvian code book PEA was compromised at the Consulate in San Francisco in March 1943. It has been useful in solving PEB, which employed a code book constructed along similar lines. Other South American code books now in use which were received, presumable from the FBI, are: the"Solar" code book (CLA), "Clave Telegrafica" (ARB), and the books used in PAA and CUA.

These examples have shown the direct benefits to cryptanalysis, but other contributions have been just as useful, although their results are not immediate. For example, the OSS recently forwarded some German Hagelin machine directions to the Military Intelligence Service. From a study of the instructions contained in this material, it was possible for the analysts to develop a solution for a new and highly complex type of indicator system. It was valuable again in that it clearly illustrated the cryptographic lines along which the Germans were proceeding. This is a factor which cannot be overemphasized: regardless of the immediate value of any material received as a source of intelligence, another use, namely, that of accurately gauging the state of the art of cryptography in foreign countries, is realized as well. For this reason, too, all compromised cryptographic material, regardless of its immediate bearing, should be received at the Signal Security Agency for study.

TOP SECRET CREAM

Doc ID: 6554247

INDEX TO VOLUME TWO

Doc ID: 6554247

INDEX TO VOLUME TWO

A-1 (Personnel) 3
A-1 priority 259
A-2 (Tabulating Machinery) 3, 4
A Building, Operations 210, 235
"A" Machine 26, 29, 31, 32
"A" Machine, basic principles of 32
"A" Machine, cryptography of 32
"A" Machine used in place of "B" Machine 32
"A" net 241
A Section (Administrative) 3
"A" type indicator 32
ABA 170
ABB 170, 176
ABB-4 178
Abbott, Mr. E. Prentice 123, 140, 143
abbreviation 82
abbreviations 34, 36
abbreviations, military 136
ABC 170
ABD 170, 178
[redacted]
Abwehr Enigma, German 234,236,238,245,246
Abwehr Enigma, German, analysis of 240
academic training 163
accessory RAM equipment 278
accounting for documents 280
accounting for records 292
accuracy 53, 109, 262, 277, 278, 287
accuracy, check on 65
accuracy of American solutions 100
accuracy of reconstruction 136
accuracy of translations 110
achievement, French group 294
achievements of B-III 287
achievements of B-III-c-3 254
achievements of the Signal Security Agency 287
achievement, outstanding 30, 179
achievements 81
achievements, cryptanalytic 66, 93
achievements, GCCS 69
achievements, greatest 83
achievements of French Section 115
Achievements of the Italian Section, summary of 111
achievements of Research Unit B-III 196
action, request for from MIS 92
Adams, Lieutenant R. H. 4
Adams, Miss Ruth 131, 132
addenda, blanks for 143
addition of personnel 179
additive 85, 89, 93, 95, 121, 131, 133, 152, 158, 175, 218, 281, 300
additive and substitution encipherment 188
additive cards 134
additive cards, method of using 134
additive chart, master 63
additive, combined 85, 93
additive, construction of 90
additive, daily 135
[redacted]

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

Doc ID: 6554247

additive, derived from GEC-GEC-GEE isologs 90
additive digits 89
additive, enciphered 148
additive-enciphered five-digit one-part code 83
additive encipherment 8, 114, 115, 118, 133, 137, 151, 178, 188, 278, 285
additive encipherment, Italian 105
additive encipherment solution 6
additive encipherment unit 7
additive encipherments 101
additive encipherments, solution of 7
additive, Five-digit 108
additive, forty-digit 177
additive, four-digit 122
additive, GEE 84, 89
additive groups 89, 90, 93, 122
additive index 89
additive key 85, 86, 218
additive key book 120
additive key books 84
additive key, resultant 84
additive key, running 108, 212
additive key sequences 218
additive lines 84-86, 87, 95, 96
additive lines, combined 86
additive machine 92
additive machines 272
additive manufacturing machine 91
additive, pads of 89
additive pattern 56
additive problems 55, 57, 132
Additive Problems Unit 54
additive, provisional 301
additive recovery 101, 103, 105, 149, 195, 200, 283
additive, recovery of 157
additive, recovery of 195
additive recovery personnel 103
Additive Recovery Section 137
additive-recovery unit 117, 119, 131, 133, 152
Additive Recovery Unit, French 116
Additive Recovery Unit, Italian 105
additive-recovery units 151
additive, removal 150
additive, resultant 85-87
additive, reuse of 84, 89
additive sequence 108
additive sequences 105
additive, simple 219
additive, strip 122
additive, strip of 157
additive system 135
additive system, Free French 133
additive system, Vichy 134
additive systems 57
additive systems, French colonial 119
additive systems, colonial 120
additive table 120
additive tables 158
additive tape, one-time 158
Additive Unit 103
Additive Units 103
additives 86, 244, 284
additives, basic 83, 84 86, 87
additives, codes enciphered by 116
additives, columns of 121
additives, compromised 89, 90, 93
additives, pad 158
additives, prediction of 90

Doc ID: 6554247

additives, recovery of 102
address 233
addressee 226
adjustment of recording apparatus 264
adjustment of wheel-setting keys 264
Adkins, Mr. Roscoe 155
administration 103, 112, 115
administration of B-III 286
Administrative (A Section) 3, 4, 9
administrative advantages 11
administrative assistant 131
administrative head 54
Administrative Office of B-III 247, 292
Administrative offices 231
Administrative organization, SIS 103
administrative problems 287
administrative purposes 228, 231
Admiralty, Japanese 216
Administrative Services Unit 80
advance, scientific 92
advancement of cryptanalytics 281
aerial production 92
aeronautical operations 204
Aeronautics, Italian Ministry of 108
AFA 170, 174
AFB 170, 174
Afghan code, basic 174
Afghan system 174
Afghanistan 170, 177, 232
Afghanistan, systems of 175
Africa, East 106
African landings, North 211
African Theater, North 208
agencies 254
agencies, Government 36, 78, 219
Agency 172
agency, Governmental 37
Agency, mission of the 229
agent 298
agent, French 85, 86, 92
agent, German 88, 300
agent, German diplomatic 82
agent in Panama 89
agents 84
agents, British 85
agents, espionage 295, 299
agents, German in Argentina 226
agents, secret 76
agents, Intelligence 299
agents, secret service 106
agreement 22, 60
agreement with British 261
agriculturists 204
ai 35
aid, cryptanalytic 294
aides, cryptanalytic 200
Aids-to-Translators Unit 80, 81
air attaché systems 186
Air Corps, meteorologist in 207
Air Force code 188
Air Force code books, German 14
Air Force, German 243
Air Force traffic, German 235, 257, 259
aircraft, Japanese 92
airmail 49
Albert, Miss Ethel R. 171
Alderson, Miss Virginia 184, 194
Alexander, Miss Virginia 80
algebraic process of combining tables 252
alien detention camp, document found near 223
aligning messages, techniques of 254
Allied blockade 75

Doc ID: 6554247

Allied control 110
Allied Control Commission 110
Allied countries 190
Allied operations 260
Allied security 211
Allies, the 229, 287
allocation of discriminants 262
allocation of responsibility 22, 289
allocation system, discriminant 265
allotments to the Bureau of Ships 272
Allred, Sergeant Fred 157
alphabet 142, 178
alphabet Baudot 238
alphabet, Cyrillic 64
alphabetical arrangement 291
alphabetical range 161
alphabets 33, 65, 146 203
alphabets, mixed 32, 65
alphabets, random 147
alphabets, symmetrical standard 65
alphabets used at Bern 195
amalgamated unit 186
amalgamation 129, 130, 180
amalgamation of B-I-f and B-II-a-1 127
amalgamation of B-I-f with French Code Recovery Unit 126
amalgamation of B-2 and B-3 8
amalgamation of Chinese units 190
amalgamation of French units 7, 117, 119, 128
amalgamation of language and cryptanalytic units 185
amalgamation of Swiss and French Code Recovery Units 124
America 171
American analogues 46
American analysts 105
American Black Chamber, The 26, 51, 298
American contribution, evaluation of 15
American contribution to British, most valuable 15
American coverage 260
American cryptanalysis 100
American cryptanalyst 46
American designations 67
American forces 260
American interception 109
American Liaison Officer 239
American Liaison Officer in GCCS 292
American machines 273
American officers 13, 14
American "one-time" systems 94
American picture of Italian cryptography 102
American representative III
American signal intelligence services 52
American solutions 100
American systems 78
American systems, descriptions of 78
American traffic, raw 78
American universities 171, 219
American University in Cairo 171
Americans 268
Americans born abroad 172
Americans, naturalized 172
Americans, the 15, 53
anagrammed 253
anagramming 53, 130
Analin Fabrik Commercial Enigma, methods of solution of traffic 234
Analin Fabrik, traffic of 238
analogous phenomena 44
analogue, "Purple" 13, 45, 277

Doc ID: 6554247

analogues 45, 46
analogues, construction of 48
analysis 28, 56, 60, 78, 79, 84, 85, 127, 143, 147 175, 195, 203, 210, 242, 244, 278, 298, 303
analysis by Morgan's method 248
analysis, cipher 150
analysis, cipher-machine 281
analysis, flag, method of 239
analysis, methods of 242
Analysis of Captured Italian Cryptographic Material 110
analysis of cipher machines 285
analysis of CNH 184
analysis of Czech systems 194
analysis of difference between two keys 249
analysis of Finnish Hagelin machine 235
analysis of FWA 245
analysis of German Abwehr Enigma 240
analysis of GEX 245
analysis of flags applicable to Hagelin systems 256
analysis of Hagelin letter-subtractor machine 256
analysis of Hagelin Machine 250
analysis of Liberian traffic 203
analysis of machines 282
analysis of our own systems 282
analysis of reports 261
analysis of SLA 193
analysis of systems 28, 246
analysis of the "19 Kana Nigori" system 240
analysis of two-period cillies 268
analysis, statistical 251
analysis, traffic 261, 262
Analysis Unit 82
analysts 63, 68, 72, 77, 83, 96, 99, 136, 300, 303
analysts, American 105
analysts, British 100
analysts, traffic 262
analytical machinery, rapid, development of 271
analytic methods 61
analytical tests 34
ancient Greek 190
Anglo-American collaboration 13, 14, 15
Anglo-American liaison 15
Anglo-American plans for cooperation 100
Ankara 31, 108, 242
Ankara circuit 166
Annual Report for the Fiscal Year 287
aperiodic substitution system 57
Apollony, Lieutenant John C. 127, 154, 230
apparatus, recording, adjustment of 264
appendix of proper names 161
appropriation 298
aptitude 173
Arita (shi) itashi tashi 35
AR 25 102, 105, 110
AR 25 code reconstruction 101
AR 30 (ITD) code book 100, 101, 104, 107, 108, 110
AR 38 ("Y") 101, 104, 107, 108, 110
AR 40 104, 107, 108, 110
ARA 150
Arab lands 171
Arabian princes 176, 178
Arabic 172, 174, 178
Arabic, colloquial 171

Doc ID: 6554247

Arabic-English, English-Arabic glossary 174
Arabic language 178
Arabic, literary 171
Arabic systems 170
ARB 150, 159, 294, 303
Argentina 152, 159, 301
Argentine code 14
Argentine code traffic 149
Argentina, German agents in 226
Arlington Autoscritcher 268-270
Arlington Dudbuster 257, 266, 267, 270
arithmetic, non-carrying 214
arithmetic of solution 91
arithmetical relationship 184
Arlington Hall Station 4, 8, 21, 22, 103, 115, 117, 119, 123, 128, 129, 150, 151, 154, 155, 206, 209, 212, 213, 235, 266
Arlington Hall Station, move to 6, 247
armed forces of the United States 297
Armendariz, Sergeant Jose 149, 150
armies, French 222
Armistice Commission Enigma 245
Armistice Commission in North Africa 222
Armstrong, Sergeant Robert 162, 163, 169
Army 155, 189
Army, British 249
Army Codes 24, 62
Army codes, JE group Japanese 284
Army cryptonets 267
Army, communications, German 13
Army cryptanalysts 234
Army Field Clerk 221
Army, German 243
Army, Japanese 243, 291, 295
Army messages, Japanese 276
Army-Navy Communications Intelligence Coordinating Committee 288
Army problems, Japanese 275
Army Security Agency 12
Army Service Forces 288
Army Specialized Training Program 172, 182
Army stations, United States 217
Army systems, Japanese 74
Army traffic, German 235, 257, 259
Army traffic, Japanese 276
Army's answer to the Enigma problem 269
Army, United States 19, 40
Army Weather Central 209, 210, 213, 215, 219
arrangement, alphabetical 291
arrangement, plugboard 39, 46
articles, newspaper 223
ASA, Historian 13
ASA Glossary of Terms 57
assignment 292
assignment of priority 289, 290
assignment of short titles 291
assignment of traffic 117
assignment, special 280
assignment to temporary duty at GCCS 16
assimilation 193
assistance 297
assistance, British 137, 183, 193, 212 (See also EU and GCCS)
assistance, clerical 89

Doc ID: 6554247

assistance from espionage 295
assistance from EU 138
assistance from GCCS 186, 193, 201, 202
assistance, linguistic 81
assistance of Navy Department 272
assistance of Research staff 285
assistance to cryptanalysis 300
assistance, ulterior 296, 298
assistant, administrative 131
Assistant Chief of Staff, G-2 12, 13, 20, 48
Assistant Chief Signal Officer 1
assistant, civilian 289
assumptions 85
ASTP training 172
astronomer 206, 212
Athens 192
atmospheric disturbances 205
atomic bomb 52
attaché in Cortina d' Ampezzo 75
attaché in Moscow 78
attaché systems 24, 25
attachés 188
attachments to the 003 265
attack 30, 43, 49, 51, 56, 70, 105, 135, 278, 297
attack, cryptanalytic 11, 15, 69, 282, 296
attack, machine 268
attack, method of 42
attack on CNJ 186
attacks on enemy systems 282
attack on Polish systems 195
attack on systems 25
attack on traffic 13, 19
attack on YOA 194
attack, Pearl Harbor 2, 16, 23, 48
attack, point of 218
attack, points of 241
attacks, cryptanalytic 239
attempts, compromise 298
audition chambers 228
Aurell, Captain Verner C. 6; (Major) 9, 59; (Lieutenant Colonel) 10, 116
Austin, Robert Y. 207
Australia 232
authorization for travel 31
autokey 243
autokey substitution 57
automatic machines 45
automatic telephony 46
automobiles, use of private 209
autonomy 132
Autoscritcher 243, 284
Autoscritcher, Arlington 268-270
auxiliary system 53
Aviation Conference, International 178
aviators 204
AW 26
Axis 105
Axis countries 164
Axis governments, suspension of communications of 225
Axis representatives in Buenos Aires 225
Axis satellite governments 190

B-1 (Bulletin Unit, the) 8
B-1 (Information Unit) 8
B-1 (Japanese) 3, 4
B-1 (Japanese Language) 9, 10
B-1 (Liaison Unit) 8
B-1 (Miscellaneous service units) 6
B-1-c 292
B-I-5 (Nisei) 10
B-I 81, 116, 228

Doc ID: 6554247

B-I, Chief of 59
B-I school 61
B-I-c 106, 128, 156, 159
B-I-f 126, 127, 155
B-I-f, amalgamation with B-II-a-1 127
B-I-f, amalgamation with French Code Recovery Unit 126
B-I-m Unit 81
B-2 (Code and additive encipherment solution) 6, 7, 8
B-2 (German) 3, 4
B-2 (Japanese Military Cryptanalysis) 9, 10
B-2-a 230
B-II 74, 119, 124, 133, 240
B-II-a 115, 116, 139, 151
B-II-a-1 123-125, 127, 139, 197
B-II-a-1, amalgamation with B-I-f 127
B-II-a-5 151
B-II-a-13 170
B-II-b 116
B-II-b-1 119, 122-124
B-3 (Cipher solution and solution of code encipherment other than additive encipherments) 6, 8
B-3 (General Cryptanalysis) 9, 10
B-3 (Italian) 3, 4
B-3 plan of organization September 1943 10
B-3 Section (new) 8
B-III 55, 74, 106, 116, 130, 132, 154, 183, 228, 236, 237, 253, 286, 289, 291, 292
B-III, achievements of 287
B-III, Administrative Office 292
B-III, Chief of 59
B-III, contributions of 282
B-III, Control Unit 289
B-III, cryptanalytic activities, exhibition of 240
B-III cryptanalytic sections 290
B-III, Officer in Charge 250
B-III, policies of 287
B-III, Research Section 201
B-III, systems studied in 280
B-III Research Unit 55, 193, 194
B-III units 290
B-III-a 132, 155, 163, 197
B-3-a 230
B-III-a, Technical Director 189
B-III-a-1 112
B-III-a-5 170
B-III-b 197-199, 203, 231, 232, 261
B-III-c 143, 243
B-III-c-1 273
B-III-c-2 237, 240, 245
B-III-c-3, 254
B-III-c-4 237, 257, 267
B-III-c-4 (B-III-f) 54
B-III-c-5 237, 267
B-III-d 117, 130, 131, 244, 294
B-III-d-1 220, 228, 285
B-III-d-2 180
B-III-d-3 170
B-III-f 186
B-III-f (B-III-c-4) 54
B-III-f-1 54
B-4 (French) 4
B-4 (Mexican, etc) 3
B-4 (Tabulating Machinery) 6, 9, 10
B-4 (traffic Analysis and Control) 10
B-5 (Stenographic) 3, 4
B-5 (Nisei) 10
B-5 (Vint Hill Translation Section) 10
B-6 (Traffic) 3, 4
B-7 (South American) 4
B-8 (Tabulating Machinery) 4

Doc ID: 6554247

B-9 (Information) 4
B-10 (Weather) 4, 5
B-211, Swedish Hagelin 245, 247
B Branch 130, 153, 231, 235, 236, 261, 262, 264, 271
B Branch Administrative Office 247
B Building, Operations 104, 210
"B" Cipher Machine 31
"B" initial letter 25
"B" Machine 32-34, 39
"B" Machines, Japanese 46
"B" Machine, mechanics of 45
"B" Machine message 36
"B" Machine, solution of 31, 44, 47
B Section (cryptanalytic) 3, 6
"B" Table 27
back traffic 59, 87
background 300
backlog 193, 292
backlog of traffic 49, 101
Badnerosky, Miss Regina 191
Bailey, Miss Clarice P. 171
Baker, Lieutenant Margaret 257
Balkan cryptography 181
Balkan Section 301
base settings, NEA, reconstruction of 255
Balkan situation 194
Balkan systems 181, 192
Balkan systems, principal problem of 193
Balkans, the 138
Bangkok 189
Bank of China 187
banks 58
Banks, Mrs. (Miss Jean Hitch) 220, 221
Barasch, Lieutenant S. 19
Barker, Miss Anne 80
Barker, Miss Julia 155
Barker, Mr. Wayne S. 118, 148, 150, 160; (Lieutenant) 155
Barnes, Jr., Lieutenant Harold M. 104
base 41, 42
Bash, Corporal Ivan 4
Bash, Mrs. (Miss Rosalie Harding) 113, 148
basic additives 83, 84, 86, 87
basic additive key 85
basic book, TUH 177
basic change 244
basic code 63, 105, 133, 135, 136, 147, 184, 185, 188, 190
Basic code,Afghan 174
basic code 300, 303
basic code book 296, 300, 301
basic code, plain 213
basic code, POJ 165
basic code book, captured 120
basic IMC synoptic 214
basic language 5
basic law 39
basic machine 245
basic principles 53
basic sequences 43, 44
basic sequences, reconstructed 44
basic square, recovery of 285
Bates, Lieutenant Joseph E. 237; (Captain) 257, 264
Bates, Mr. Lewis E. 170, 171, 176
Battle of Britain 12, 17, 260
Baudot alphabet 238
BEA 198, 233
Bearce, Mr. Herrick F. 2, 29, 113; (Lieutenant) 4, 115, 118, 126 (Captain) 116, 151; (Lieutenant Colonel) 113

Doc ID: 6554247

Bearce's section 112, 118 147, 148, 160
Bearce's staff, Mr. 148
BEB 198, 233
BEC 198, 233
BED 233
BEE 233
Beechnut Project 264
Begin-spell group 143
beginning groups 283
Beikoku 35
Belgian government 130
Belgian solution 198
Belgian traffic 132, 197-199
Belgium 126, 233
Belgium, systems of 197
Bell Telephone Laboratories 257, 258
Bell Telephone personnel 263
belligerent 141, 142, 145
Bennett, Mr. Emmett 79
Bennett, Miss Mary M. 173
Berkeley Street 17, 20
Bentley's Second Phrase Code 185, 187
Berlin 31, 83, 91, 241, 242
Berlin Foreign Office 245
Berlin-Lisbon traffic 241
Berlin-Tokyo circuit 92
Berlin, traffic from 246
Bern 146, 237
Bern, alphabets used at 195
Bern-Caracas circuit 146
Bernstein, Lieutenant Carlos 157
Berryman, Mrs. Wilma Z. 48, 98, 100, 101
Bevans, Dr. Caleb 112, 114, 117, 123, 132, 140, 143, 197, 201, 202
BEZ 233
bibliography on Hagelin solution 247
Bicher, Colonel George 264
Bickwit, Captain Leonard 116
Bidwell, Miss Mary 140, 145
"Bings" 268
biographical file 174
bipartite indicator 83
Blank, Miss Frances G. 102, 106, 107
blanks 283
blanks for addenda 143
blanks, pattern of 52, 53, 55
Bletchley Park, Bletchley 12, 17, 20, 21
blockade, Allied 75
block of sheets, homogeneous 90
blocks, key 201
blocks of groups 63
Bloom, Lieutenant Seymour 120, 121, 133, 202
Bogota 168
Bolivia 152
bombe 262
Bombe (003) 236, 237, 242-244, 246, 264 (See the "003")
Bombe 003, installation of 262
bombe maintenance crew 263
Bombe methods of solution 267
Bombe operations 264
bombe operators 263
bombe, relay 260
bombe, rotary 257, 259
bombings in the Far East 137
book 301
book IRA 302
book recovery 179
book, TUH basic 177
book YOA 301
books, JN-36 key 219
books, phrase 182
Bordeaux 241
Bordy, Mr. Laurence 80
Boston Series, the 300, 301
"BP" 17
Bradley, Miss Helen J. 112 114, 117, 119, 131, 132, 197
Brainerd, Miss Virginia 206
branches 11
Brazil 2
Brazilian code 14
Brazilian code traffic 148, 149

Doc ID: 6554247

Brazilian Codes and Ciphers 1917-1945 169
Brazilian cryptography 169
Brazilian five-digit traffic, index of 161
Brazilian five-letter system 160
Brazilian Government 51
Brazilian messages 161
Brazilian systems 8, 149, 160-163, 167, 168
Brazilian systems, study of 151
Brazilian traffic 160
Brazilians 160
"break", a 300
break pattern, wheel 244
break wheel 32
breaking of Japanese code 31
Briggs, Mrs. Annie H. 231
Brisbane 54
Brisbane, Cipher Bureau 103
British 13, 37, 58, 59, 78
British and American sections, liaison between 59
British agents 85
British, agreement with 261
British analysts 100
British Army 249
British assistance 183,193 (See also under EU and GCCS)
British Colossus machine 239
British compilation unit 12
British contribution, largest 15
British contributions 100, 183, 212
British contributions to the Signal Security Agency, evaluation of 14
British cooperation 17, 59, 165
British cryptanalysts 137, 177, 212
British, cryptanalytic liaison with 11
British cryptanalytic units 12
British Empire, the 146
British, exchange of military information with 11
British, experience of 212
British firm 94
British Foreign Office 95
British Government 51, 247, 259
British Government Code and Cypher School 69, 100, 138
British information 12, 169
British, information supplied by 165
British intercept sets, release of 260
British intercept stations 70
British interception 260
British Liaison Officer 59, 259
British Liaison Officer in Washington 16
British method of operation 261
British officer 57
British operations 17, 260
British personnel 260, 266
British point of view 261
British procedures 17
British reconstruction of CNB, photograph of 183
British Secret Service 301
British Section 59
British solution 63
British source 94
British staffs 19
British study, results of 14
Brazilian systems 169
British technique 17, 19
British, the 57, 84, 85, 94, 95, 100-102, 104, 106, 108, 111, 114, 119, 125, 133, 134, 136, 141-145, 160, 165, 166, 187, 209, 215, 219, 238, 242, 249, 262, 266-269, 301, 302
British unit 263
British translations 193

Doc ID: 6554247

British units, organization 19
British, violation of pledge to 13
British, willingness to cooperate 12
British work, copies of 169
British work on POD and POJ, photographs of 165
broadcast 206
broadcast conditions 206
broadcast, intervals of 205
broadcasting 213
broadcasting of weather reports 204
broadcasting of weather reports from Dakar 211
broadcasting of weather reports, German 215
broadcasting schedules, Japanese 217
broadcasts, Domei 226
Brod, Miss Olga 102
Brooklyn Museum, Director of 181
Brown, Miss Jean 159
Brown, Dr. Calvin S. 22, 119, 120, 121, 129, 132, 201, 202
Brown, Lieutenant William Edward 133, 140, 142, 144 (Captain) 139
Brumbaugh, Mr. Robert S. 253; (Private) 256
Brussels 31
Bryan, Mr. William 54, 281
BUA 192, 193
BUA, paginations of 192
BUB 192
BUC 192, 193
BUD 192
Buchanan, Dr. Percy 81
Bucharest 75
Bucharest circuit 166
Bucharest, fall of 203
Budapest 70
Budapest circuit 166, 200
Buenos Aires 86, 226
Buenos Aires, Axis representatives in 225
Buenos Aires, ban on messages out of 252
Buenos Aires circuit 166
Buenos Aires messages, relay from Washington 252
Buenos Aires traffic 127
Buenos Aires version of FIA systems 254
Buffham, Lieutenant Benson K 208, 209, 289; (Captain) 229, 231, 288
Buffham, Mrs. Kathryn Dubois 62
Bulgaria 177, 191, 232
Bulgaria, Nazi government of 180
Bulgaria, surrender of 193
Bulgarian cipher (BUC) 193
Bulgarian code 192, 196
Bulgarian military attache ciphers 192
Bulgarian systems 191
Bulgarian traffic 192
bulletin (collective) 204
Bulletin, daily 35
Bulletin, Daily Information 286
Bulletin, first translation submitted 28
Bulletin, the 6, 28, 174, 203
Bulletin, the SSA 87
Bulletin Unit, the (B-1) 8
Bullock, Colonel Frank W. 257
Bundy, Lieutenant William P 236, 251, 254
Bunting, Corporal James 200
Burch, Miss Evelyn 263
bureau, central, location of 205
Bureau of Ships, assistance of 272
bureaus, cryptographic 108
Burn, Mrs. K. 155
Butler, Miss Nellie 80
BZA 169
BZB-1 169
BZB-2 169
BZC 160, 161, 167-169

Doc ID: 6554247

BZD 160-163, 167-169
BZD (?) 160
BZE 168, 303
BZF 163, 168, 169
BZG 169
BZH 168, 169
BZI (?) 160
BZL 169
BZM 169
BZN 169
BZO 169
BZP 169
BZQ 169
BZR-1 to BZR-8 169

C-36 Hagelin 247
C-38 Hagelin 247
C-38 machine 253
C-41 Hagelin 247
"C" period traffic 71
C Section (Cryptographic) 3
CA 26, 27, 53
cable 69, 75, 266
cablegrams 223
Cairo, American University in 171
calculation, statistical 38
California, Pasadena 213
call signs 291
calligraphy, Chinese 181
camera, Dudbuster 266
camera, special with lucite rods 279
camera, Tetragraph Tester 275, 276, 279
cameras, IC 272, 279
Campbell, Dr. Mary T. 102, 106
Canadian cryptanalysts 137
Canadian Examination Unit 60, 120, 138
Canadian organization 18
Candaian stations 217
Canadians, the 113, 133, 134, 136
Canal Zone 300
capacity of the 003 265, 266
capacity of the Dudbuster 266
capitals 70, 164
capitulation of Italy 213
capitulation of Japan 47
capture 297
capture of code 118, 199
capture of Japanese weather code 216
capture of the Miquelon code 113
capture of system 226
captured code 109, 128, 136, 219
captured code book 120
captured code books 201
captured cryptographic materials 110
captured diaries 222
captured documents 94, 95, 111, 297
captured encode 128
captured German pads 88
captured Japanese Army machine, Green 284
captured key books 218
captured loose sheets 222
captured machine 264
captured material 118, 219
captured materials 108
captured notebooks 222
captured plain text 253
captured pads 89
captured stenographic documents 221
captured systems 137
Caracas 168
card, five-fold 71
card reproducer, IBM 277
cards 292
cards, additive 134
cards, IBM 283
cards, photographing of 283
cards, reproduction on 277
carelessness 85

Doc ID: 6554247

Carl, Corporal Ralph 120
Carlson, Captain Paavo 253
Carrol, Lieutenant John E. 112, 114, 116, 123; (Captain) 119, 124, 125, 131, 133
Carter, Dr. Albert Howard 112, 114, 140, 236, 249-251, 253, 255, 256, 261, 286
Casassa, Miss Betty 122
Cassity, Dr. Ronald 79
Catalan 150
catalog 242
Catalog, Eggs 242
catalogging of documents 280
catalogs, reference 241
Cate, Mr. Paul S. 48
causal repetitions 38
Cayenne 168
cells 65
Censorship, Office of 150, 220, 223
centers, cooperating 22, 58, 91
centers, crypanalytic 257, 263, 287
centers, intercept 261
centers, two 79
Central American governments 148
Central, Army Weather 209, 210, 213, 215, 219
Central bureau, location of 205
Central Europe 180
Centrals, Japanese Weather 216
Cerecedo, Captain Javier H. 148-151, 156; (Major) 147
Cerecedo's unit 152
cessation of German military activities 266
cessation of hostilities 50
cessation of Italian traffic 212
cessation of traffic 266
CGX 302
"CH" Code 27
Chamberlain, Lieutenant Culver C. 182
change 11, 55, 66, 72, 74, 75, 79, 84, 107, 178, 262, 298
change, basic 244
change in cipher tables 193
change in encipherments 185
change in indicatives 212
change in key book 253
change in plate gate of IC projector 276
change in plugging 267
change in policy 176
change in system 68
change of elements of a system 297
change of indicator system 282
change to A Dictionary of United States Army Terms 288

changes 67, 83, 110, 115, 134
changes, cryptographic 242
changes in cryptography 76
changes in Japanese cryptography 277
changes in keys 46
changes, periodic 66
changes in personnel 229
changes in system 28, 69
changing keys, daily 53
channels 70
channels, clandestine 246
channels, communication 263
channels, communications 53
channels, German 190
channels, regular 301
character 279
characteristic 143
characteristic frequencies 218, 301
characteristics 141, 300
characteristics, external 289
characteristics, frequency 182

Doc ID: 6554247

characteristics, identifying 291
characteristics of traffic 200
characters 275
characters, Japanese 64
chart, 10 x 8 65
chart, 26 x 26 65
chart, code 66--68
chart, deciphering 33
chart, digraphic 64
chart, indicator key 66, 67
chart, JAS serial number key 69
chart, master additive 63
chart, progress 222
chart, serial number 66
chart, tetragraphic 64, 70
charting techniques 183
charts, key 71
charts of logarithmic value 71
check on accuracy 65
checking 264
checking of runs 263
checking, system of 292
checking of work 289
Chemnyco Company, traffic of 238
Cherniss, Dr. Ruth 112, 126--128, 293
Chicago 178
Chief of Cipher Bureau 298
Chief of Staff 18, 259
Chief Signal Officer 1
Chief, SIS 12, 13, 16
Chile 105, 152, 159
Chilean cipher, five-alphabet 150
Chilean ciphers 155
Chilean code 14, 150
Chilean code traffic 149
Chilean codes 152
China 181, 232
China-Burma-India Theater 207, 219
China, North 182
Chinese 184, 186
Chinese calligraphy 181
Chinese code 183
Chinese code system, enciphered 184
Chinese code, two-part 188
Chinese codes 196
Chinese, colloquial 181
Chinese cryptanalytic problems 184
Chinese cryptanalytic unit 190
Chinese digit systems 187
Chinese diplomatic systems 17
Chinese enciphered codes 118
Chinese encipherments 183, 194
Chinese, experts in 185
Chinese Foreign Office 187
Chinese Foreign Office systems 188
Chinese government 196
Chinese government codes 187
Chinese Government Salt Monopoly 181
Chinese language, expert in 181
Chinese language problems 186
Chinese language unit 190
Chinese Ming Code 182, 185
Chinese Mission in Washington 183
Chinese problems 194
Chinese Systems 180, 181, 189, 194, 191
Chinese systems, solution of encipherment of 180
Chinese, telegraphic 182
Chinese traffic 182
Chinese transposed code 187
Chino-Thai Unit 132
Chinov (FBI) 120
Christopher, Mr. Edward E., Jr. 48, 62, 79, 80, 100, 101, 114
Chunking government 180
Chungking, National Military Council in 188

Doc ID: 6554247

Chungking systems 186, 187
cifax 281
cilli 267
cillies, two-period 267, 268
cipher 72, 105, 106, 153, 176
cipher analysis 150
cipher, Bulgarian (BUC) 193
Cipher Bureau, Brisbane 103
Cipher Bureau, Chief of 298
cipher bureau, Netherlands 54
cipher, Chilean five-alphabet 150
cipher, Colombian 148
cipher component 72
cipher device, U. S. M-138-A 127
cipher equivalents 43, 165
cipher, fractionating 245
cipher, French military 135
cipher, French military machine 245
cipher group 283
cipher groups 284
cipher, Iraqian 174
cipher, Japanese secret 31
cipher letters 33, 38
cipher, machine 26, 51, 88, 159
cipher-machine analysis 281
cipher machine, combined-operations 282
cipher machine for field use 247
cipher machine, German-manufactured 146
cipher machine, Hagelin, invention of 247
cipher, machine, Japanese Army 240
cipher machine, Japanese Navy 30
Cipher-Machine, Kryha 83
cipher machine lists 301
cipher machine problems 237
Cipher Machine Section 280
cipher-machine systems, German 282
cipher-machine systems, Japanese 282
cipher machines 29, 234
cipher machines, analysis of 285
cipher mail 301
cipher mechanisms 39
cipher message 249
cipher messages 246
cipher messages, German teletypewriter 276
cipher, Mexican 14
cipher, Mexican "Guion" 150
cipher, Mexican two-alphabet 150
cipher, military (BUC) 193
cipher, plain text mixed with 227
cipher, polyalphabetic 147, 150
cipher, polyalphabetic substitution 108, 140
cipher problems 8
cipher problems, specialized 154
cipher, "Purple" Machine 59
Cipher Section 106, 116, 119, 129, 140, 143, 144, 146, 153, 154, 168, 183, 230, 235, 243
Cipher Section, Officer in Charge 236, 250
cipher section in Singapore, British 14
Cipher Security Mission 111
cipher sequences 30, 40
cipher, Slovakian (SLA) 193
cipher, solution of 5, 6, 132, 149
Cipher Solution Unit 151, 154, 155
cipher square 65, 66, 68, 69, 72, 76
cipher square, random 278
cipher squares 63, 75
cipher squares, reconstruction of 63
cipher system 146, 168
cipher system, diplomatic 203

Doc ID: 6554247

cipher system, "Purple" 58
cipher system, Turkish 177
cipher systems 150, 152, 154, 155, 162, 184, 196
cipher systems, Mexican 148
cipher systems, Portuguese 167
cipher systems, Spanish-American 153, 156
cipher systems, Syrian 178
cipher tables 193
cipher tables, Swedish 249
Cipher Teleprinter Regulations (SFV) for the Wehrmacht after 1 December 1942. 234
cipher teletypewriter, SIGCUM 280
cipher, teletypewriter, solution of German 277
cipher text 29, 53, 56, 57, 76, 252, 246, 253, 275, 276, 278
cipher-text frequency 246
cipher-text letters 3
cipher text, matching 283
cipher text, mechanical means of sliding crib against 239
cipher text, slide-testing of 92
cipher-text values 34
cipher texts 200, 267
cipher traffic, Colombian 149
cipher traffic, Dominican 149
cipher traffic, Mexican 149
cipher traffic, Venezualan 149
cipher, transposition 178, 195
cipher, twenty-alphabet Mexican 14
Cipher Unit 116, 117, 121, 122, 123, 125, 130, 131, 154
Cipher Unit, French 115, 118, 119
Cipher Unit, French Transposed 126, 129, 130
Cipher Unit, Miscellaneous 153, 154
cipher units 154
cipher units, Machine 146
cipher used by Mihailovic 194
cipher wheels 29, 30
ciphers 8, 169, 194
ciphers, Bulgarian military attache 192
ciphers, Chilean 155
ciphers, codes and 223
ciphers, Colombian 150
ciphers, Cuban 150
ciphers, digraphic substitution 178
ciphers, German Teleprinter 240
ciphers, machine 21, 23, 236, 240, 251, 261, 278, 284
ciphers, machine, cryptanalysis of 235
ciphers, Mexican 150
ciphers, military 167, 192
ciphers, solution of 5, 277
ciphers, Swiss 140
ciphers, Teleprinter, German 234
ciphers, Venezuelan 150
ciphony 281
circuit, Ankara 166
circuit, Berlin-Tokyo 92
circuit, Bern-Caracas 146
circuit, Budapest 166
circuit, Buenos Aires 166
circuit, Damascus-Ryadh 178
circuit, Istanbul 158
circuit, Mexico City 167
circuit, New York 166, 168

Doc ID: 6554247

circuit, reflexing 282
circuit, Rome-Washington 111
circuit, Tokyo-Berlin 92
circuit, Tokyo-Kabul 60
circuit, Tokyo-Kuibishev 60
circuit, Tokyo-Vatican City 60
circuit, Washington 161, 164 167
circuits 135, 147, 182, 249, 289, 291, 302
circuits, Bucharest 166
circuits, clandestine 242
circuits, European 161
circuits, point-to-point 290
circular isologs GEC-GEE 89
circular messages, instructions for 75
circular numbers 86
circular system, special 76
circulars 75, 200
cities, South American 158
Ciudad Trujills 99, 168
civilian assistant 289
civilian employee 12
Civilian in Charge 4
civilians 9, 163, 164, 229, 273
civilians, Negro 231
"(civil)isati(on)" 253
CLA 150, 153, 156, 159, 294, 303
clandestine channels 246
clandestine circuits 242
clandestine interception 228
clandestine traffic 225, 226
clarity 287
Clark, Mrs. Constance 123, 139, 140, 144
Clark, Mr. H. Lawrence 29, 48, 63
Clark, Miss Kathryn (Mrs. Novak) 122
Clarke, Mr. A. B. 257
Clarke, Major Stanley 112, 114, 116, 119
classes of students 61
classical scholar 190
classified material 210
Clave Telegrafica (ARB) 303
Clayton, Dr. Vista 114, 120, 121, 123
CLE 150
clear, in the 205
clerk, code 62, 65, 129
clerical assistance 89
clerical personnel 89, 163, 237
clerical personnel, shortage of 263
clerical work 48
clerks 127, 162, 191, 208, 249
clerks, code 85, 86, 143
clerks, enlarged staff of 191
clerks, Japanese code 74, 219
climatological data 216
climatological information 215
climatological studies 219
climatology, science of 211
clip setting 267
clue 36, 253
CNA 182
CNB (Dryo) 182, 186
CNB, British reconstruction of 183
CNC (Win) 182, 186
CND (Invincible) 182, 186
CNF 183, 186
CNG 183, 184, 185, 188
CNH 183, 184, 185
CNJ 186
CNK 187
CNL 185, 186, 188
CNM 186-188
CNN 187
CNO 187

Doc ID: 6554247

CNP 187, 188
CNQ 187, 188
CNS 187
CNT 187, 188
CNW 188
CNX 188
CNY 188
COA 148, 150
Coast Guard, United States 160, 242, 246
coastal stations 212
code 35, 83, 96, 104, 107, 110, 125, 136, 137, 143, 153, 157, 166, 188, 199, 212, 232, 299
code, additive 83
code, Air Force 188
code and additive solution (B-2) 6
Code and Cypher School, British Government 100
code, basic 63, 133, 135, 136, 146, 184, 185, 188, 190, 213, 303
code, basic Afghan 174
code, basic POJ 165
Code, Bentley's Second Phrase 185, 187
code book 82, 158, 161, 203, 301
code book, AR 30 100
code book, basic 120, 296, 300
code book compromised 303
code book, DESAB No. 3 82
code book, GRB 301
code book, Guedes 303
code book No. 4 83
code book, Peruvian 303
code book, photographed 99, 158
code book, RA-1 100
code book, two-part 157
code books 95, 219, 301
code books, captured 201
code books, compromised 7
code books, copies of 302
code books, German Air Force 14
code books, photographed 302
code books, South American 303
code, Brazilian 14
code, Bulgarian 192, 196
code, CA 53
code, capture of 118, 199, 219
code, captured 128, 129, 136
code "CH" 27
code chart 66-68, 70
code charts, list of 67
Code, Chinese Ming 182, 185
code, Chinese transposed 187
code clerk 62, 65, 129
code clerks 85, 86, 143
code clerks, Japanese 74, 219
code, commercial 233
code communications 108
code, compromise of 299
code, compromised 104, 122, 133, 144, 148, 167, 174, 175, 191
code, Croatian puppet government 193
code digraphs 71
code, diplomatic 165
code, DR 125
code, enciphered 64, 115, 144, 168, 175, 177, 195, 198, 202
code enciphermentes 5
code, English 187
code "EK" 27
code, FES 125
code, five-digit 83, 121
code, five-letter 147
code, four-digit 129
code, four-letter 26
code, General Staff 188
code, General Tai Li's 188
code group 99, 142, 219
code-group limitation 168
code group, permutations of the 145

Doc ID: 6554247

code-group values 109
code groups 35, 64, 70, 110, 122, 130, 136, 141, 160, 202, 283
code groups, five-digit 135
code groups, four-digit 157, 177
code groups, four-letter 25
code groups, three-letter 25
code groups, two-letter 25
code groups, high-frequency 283, 284
code groups, tetragraphic 283
code groups, unidentified 294
code, Hanoi 114
code "HE" 27
code identification 231, 232
code, Impero 108
code-instruction messages 134, 252, 268
code, Italian commercial 105
codes, Italian diplomatic 109
Code, International Meteorological 4, 204, 205, 210
Code, International Meteorological, Japanese nonuse of 216
code JG 25
code, K-1 36
code limitations 201
Code, Mascotte Commercial 160, 303
code materials 74
code messages 127, 141, 142
code, Miquelon 113
code, most secret diplomatic 177
code, naval 129
code, "OG" 27
code, one-part 83, 122, 136, 142, 158, 174, 182, 186, 219
code, open 150, 220, 223, 225, 226
code, open, first solution of 223
code, open, testing for 224
code, pentagraphic 99
code, pentanomic 133
Code, Phillips 34
code, plain 178
code, Polish 195
code, Portuguese diplomatic 167
code, preamble of 231
code reconstruction 5-8, 70, 301, 302
code reconstruction, AR 25 101
code reconstruction, Impero 101
code reconstruction problems 8
code reconstruction unit 7
code, reconstructions of 14, 17
code reconstructors 96
code recovery 101--103, 108, 114--116, 121, 122, 132, 133, 135, 136, 137, 144, 145, 149, 152, 156, 164, 175, 185, 186, 189, 193, 198, 199, 202, 203, 294
code recovery problems 101, 140, 195, 302
code recovery, Swiss 140
Code Recovery Unit 104, 117--119, 121--124, 126, 131, 134
Code Recovery Unit, French 116, 145
Code Recovery Unit, Italian 125

Doc ID: 6554247

Code Recovery Unit, Spanish 151, 155
code, relined 177
code, repaginated 161, 177
code, revised 64
Code Room, OWI 255
Code, Rudolf Mosse Commercial 83, 96
code, secret 216
Code Section, Transposed 134
code, simplified 178
Code, Sittler Commercial 199
code, solution of 5
code, Spanish diplomatic and consular 298
code system 158, 184, 190, 203
code system, enciphered 296
code systems 152, 154, 193
code systems, enciphered 118, 183, 189
code systems, enciphered Japanese diplomatic 283
code systems, Spanish language 159
code, Swiss 145
code, tetranomic 133
code, tetranomic one-part enciphered 144
code text 65, 73
code text, enciphered 65
code, Thai 189
code, three-digit 135
code traffic 152, 153
code traffic, Argentine 149
code traffic, Brazilian 148, 149
code traffic, Chilean 149
code traffic, Mexican 149
code traffic, Portuguese 149
code, transposed 134
code, trigraphic 64
code, trigraphic enciphered 144
code, trigraphic Foreign Office 188
code, two-letter 26
code, two-part 101, 119, 111, 114, 120, 124, 136, 145, 161, 186, 188
code, two-part Turkish 174
code "UJ" 27
code, underlying 195
code, unenciphered 64, 96, 121--123, 126, 168, 198, 202
Code Unit 104
code units 103
code, unknown 55
code used in polic work 109
code values 70, 102, 125
Code, Vichy DX 122
code work, German 21
code writing 35
code "X" 99
code, Yugoslavian 192, 196
codes 8, 27, 62, 139, 141--143, 145, 175, 202, 231, 293
codes and ciphers 223
codes, Army 24, 62
codes, captured 109
codes, Chilean 150, 152
codes, Chinese 118, 187, 196
codes, commercial 229, 232
codes, companion 144
codes, compromised 124
codes, diplomatic 109, 187
codes, enciphered 107, 116, 121, 165
codes, English language 25, 230
codes, five-digit 202
codes, French 17, 18, 124, 127
codes, German 140
codes, Japanese 17
codes, Japanese Army, JE group 284

Doc ID: 6554247

codes, language 219
codes, Mexican 150, 152
codes, Navy 24, 109
codes of limited distribution 169
codes, one-part 141, 152
codes, open 221
codes, Portuguese 165
codes, Russian 78
codes, secret 182
codes, separation of 153
codes, solution of 196
codes, Spanish 17, 150
codes, Spanish-American 153, 156
codes, Spanish government 299
codes, special purpose 169
codes, study of 152
codes, syllabary 24
codes, Swiss 131
codes, underlying 184
codes, unenciphered 113, 141, 182
codes, unknown 182, 186
codes, U-type (JU) 24
codes, Vichy 114, 137
Coffee, Mr. William D. 229, 231
coincidence 276
coincidence counting, high-speed 274
coincidence, index of 271, 274
coincidence tests 274
coincidences 267, 271, 273
coincidences, counting of 275, 277
Cole, Miss Abbie 184
collaborated 189
collaboration 2, 103, 127, 144, 150, 184, 185
collaboration, Anglo-American 15
collaboration with British 177
collaboration with the Navy 58
collective 204, 205
collective message 217
collective system, inter-service 217
collectives 211
college, Finnish 254
Collins, Lieutenant Charles P. 237, 263, 264; (Captain) 257
Collins, Lieutenant Morris R 235, 263
colloquial Arabic 171
colloquial Chinese 181
Colombia 2
Colombian cipher 148
Colombian cipher traffic 149
Colombian ciphers 150
Colombian traffic 147
colonial development companies 57
Colonial E-5 120
colonial office, Portuguese 167
colonial system, Spanish 159
colonial systems 166, 167
colonial traffic 166
colonies 120
Colossus machine, British 239
Columbia University 171
column 284
columnar transposition 129, 188
columns 39, 65, 70, 75
columns of additives 121
combination 86
combination safes 297
combined additive lines 86
combined additives 85, 93
combined-operations cipher machine 282

Doc ID: 6554247

combining of tables through algebraic process 252
combining operations 7
commanding officer 3
commercial code, Italian 105
Commercial Code, Mascotte 160, 168, 303
Commercial Code, Rudolf Mosse 83, 96
commercial dealings 87
Commercial Code, Sittler 199
commercial code traffic 233
commercial code book 203
commercial codes 229, 232
commercial codes, exploitation of 232
commercial codes, publication of 229
commercial codes, traffic in 229
commercial companies 57, 58
Commercial Enigma 236
Commercial Enigma, Analin Fabrib, methods of solution of traffic 234
commercial Enigma machine 234, 238
commercial houses 232
commercial intelligence 203
commercial matters 233
commercial plain text 233
commercial section 198
Commercial Section (B-III-b) 197
commercial system, Italian 105
commercial system, Japanese 233, 243
commercial system, two-digit 177
commercial systems 57, 59
commercial traffic, 57, 198, 230, 231
Commercial Traffic Section 232, 233
commercial traffic, isolation of 229
commercial traffic, Japanese 186
commercial traffic, processing of 229
commercial treaty 36
commercial unit, discontinuance of 230
Commission, Allied Control 110
Commission, Armistice, in North Africa 222
commissioned officers 210
committee 49, 285
Committee, Army-Navy Communications Intelligence Coordinating 288
committee, central 117, 130
committee, coordinating 7
Committee on Terminology 287, 288
committee, working 288
common groups 165
communicate 107
communication 99, 108, 280
communication channels 263
communication, land line 192
communication, principal means of 64
communication, radio 192
communications 24, 31, 135, 144, 244
communications, Axis cryptographic, suspension of 225
Communications Branch 209, 289, 291
communications channels 53
communications, code 108
communications, cryptographic 152, 153

Doc ID: 6554247

communications, Enigma 243
Communications Expert 31
communications from GCCS 183
communications functions 10
communications, German secret 13
communications, Japanese 81
communications, Japanese Army 7
communications, Japanese diplomatic 7
communications, Japanese military attaché 7
communications, radio 291
communications, secret 31, 144, 225, 282
communications, security of 26, 273
communications systems 11
commutator, rotating 32, 40
companies, colonial development 57
companies, commercial 58
companies, Japanese commercial 57
companion codes 144
Company, Chemnyco 238
Company, Eastman Kodak 272, 273
Company, Grey Manufacturing 272
Company, International Business Machines (IBM) 272
Company, National Cash Register 272
Company, Philips Export 226
Comparator, 70-mm 271, 272, 274, 276, 278
comparators 279
comparators, IC 271
comparison 274, 275
comparison of data 239, 277
comparisons 274
compilation 25, 289, 291
compilation bureaus, cryptographic 50
compilation unit, British 12
compilers 143
completness 287
complexities 238
complexity 236
complexity of systems 26
complicating changes 28
complication of machine action 245
component, cipher 72
compromise 85, 86, 306
compromise attempts 298
compromise, data acquired by 252
compromise of code 299
compromised 134, 175
compromised additives 89, 90, 93
compromised code 122, 133, 144, 148, 167, 175, 191
compromised code book 82, 303
compromised code books 7, 84
compromised codes 8, 124
compromised copy 96, 104, 114
compromised cryptographic material 303
compromised documents 297
compromised Iranian codes, photographs of 174
compromised material 85, 92, 295, 300, 302
compromised plain texts 246
compromised Swedish tables 249
compromised system 113, 118, 120
compromised systems 125, 126, 127, 293
compromised tables 252
compromises 298

Doc ID: 6554247

computing of frequencies 211
concessions, weather 216
conditions, broadcast 206
conditions, weather 211, 214
conference in Teheran 77
conference, international 296
Conference, International Aviation 178
Conference on International Organization, United Nations 188
conference on Japanese diplomatic solution 59
Conference, San Francisco 178, 179, 192, 290
conferences, international meteorological 216
confidence 298
confirmation 268, 275
conflicts 43
conflicts in endplate plugging 265
Congress, Library of 173, 174
Connor, Captain John H. 10
conquered territories 57
consecutive series 194
consistency 288
consolidation 130
consonants 29, 85
construction 242, 258, 259, 265, 266, 269, 271, 277
construction of additive 90
construction of analogues 48
construction of the Arlington Autoscritcher 268, 269
construction of indicator keys 96
construction of key 94
Consul 299
consular offices 58, 158
Consular Service, United States 181
consulate, German 85
Consulate, Peruvian 303
consultation 23, 132
Contract File (SPSIF) 257
content 77
context 34
contiguous quarters 185
Continent, the 253, 302
continuation of studies 101
continuity 58, 147, 148
continuity, cryptanalytic 15, 176, 237
continuity, cryptographic 28
continuity of weather types 205
continous dissemination 292
continuous research 289
contracts, research 272
contradiction 268
contradictions 264, 275
contribution 61, 79, 81, 87, 284, 289
contribution of Arlington Dudbuster 266
contribution of British 183, 212
contribution of British, largest 15
contribution of GCCS 183, 201, 202, 254
contribution of Machine Cipher Section 240, 243
contribution of Planning and Priorities Unit 289
contribution of RAM 278
contribution to British 13, 266
contribution to GCCS 239, 279
contributions 79, 173, 206, 260
contributions, British 100

Doc ID: 6554247

contributions of Recorder's Group 287
contributions of Research Section, B-III 281--284
contributions of Special Examination Unit 227
contributions of Signal Security Agency 270
contributions to cryptanalysis 303
contributions to cryptanalytics 286
control 65, 175
control, Allied 110
Control Commission, Allied 110
control, JAS 69
control officers 263
controls, punch 272, 278, 279
Control, Relay, 70--mm. 272
Control Unit (B-III) 289
control units 279
control wheel 30
conversations 228
conversations, radiotelephone, translation of 220, 227, 228
conversations, telephone 220, 228
conversion, method for 42
conversion process 42
conversion squares 66, 71, 75, 78, 243
conversion square 67, 71, 72, 74, 77, 83
Conversion Square, JAS 278
Converter M-209 247
Converter M-325 (SIGFOY) 40
converting 42
Cook, Captain Earle F. 16; (Colonel) 9, 257
Cooley, Mr. Vernon E. 98
cooperating centers 22, 58, 91
cooperation 14, 18, 20, 37, 60, 81, 86, 107, 111, 117, 129, 133, 165, 185
cooperation, Anglo-American 100
cooperation between SIS and EU 18
cooperation, British 17
cooperation of GCCS 57, 243
cooperation with British 138
cooperation with GCCS 263, 264, 277
cooperation with GCCS and EU 137, 290
coopeation with OP-20-G 23
coordinating committee 7
coordination 48
coordination of information 230
copies, faulty intercept 238, 241
copies of British work 169
copies of code books 302
copies, photographic 157, 300, 301
copies, photographs of 301
copy, compromised 96, 114
copy machine 272
Corderman, Colonel W. Preston 20
Coroneas, Lieutenant Praxythea M. (Mrs. L. A. Rutledge) 190--192, 195
corrected message 179
correlation 174, 301
correlation of encipherments 165
correspondence 183
correspondence, diplomatic 46
correspondence, enemy officer's 223
correspondence, Italian diplomatic 111
correspondence of Finnish legation 251
correspondents 30, 226, 227
correspondents, suspect 225

Doc ID: 6554247

correspondents, suspect 225
Cortina d' Ampezzo, attaché in 75
cost of the 003 equipment 265
Costa Rica 148, 152
Costa Rican traffic 148
costs of transmission 229
Coudert, Captain Ferdinand W. 190, 191
count, IC 273
counter electronic 274, 275
Counter Printer, 70-mm.
counters 279
Counting and printing units 279
counting, electronic high-speed 276
counting of coincidences 275, 277
countries 229, 232, 233, 280
countries, Allied 190
countries, Axis 164
countries, foreign 303
countries of Near and Middle East 174
countries, Near Eastern 179
countries, oriental 172
countries, Spanish-American 2
countries, Spanish-speaking 230
country 232
Cournoyer, Miss Madeline 139, 145
course 61, 235
course, introductory 61
course in Portuguese language 164
course of training 211
course, short 163
courses 236, 239, 284
courses in key recovery 73
courses, specialized training 285
court 223
court reporting 221
Coury, Miss Mary Lou 201
cover letter 227
cover name 64
cover names, use of colors as 29
coverage 76, 175, 209, 212, 217, 241, 260
coverage, British 215
coverage, intercept 205
coverage of station TOYOHATA 217
coverage, report on 290
Cox, Miss Noe 126
CPA 185
CPB 185, 189
CPC 185, 189
CPD 185, 189
CPI 189
CPJ 189
Craugh, Miss Margaret J. 173
crib, indicator 267
crib, length of 269
crib material 262
crib messages, isolation of 261
crib, plain-text 282
crib sheets 241
cribs 77, 86, 87, 89, 91, 240, 241, 243, 246, 262, 277, 278, 300, 301
cribs, cross-system 93
cribs, current 244
cribs for unreadable German messages 214
cribs, Hanoi 120
cribs, lack of 242, 265
cribs, out-of-date 238
cribs, partial 74
cribs, plain-text 70, 252
cribs, search for 276
crises, political 137
Croatian 222
Croatian puppet government 180, 193
Croatian systems 191
cross-reference filing system 232
[redacted] . . . .

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

Doc ID: 6554247

cross-section paper 224
cross-system cribs 93
cryptanalysis 4, 10, 30, 47, 111, 115, 127, 169, 170, 173, 175, 186, 191, 238, 257, 261, 262, 280, 285, 293, 300-302
cryptanalysis, American 100
cryptanalysis, contributions to 303
cryptanalysis, Enigma 261, 262
cryptanalysis, Enigma, Methods of 238, 241, 257
cryptanalysis, Enigma, procedures in 236
cryptanalysis, experts in 185
cryptanalysis, Japanese 16
cryptanalysis, machine, course in 235
cryptanalysis, machine, training ground in 251
cryptanalysis, modern techniques 295
cryptanalysis of GEC 300
cryptanalysis of indicators 250
cryptanalysis of Japanese and German diplomatic systems 21
cryptanalysis of Japanese problems 207
cryptanalysis of JBH 243
cryptanalysis of machine ciphers 235
cryptanalysis of Swiss systems 118
cryptanalysis of systems 286
cryptanalysis of weather traffic 207
cryptanalysis, practical 302
cryptanalysis, training in 101
cryptanalyst 33, 34, 36, 82, 255, 272
cryptanalyst, American 46
cryptanalyst, mature 296
cryptanalysts 4, 25, 30, 38, 47, 50-52, 57, 61, 79, 82, 88, 90, 91, 95, 98, 100, 109, 114, 132, 143, 149, 173, 180, 184-186, 191, 202, 235, 240, 268, 280, 284, 287, 295, 297, 300, 301
cryptanalysts, Army 234
cryptanalysts, British 137, 212
cryptanalysts, British, collaboration with 177
cryptanalysts, Canadian 137
cryptanalysts, original 24
cryptanalytic achievements 66, 93
cryptanalytic activities 16, 295
cryptanalytic activities, B-III, exhibition of 240
cryptanalytic activity 98
cryptanalytics, advancement of 281
cryptanalytic aid 294
cryptanalytic aides 200
cryptanalytic attack 11, 69, 239, 282, 296
Cryptanalytic Branch 8, 9, 10, 11
Cryptanalytic Branch, General 11, 24, 82, 130, 232, 270 280, 284-286, 288, 295, 299
Cryptanalytic Branch, Military 11, 102, 103, 119, 124, 133, 284
Cryptanalytic Branch, organization 10
cryptanalytic centers 58, 263
cryptanalytic continuity 15, 176, 237
cryptanalytic data 286

Doc ID: 6554247

cryptanalytic development 194
cryptanalytic devices 201
cryptanalytic discoveries 59
cryptographic documents 298
cryptanalytic equipment 271
cryptanalytic examination 150
cryptanalytic field 100
cryptanalytic group 263, 264
cryptanalytic history 253
cryptanalytic information 15, 91, 290
cryptanalytic information, interchange of 18
cryptanalytic liaison with the British 11
cryptanalytic literature 288
cryptanalytic-machine time 23
cryptanalytic machinery 76, 284
cryptanalytic machines 285
cryptanalytic material 16, 77
cryptanalytic materials 242, 286
cryptanalytic means, solution by 111, 205, 295
cryptanalytic mechanized procedures 282
cryptanalytic methods 286
cryptanalytic operation 115
cryptanalytic operations 7, 295
cryptanalytic personnel 81, 237, 260, 263
cryptanalytic phases of work 159
cryptanalytic problem 179, 258, 277
cryptanalytic problems 47, 66, 76, 154, 173, 177, 191, 193, 243, 287
cryptanalytic problems, Chinese 184
cryptanalytic procedures 236, 259
cryptanalytic production 250
cryptanalytic progress 163
cryptanalytic projects 1
cryptanalytic research 139, 191, 193
cryptanalytic purposes 271
cryptanalytic relations between systems 286
Cryptanalytic report No. 2 234, 257
cryptanalytic requirements 302
Cryptanalytic (B) Section 3, 4, 5, 6, 10
Cryptanalytic Section, Enigma 261
Cryptanalytic Section, General 130
cryptanalytic sections 230, 290
Cryptanalytic Series 169
cryptanalytic skill 156
cryptanalytic staff 185, 187, 194, 213
cryptanalytic studies 38
cryptanalytic study 19, 178
cryptanalytic success 8, 300
cryptanalytic task 55
cryptanalytic techniques 5, 33, 77, 134, 180
cryptanalytic tool 277
cryptanalytic training 61
Cryptanalytic Unit 89, 132, 160, 180, 185, 194

Doc ID: 6554247

cryptanalytic units 2, 156, 157, 235, 289 291, 293, 294
cryptanalytic units, British 12
cryptanalytic work 78, 286, 292
cryptanalytics 285
cryptanalytics, contributions to 286
cryptogram, Hagelin, first solution of 251
cryptograms 38
cryptograph 46
cryptograph, Finnish use of 249
cryptograph, Hagelin, insecure use of 255
cryptograph, "Red" 45
cryptographed traffic, Lebanese 178
cryptographers 296
cryptographers, Finnish 300
cryptographic art 51, 52
Cryptographic Branch 254
cryptographic bureaus 108
cryptographic changes 242
cryptographic communications 152, 153
cryptographic communications, suspension of Axis 225
cryptographic compilation bureaus 50
cryptographic continuity 28
Cryptographic Description of the "88.." System 62
cryptographic details 192
cryptographic devices 301
cryptographic documents, captured 297
cryptographic elements 44
cryptographic habits 25
cryptographic habits of the Italians 101, 111
cryptographic history, Italian 102
cryptographic improvement 66
cryptographic information messages 291
cryptographic instruction 61
cryptographic instruction messages 28, 55, 72, 89
cryptographic instructions 95
cryptographic intelligence 60
cryptographic laws 43
cryptographic machine 13
cryptographic machine, German Enigma 13
cryptographic machinery 281
cryptographic machines, Japanese 45
cryptographic material 219, 302
cryptographic material, captured 110
cryptographic material, compromised 303
cryptographic materials 75, 107, 108, 300
cryptographic materials, Finnish 251
cryptographic materials, U. S. State Department 77
Cryptographic Material Branch 281
cryptographic mechanisms 29
cryptographic messages out of Buenos Aires, ban on 252
cryptographic method, grouping of subsections in accordance with 153
cryptographic methods, Greek 301
cryptographic paraphernalia 31

Doc ID: 6554247

cryptographic period 251
cryptographic periods 250
cryptographic personnel 297
cryptographic phenomena 44, 45
cryptographic problems 28
cryptographic procedure, German 303
cryptographic properties 60
cryptographic relationship 34
Cryptographic (C) Section 3, 4
cryptographic similarities 39
cryptographic structure of JAS 64
cryptographic system 50, 84, 296
cryptographic system, solution of German Foreign Office 88
cryptographic systems 1, 51, 139, 153, 196, 286
cryptographic systems, foreign 291, 295
cryptographic systems, Italian 98, 103
cryptographic techniques 51
cryptographic terms, dictionary of 288
cryptographic text 43
cryptological units 221
cryptographs 40
cryptography 4, 45, 50, 54, 63, 169, 303
cryptography, Balkan 181
cryptography, Brazilian 169
cryptography, changes in 76
cryptography, Finnish habits of 250
cryptography, Hagelin 252
cryptography, Japanese, changes in 277
cryptography, Japanese diplomatic 26
cryptography, Japanese diplomatic 26
cryptography, JAS 66
cryptology, literature of 287
cryptography of "A" Machine 32
cryptography of system 69
cryptography, Swiss 141, 143
cryptonet 266
cryptonets 262, 265, 267, 268
cryptonets, Army 267
cryptonets, German 260
CUA 159, 294, 303
CUB 150
Cuba 159
Cuban ciphers 150
CUD 150
current cribs 244
current intelligence 91
current material 28
current priorities 290
current solution 2
current systems, solution of 1
current traffic 63, 87, 210, 241, 244, 262, 264, 265
customs of the country 222
CTA 193
CTB 193
CTX 302
CTX-1 133
CV (FAV) 124
cycle 32, 33, 39
cycles 248
cyclic interruption 249
cyclic repetition 3
cyclic sequences 41, 43
cyclic wheels 276
cyclically-repeating keys 40

Doc ID: 6554247

cyclically-repeating sequences 40
Cyrillic alphabet 64
CZA 195
CZB 194, 195
CZD 195
Czech 191
Czech systems 191, 194
Czech systems, researches on 195
Czechoslovakian government in London 180
"D" net message 242
D period traffic 71
D Section (Secret Ink and photographic Laboratory) 3
DA 27
daily additive key 122, 135
daily indicator 83
daily indicator keys 85
Daily Information Bulletin 286
daily keys 242, 250
daily strip system 121
Dakar 211
Dakar station 211
Dakar traffic 211
Damascus 178
Damascus-Ryadh-circuit 178
Daniels, Miss Eloise E. 231
date 53, 141
date, "B" Machine effective 31
Davidson, Mr. Hugh 148, 150, 152
Davis, Miss Ann 147, 159
Davis, Miss Marcella 207, 213
Dawson, Corporal Ruell E. 118; (Sergeant) 236
DE (FAE) 124
decipher of message 47
deciphered 120, 154, 167, 212
deciphered material 195
deciphered messages 26, 71, 73, 193
deciphering 4, 94, 115, 156, 186
deciphering by hand methods 81
deciphering chart 33
deciphering machines, electromechanical 73
deciphering of messages 13
deciphering tables 192
decipherment 45, 158, 241, 248, 253, 264
decipherment, daily 45
decipherment, methods of 252
decipherment of messages 227, 251, 252
decipherment of shorthand notes 223
decipherments 73, 237
decision, War Department 11
declaration of war, Syria's 178
decline in requirements of Section III 9
decode 159, 182
Decode Unit 116, 128, 129, 131, 156, 159
Decode Unit, French 112, 128, 129
decoded messages 35, 49, 71, 116, 165, 203
decoded traffic 159
decodement 143
decodements 119, 120, 137
decoders 163
decoding 4, 87, 105, 115, 116, 128, 134, 137, 156, 159, 164, 231
decoding activities 56
decoding by hand methods 81
decoding, delay in 49
decoding, French 293
decoding, IBM 87
decoding messages 294
decoding methods 92

Doc ID: 6554247

decrypting of CNH 184
decoding of JBC messages 60
decoding, spot 137
decryptographed messages 185
decryptographers 294
decryptographing 6, 132, 249
Decryptographing and Transposed Code Solution Unit 54
decryptographing group 137
Decryptographing Unit abandonment of 293
Decryptographing Unit (B-I-C) 106, 292, 294
decryptographing work 6
deduction 84
Deeter, Captain C. R. 269
defense of the United States 50
defense plant, suspicious document found in 223
deficiencies, linguistic 172
deficiency of translators 14
definitions of terms 287
DeGray, Mr. Julian 149, 150, 154, 157
DeGomar, Lieutenant Theodore F. 162, 208
delay 302
delay in decoding 49
delayed messages 218
delayed reports 217
delayed WAC program 263
delays 37
delegation, Turkish 177
delegations, Japanese, uncooperative attitude of 216
demonstration 258, 259
Denniston, Commander A. G. 16--18
Department, Hawainan 82
Department of Military Intelligence 227
depth 133, 134, 212, 218, 244, 284
depth, message in 158, 255
depth, placed in 71
depth, traffic in 120
Derbyshire, Lieutenant Lowell G. 101; (Captain) 103--105, 132, 162, 164; (Major) 101
derivation of basic additive key 85
derived additive from GEC-GEE isologs 90
DESAB Code Book No. 3 82, 83
DESAB, first translation 96
DESAB, reconstruction of 96
Description of JAS 62
description of systems 289
descriptions 76
descriptions of systems 24
design 275
designs 260, 284
designs for RAM equipment 283
destruction of equipment 260
destruction of material 297
destruction of personnel 260
detached service 228
details, cryptographic 192
detection 297
Deutsch, Miss Rosamund 120
Deutsches Satzbuck 82

Doc ID: 6554247

development 33, 44, 47, 55, 87, 134, 178, 203, 243, 258, 271, 274, 276, 278, 302
Development Branch 237, 243, 264, 268, 270, 272
Development Branch, engineers of 269
development, cryptanalytic 194
development of Arlington Autoscritcher 268
development of Arlington Dudbuster 266, 270
development of Hagelin cipher machine 247
development of Hagelin techniques 247, 248
development of JAM 56
development of machine methods 268
development of new techniques 72, 283
development of Purple machine 277
development produced by reflector 242
development, RAM 277
development, research and 51
development sheets, JAA 59
developments 259, 286
developments, Hagelin 247
Devenney, Miss Maude 229-230
device 282
device, electrical 144
devices, cryptanalytic 201
Dewey, Governor 50
DG 27
diaries 24
diaries, enemy officer's 223
diaries, personal, captured 222
diary 62, 292
diary of a German Officer 222
Diccionario Cryptographico 303
Diccionario do Cifra de Ministerio dos Negocio Estrangeiros 302
Dickinson, Mrs. Velvalee 227
dictionary of cryptographic terms 288
dictionary of the Thai language 189
Dictionary of United States Army Terms 288
differences, listings of 201
difficulties 35, 228
difficulty of the work 222
Digepol 106
digit 135, 279
digit codes, Vichy French 114
digit systems, Chinese 187
digits 58, 218
digits, additive 89
digits, groups of six 214
digits in synoptic 204
digraph 74, 142
digraphic chart 64
digraphic coincidences 271
digraphic substitution 65, 135, 178, 188
digraphic substitution ciphers 178
digraphic-substitution encipherment, Italian 105
digraphic substitution system, Funchal 106
digraphic substitution system, Port au Prince 83
digraphic substitution systems, Japanese 26
digraphic substitution tables 184, 192, 195
digraphic substitutions, solution of 101
digraphs 53, 141, 283
digraphs, code 71

Doc ID: 6554247

digraphs, plain 62
digraphs, plain-text 24
Dill, Field Marshal Sir John 259, 260
Diller, Dr. Aubrey 184, 190
Dillinger, Mr. Norman 114, 119-121
diphthong 35
diplomatic agent, German 82
diplomatic and consular code, Spanish 298
diplomatic cipher system 203
diplomatic code 165
diplomatic doe, most secret 177
diplomatic code, Portuguese 167
diplomatic codes 109, 187
diplomatic codes, Italian 109
diplomatic communications, Japanese 7
diplomatic correspondence 46
diplomatic correspondence, Italian 111
diplomatic Hagelin messages, Swedish 273
diplomatic heading 233
diplomatic information 58, 232
diplomatic intelligence 203
diplomatic language, Japanese 61
diplomatic machine 30
diplomatic machine, high-security 13
diplomatic machine, "Red" 30
diplomatic matters 47
diplomatic messages 146, 203
diplomatic missions, German 83
diplomatic negotiations 109
diplomatic net, Spanish 157, 158
diplomatic offices, Japanese 31
diplomatic plain text 233
diplomatic pouches 297
diplomatic pressure 211
diplomatic problems, Japanese 54, 58
diplomatic Purple machine messages, Japanese 277
diplomatic relations 179
diplomatic representative 147
Diplomatic Section, German 2, 82, 88, 90
Diplomatic Section Italian 2
Diplomatic Section, Japanese 2
Diplomatic Section, Mexican 2
Diplomatic Section of GCCS, Italian 102
diplomatic sections, British 17
diplomatic solution, German 82
diplomatic system 50, 158, 178, 187
diplomatic system, Japanese 274
diplomatic systems 19, 20, 23, 55, 56, 62, 166, 219, 233, 290, 297, 299
diplomatic systems, German 21, 82
diplomatic systems, Iranian 301
diplomatic systems, Italian 105
diplomatic systems, Japanese 15, 21, 22, 24-26, 28, 30, 54, 57, 61, 284
diplomatic systems, Japanese enciphered code 283

Doc ID: 6554247

diplomatic systems, Polish 195
diplomatic traffic 2, 197, 205, 206
diplomatic traffic, Italian 98
diplomatic traffic, Japanese 28, 48
diplomatic transactions 87
diplomatic work, Japanese 21, 22
diplomatic work at GCCS, Japanese 59
direct method 301
direct symmetry 66
direction, technical 2
directions, German Hagelin machine 303
directives 1, 2, 3, 6
Director of Brooklyn Museum 181
Director of Communications Research, SSA 257, 258, 298
Director of Military Training, Office of 287, 288
Director of MIS 92
Director of Training 131
Direzione Generale di Polizia 106
discoveries 300
discoveries, cryptanalytic 59
discoveries, early 90
discovery 90
discovery, initial 90
discriminant 82, 231
discriminant, four-digit 63
discriminant list 264
discriminants 114, 141, 262
discriminants, allocation of 262, 265
discriminants, research on 261
discussions 258
dispatches, press 221
displacement 146
dissemination, continuous 292
dissemination of information 289
dissolution 116
dissolution of the South American Section 149, 221
distribution 35, 37, 50, 246, 297, 300
distribution, key 255
distribution of documents 280
distribution of traffic 290
distribution tables 42, 43
distributions, frequency 130, 244
disturbances, atmospheric 205
divided arrangement 156
division of function 7
division of responsibility 19
divisional units 109
Dixon, Lieutenant George 276
DN-1 (FAP) 302
DO (FAC) 124
DOA 150
Doane, Miss Elizabeth S. 102, 104, 106, 132
document 36, 38, 160
document found in defense plant 223
Document Section 292
document, suspicious 223
documentary material 292
documents 37, 62, 112, 139, 223, 224, 234, 280
documents, accounting for 280
documents, captured 94, 95, 111
documents, captured stenographic 221

Doc ID: 6554247

documents, captured stenographic 221
documents, catalogging of 280
documents, compromised 297
documents, cryptographic 297, 298
documents, distribution of 280
documents found in baggage of enemy agents 223
documents, German stenographic 222
documents, listing of 224
documents on file 24
documents passing through Military Censorship 223
documents, processing of 220, 223
documents, questioned 150
documents, reading of stenographic 220
documents, registration of 292
documents, stenographic 220
documents, stenographic, transcribing of 220
documents, transmission of 22
Domei broadcasts 226
domestic net, Japanese 22
dominant letters, system of 168
Dominican cipher traffic 149
Dominican ciphers 150
Donahue, Lieutenant Charles J. 183, 236, 248, 249; (Captain) 261
Donahue, Miss Mary 206
double additive encipherment system, Japanese Army 285
double encipherment 83, 84, 86
double film gates 276
double input method 265
double transposition 179, 194,
Doud, Lieutenant Colonel Harold 4, 6
Downey, Lieutenant Glanville 104, 171
DQ (FAD) 124
DR code (FAE) 125
Dragon machine 239, 277
Dribin, Dr. Daniel M. 118; (Sergeant) 201, 203, 236, 281
Dronenburg, Miss Hazel 48
drudgery 224
drums 158
Dryo (CNB) 182
DS (FAF) 124, 125
DT (FAG) 124, 125
Dubberstein, Dr. Waldo H. 62, 80
Dublin 83, 95
Dubois, Kathryn (Buffham) 62
dud messages, solution 266, 267
Dudbuster, Arlinton, 266, 270
duds 266, 269
"Duenna the" 269
Duke, Lieutenant Francis 104, 106; (Captain) 111
Dumey, Lieutenant Arnold I. 250, 251, 254, 255
Dunn, Miss Jane E. 173
Dunn, Miss Mary 163
Dunning, Miss Mary Jo 48
Dunwell, Lieutenant Stephen 248
duplicate encipherments, suppression of 39
duplication, avoidance of 14
duration of the War 280

Doc ID: 6554247

Dutch government 247
duty, temporary 19
duty, tour of 22
duty with Naval Section GCCS 21
DV (FAH) 124
DX (FAI) 124, 125
DX code, Vichy 122
E-5 122
E-5, Colonial 120
E Branch 10, 262
"E" operations, British 13
E-period traffic 70, 71
E Section 5, 6
early days 83
early discoveries 90
Early, Miss Jeannette 118, 236, 263
early work 24, 62, 82, 98
East Africa 106
East Indies, Netherlands 216
Eastman Kodak Company 272, 273
echelons, highest 109
Economic Administration, Foreign 232
economic data 58
economic information 243
economic situation of the enemy 229
Ecuador 152
Edgerton, Captain William F 112, 119, 124, 197, 229; (Major) 131, 132
editing of traffic 174
editing, rapid 210
"Eel" system 122
effective date for "B" Machine 31
efficiency 81, 289
effort required for solution 296
EGA 170
Eggs Catalog 242
Egleston, Corporal Oliver F. 171; (Sergeant) 170, 173, 176
Egypt 170, 177, 232
Egyptian systems 174, 175
Ehninger, Mrs. Flobeth 173, 175, 199
Eire, systems of 197
electrical device 144
electrical means of scritching 243
electrical techniques 15
Electromatic typewriters, remote operation of 272
electromechanagrammer 53, 155
electromechanical deciphering machines 73
electromechanical machines 236
electronic counter 274, 275
electronic counting, high-speed 276
electronic machine 270
electronic model 258
electronic techniques 15
electronics engineer 276
elements 33, 50, 57, 66, 68, 79, 90, 302
elements, cryptographic 44
elements of key 266
elements of machines used 90
elements of system, change of 297
elements of text 73, 277
elements, of weather 204
elements, related 300
elements, transposition of 99
Ellis, Dr. Lowell B. 149, 154, 157
Ellison, Lieutenant Reuben Y. 114, 119
Elmquist, Mrs. Anne M. 191, 195

Doc ID: 6554247

Elmquist, Lieutenant Karl 189
Ely, Miss Elenor 163
embassies 158
embassies, Japanese 31
embassies, Spanish 157
embassies, Turkish 178
emergency solution 7
emergency, training for 1, 28
Emerson, Dr. Helen 140
encipher 157
enciphered 32, 84, 85, 108, 129, 217
enciphered additive 148
enciphered by additives, codes 116
enciphered by substitution 188
enciphered Chinese code system 184
enciphered code 4, 64, 115, 144, 195, 177, 198, 202, 212
enciphered code system 158, 203, 296
enciphered code systems 18, 183, 189
enciphered code systems, Japanese diplomatic 283
enciphered code, tetranomic 144
enciphered code text 65
enciphered code, trigraphic 144
enciphered codes 107, 121, 165, 168
enciphered groups 214
enciphered, highly 192
enciphered identically 3
enciphered indicators 69
enciphered key text 252
enciphered messages 72, 273
enciphered, messages, in same key 218
enciphered messages, methods of solution 275
enciphered systems 105, 219
enciphered trigraphic code 175
enciphering 94, 205
enciphering keys 122
enciphering messages 26
enciphering process 50
enciphering squares 275
encipherment 52, 62, 65, 78, 83, 88, 90, 95, 96, 101, 105, 108, 116, 124, 126, 129, 134, 135, 144-146, 165, 168, 175, 178, 187, 190, 200, 202, 203, 209, 216, 219, 244, 266, 267, 282, 294
equipment, accessory RAM 278
encipherment, additive 8, 114, 115, 118, 133, 137, 151, 178, 188, 278
encipherment additive and substitution 188
encipherment, double 83, 84, 86
encipherment, first Polish code to be cleared of 195
encipherment, French transposition 130
encipherment in pairs 135
encipherment,indicator 63, 85, 134, 158
encipherment, indicator, solution of 158
encipherment, instructions concerning 17
encipherment, Italian additive 105
encipherment, Italian digraphic-substitution 105
encipherment, JN-36 218
encipherment, JN-37 218
equipment, modification of 276
encipherment of Chinese systems, solution of 180

Doc ID: 6554247

encipherment of letters 282
encipherment POB 166
encipherment, polyalphabetic 186, 203
encipherment, problems of 101, 131
equipment, RAM 283
encipherment recovered 128
encipherment, removal of from weather reports 205
encipherment, secondary 167
encipherment, simple 152
encipherment, single 252
encipherment, solution of 7
encipherment, substitution 118, 144, 195, 214
encipherment, systems of 111
encipherment, text 83
encipherment, transposition 137, 187
encipherment unit, additive 7
encipherments 62, 136, 166, 167, 170, 175, 186, 187, 193, 201, 214
encipherments, additive 101
encipherments, change in 185
encipherments, Chinese 183, 194
encipherments, CNL 185
encipherments, code 5
encipherments, correlation of 165
encipherments, identical 39
encipherments of Thai 190
encipherments, series of 168
encipherments, solution of 7, 132, 231
encipherments, spelling 185
encipherments, substitution 114
encipherments, superimposed 184
encipherments, suppression of duplicate 39
encipherments, transposition 129, 188
encode 105, 108
encode captured 128
encoded messages 65, 136, 141, 178
ending, inflectional 143
endplate plugging 237, 238, 243, 244, 264, 267, 268
endplate plugging and reflector wiring, simultaneous recover of 267
endplate plugging, conflicts in 265
endplates, pluggable 282
enemy 52, 205, 223, 268
enemy agents, documents found in baggage of 223
enemy, economic situation of 229
enemy lands 229
enemy machine ciphers 284
enemy materiel 92
enemy meteorological traffic, solution of 206
enemy officer's correspondence 223
enemy officers' diaries 223
enemy systems, attacks on 282
Engel, Mr. A. Ferdinand 98-101, 103, 107, 125, 189
engineer, electronics 276
engineer, radar 276
engineer, Swedish 247
engineering 257
engineering problems 48
engineering survey 258
engineers of Development Branch 269
England 17, 18, 20, 37, 236, 240, 241, 259, 260, 263, 264, 276, 280
England, Mr. Friedman's missions to 12

Doc ID: 6554247

England, Sinkov-Rosen Mission to 11
English 139, 156, 182, 189, 222, 227, 233, 253
English book 253
English code 25, 187
English form 143
English, French to 127
English language codes 230
English messages 225, 231
English plain text, fragments of 253
English-speaking governments of the Far East 143
English Spelling and Vocabulary 27
English Spelling CA 27
English Spelling JE 27
English Spelling PA 27
English systems 170
English text 36,47
English-text messages 37, 41
English versions 131
Enigma 40
Enigma, Armistic Commission 245
Enigma cipher machine 146
Enigma commercial 236
Enigma communications 243
Enigma cryptanalysis, methods of 238, 241, 257, 261, 262
Enigma cryptanalysis, procedures in 236
Enigma Cryptanalytic Section 261
Enigma frames 258, 266, 267
Enigma, German 13
Enigma, German Abwehr 234, 236, 238, 246
Enigma,German Abwehr, analysis of 240
Enigma, German Military 234, 236
Enigma, German Naval 260
Enigma machine 238, 244-246, 260, 264
Enigma machine, commercial 234, 238
Enigma machine, German 273
Enigma machine, three-wheel 258
Enigma, Military 237, 244
Enigma operations 260, 269
Enigma problem, German 257, 269
Enigma problems 267
Enigma research 267
Enigma Section of GCCS 261
Enigma solution 13, 269
Enigma, Swiss 238
Enigma, Swiss, messages enciphered by 237
Enigma systems 284
enlisted 9
enlisted men 162, 172, 207-209, 273
enlisted women 273, 276
enlisted personnel 10, 264
entries 174
entry 70, 79, 87, 90, 99, 141
entry, initial 69
entry into Finnish systems 249
entry into JAM 55
entry into JAS 70
entry into LBA 203
Epilogue: Summer 1944 107, 109, 110
equipment 237, 257, 266, 274, 275
equipment, 003 265, 269
equipment, 35--mm. film 279
equipment, 70--mm. 279
Equipment Branch, SSA 272, 273, 277, 281
Equipment Branch, SSA, Chief of 257
equipment, destruction of 260
equipment, German 77
equipment, high speed cryptanalytic 271

Doc ID: 6554247

equipment IBM letter writing 278
equipment, IC 273, 279
equipment, list of 272
equipment, RAM 272—274
equipment, RAM, modification of 275
equivalent, plain 141, 142, 219, 226
equipment, teletypewriter tape 272, 278
equivalents, cipher 43, 165
ERIKO 217
error, cause for 290
error, margin of 271
Erskine, Miss Mildred 206
Esperanto 222
espionage 96, 227
espionage agents 295, 299
espionage, assistance from 295
espionage, reports on 150
ETA 170
ETB 170, 179
Ethiopia 170, 177
Ethiopian system 179
ETOUSA 265
EU 18, 19, 22, 60
EU, assistance from 138
EU, exchange of information with 290
EU, liaison with 289
EU, requests from 290
Europe 53, 76
Europe, Central 180
Europe, Middle 180
European centers 252
European circuits 161
European governments 190, 215
European languages 222
European points 200
European powers 12
European stations 107
European systems, Middle 181
European tongues 173
evaluation of British contribution 14
evaluation of priority 290
evaluation, photoelectrical 271
Evans, Sergeant Gwyn 54
Evans, Mr. Robert 148, 150
Evening Star, Washington 48
Everett, Corporal Paul 123
Ewing, Sergeant Gerrett L. 114
"EX" Code 27
examination 268
examination of Japanese weather reports 207
examination of material 224
examination of new messages 231
examination, preliminary 183
Examination Unit (EU) 18
exchange 60
exchange of ideas 281
exchange of information 20, 22, 58, 78, 91, 102
exchange of information with GCCS and EU 290
exchange of jobs and solutions 263
exchange of material 16, 18
exchange of material with GCCS 179
exchange of military information with the British 11
exchange of telegrams 22
exchange, routine 16
exchanges with British 176, 183, 193
exchanges with GCCS 186, 193, 237, 263, 264
Executive Officer, B-III 289
Executive Officer, SIS 16
exhibition of B-III cryptanalytic activities 240
expansion 8, 114, 162, 171, 176, 179, 276

Doc ID: 6554247

expansion of Signal Intelligence Service 149
expenditure, authorization of 258
expenditure of time 295
expense, telegraphic 29
experience 19, 71, 74, 79, 102, 136, 163, 171-173, 177, 184-186, 191, 207, 280
experience of the British 212
experimental Enigma frame 258
experimental period 263
experimental relay frame 258
experimentation 39, 258, 268
experimentation in method 183
experiments 74, 218, 269
expert 207
expert, in Chinese 181
expert in Finno-Ugrian languages 250
expert in stenography 221
expert, technical 206
expert in Thai 189
expert in Turkish 171
experts 172, 227
experts in Chinese 185
experts in cryptanalysis 185
experts in Finnish 250
experts, Japanese 35, 81
experts, linguistic 180, 210
experts, supervision of 273
experts, well-trained 164
explanation of Chinese encipherments 183
exploitation 55, 56, 87, 203, 237, 244, 254, 259, 260, 294, 300, 301, 302
exploitation of commercial codes 232
exploitation of GEE 285
exploitation of JAH 233
exploitation of JE codes 284
exploitation of systems 28
exploitation of traffic 233
exploitation of TUH 177
exploitation of unread messages 91
exploration of Chungking System 186
exploratory work 82
exposures 284
exposures, multiple 275
extracts, file of 222

F Franch 281
Fabian, Mr. Donald L. 147, 149, 150, 152
FAC 114, 124, 127, 128, 137, 294, 302
facilities, intercept 205, 209
facilities, teletype 210
FAD 114, 124, 125, 127, 128, 294, 302
FAE 114, 124, 125, 127, 128, 294
FAF 114, 124, 125
FAG 114, 124, 125, 127, 129, 294
FAH 114, 124, 127, 128, 137, 294, 302
FAI 114, 124, 125, 135, 137
failures of the Signal Security Agency 287
FAL 125
Fall of Bucharest 203
fall of France 85
FAM 125, 294, 302
FAN 125, 129, 294, 302
Fanning, Miss Margaret 140
FAO 118, 125, 127--129
FAP 302
Far East 107, 108, 137, 180, 219
Far East, English-speaking governments of 143
Far Eastern field 187
Far Eastern problems 14
Far Eastern Subsection 184
Far Eastern systems 180
Far Eastern Unit 181

Doc ID: 6554247

Farricker, Lieutenant Richard 262
Fascist government, Republican 108, 110
FAT 125, 127
FAU 125
faulty indicators 266
faulty intercept copies 238, 241
FAV 113, 124, 125, 127, 128, 294, 302
FBB 118, 125
FBI (Chinov) 120
FBI, the 19, 82, 85, 88, 92, 93, 165-167, 226, 227 238, 301-303
FBM 114, 120, 133, 134
FBN 120
FBO 120
FBP 120
FBQ 120
FBR 120
FBT 113, 125, 127, 128 294
FBU 125, 127, 128, 294
FBX 125, 128
FCB 134, 302
FCD 135
F. D. R's memorandum for General Marshall 17
FEA 125
Feinstein, Mrs. Genevieve G. (Miss Genevieve Grotjahn) 129, 140, 235, 248, 280, 281
"FELIX" system 96
Fennel, Miss Mary 190
Ferguson, Lieutenant Talbot O. (WAC) 122
Ferner, Mr. Robert O. 21, 29, 48, 53, 82, 140, 235, 236, 248, 269, 280
FES 125
FFA 123, 126, 134, 138
FFB 123, 134
FFC 121, 122
FFD 123
FFE 123, 130, 134-136
FFF 123
FFW 136
FFY 133, 135, 136
FIA 254, 255
FIB 255
FID 252
"Fido" system 123
FIE 253, 256
field unit 219
FIF 252, 254, 255
FIG, solution of 253
file 82
file, biographical 174
file of correspondence of Finnish legation 251
file of extracts 222
file of progress reports 204
file of traffic 202
file, on 298
File on the 003 in SPSIB-3 257
files 36, 292
files, B-III 300
files, MI-8 24
files of Signal Security Agency 229
files, State Department 38
Files Unit 82
filing 191, 231
filing of traffic 193
filing system, cross-reference 232
film 274
film, 35--mm. 274
film, 35--mm., equipment 279
film gates, double 276
film projectors, IC 275, 279
film projectors, methods of using 276
film, recording on 267
films 239, 276
financial systems 187
Finland 177
Finland, negotiations with 252

Doc ID: 6554247

"finnery" 249
Finnish 247, 300
Finnish-American relations, rupture of 251
Finnish college 254
Finnish cryptographers 300
Finnish Embassy 300
Finnish, experts in 250
Finnish government 247
Finnish Hagelin machine, analysis of 235
Finnish habits 250
Finnish language 253
Finnish language notes 255
Finnish Legation 251, 254
Finnish machine cipher systems 300
Finnish messages 274
Finnish plain text, study of 249
Finnish-speaking commities 254
Finnish systems 249, 252, 256
Finnish techniques 300
Finnish traffic 249, 255, 300
Finnish transposition system, solution of 256
Finno-Ugrian languages, expert in 250
Finns, the 251,
FIR-2, solution of 256
Firestone, Mr. Willie J. 255
firm, British 94
Fiscal Year 1943, the 8
Fish, Mrs. Gordon T. 140
Fish, Captain Gordon T. 102, 103, 151; (Major) 10, 104, 140
Fish, Mrs. Jeanne S. 114, 123
five-digit additive 108
five-digit group 174
five-fold card 71
five-letter groups 65
five-letter system, Brazilian 160
five-wheel Hagelin, C-36 247
fixed reflector 258
flag analysis, method of 239
Fleischman, Lieutenant William 207, 215
flexibility 260
flexibility of RAM 278
"Floradora" system, solution of 83
Florida, Tyndall Field 207
fluidity, policy of 163
FMA 122, 134
FMB 121, 122
FMC 122, 126, 129
FMD 121, 122, 134
FME 121, 122
FMF 121, 122, 133, 135, 136
FMH 122
FMJ 133
FMN 133, 137
FMO 138
FMP 135, 136
FMP-A 136
FMP-B 136
FMP-C 136
FMS 133, 138, 302
FMV 135, 137
FMX 133, 137
forces, American 260
forces, armed, United States 297
forecasting of weather conditions 204
Foreign Affairs, Italian Ministry of 108
foreign countries 303
foreign cryptographic materials 107
foreign cryptographic systems 291, 295
Foreign Economic Administration 232

Doc ID: 6554247

foreign intercept sources 217
foreign language 222, 228, 231, 301
Foreign Office 95
Foreign Office, British 95
Foreign Office, Chinese 187
Foreign Office code, trigraphic 188
Foreign Office, Japanese 31
Foreign Office systems, Chinese 188
foreign systems 11
format 301
forms, grammatical 25
forms, Japanese weather report 216
forms, variant 195
Fort Monmouth 163
four-digit discriminant 63
four-digit groups 63
four-letter code 26
four-letter code groups 25
Fowlkes, Miss Jacquelin 221
Fox, Miss Aubrey V. 231
fractionating cipher 245
fractionating device 245
frame, Enigma 258, 267
frame, experimental relay 258
frames 269
frames, 003, rewire of 267
frames, bombe 265
frames, bombe, completion of 264
frames, bombe, maintenance of 264
frames, Enigma 266
frames, X68003 258, 259
France, fall of 85
France, Radio Intelligence Section, General Staff 221
Francis, Miss Mary B. (Mrs. Vandenberg) 123
Franco regime 157
"Fraco" system 123
Frank, Lieutenant John V. 231
Frazier, Private Stuart W. 102
Free French additive system 133
Free French Government 123
Free French Systems 122, 123, 137, 138
Free French traffic 121
Free French transposition system (FMC) 121
French 116, 130, 131, 139, 140, 156, 163, 178, 222, 233
French Additive Recovery Unit 116
French Additive Solution Unit 7
French additive system, Free 133
French agent 85, 86, 92
French armies 222
French (B-4) 4
French Cipher Unit 115, 117--119, 129
French coast 77
French code 127
French Code Reconstruction Unit 7
French Code Recovery Unit (B-III-a-1) 116, 124, 126, 139, 140, 145, 151, 197, 198
French codes 17, 18
French colonial additive systems 119
French consulate at Los Angeles, photographs from 127
French Decode Unit 112, 128, 129
French decoding 293
French Decoding Unit 7

Doc ID: 6554247

French digit codes, Vichy 114
French diplomatic systems 17
French enciphered code systems, Vichy 118
French government 247
French Government, Free 123
French governmental traffic 130
French Government, Vichy 116
French governments 112
French group 293, 294
French Indo-China 137
French keys 17
French language 6, 125 126, 197
French materiel 222
French messages 116, 127, 128
French messages, solution of 211
French military B-211 244
French military cipher 135
French military machine cipher 245
French Military Mission 135
French Mission 123
French Mission systems 122
French plain text 126
French problems 112, 115, 119, 131, 132
French Section 112, 116, 117, 126, 129-132, 138 140, 150, 155, 197, 247 294, 302
French Section, achievements of 115
French Section, breaking up of 128
French Section, consolidated 131
French specialists 114, 139
French Spelling and Vocabulary 27
French systems 19, 22, 113, 114, 128, 132, 147, 170, 294
French Systems, Free 122, 123, 137, 138
French, systems using 293
French SZM 144
French, the 128, 222, 245, 302
French to English 127
French traffic 4, 112, 115, 128, 130, 137, 199, 211
French traffic, Free 121
French traffic, Vichy 207
French translation 6
French Translation Unit 7, 116, 126-128, 155
French translations 140
French Transposed Cipher Unit 129, 130
French transposition encipherment 130
French transposition system, Free 121
French unenciphered codes, recovery of 124
French Unit 140
French units 123, 126, 129, 130
French units, amalgamation of 7, 117, 128
French version 127, 145
French version, SZG and SZH 144
French, work in 113
frequencies 25, 211, 245
frequencies, characteristic 218, 301
frequencies, computing of 211
frequencies of letters 251
frequencies of words 251
frequencies, plain-text 174
frequency 32

Doc ID: 6554247

frequency characteristics 182, 253
frequency, cipher-text 246
frequency counts 136
frequency distributions 130, 244
frequency studies 232
frequency tables 71
Frey, Lieutenant Eugene F 162, 163, 168
Fried, Lieutenant Walter J 230, 250, 251, 254, (Captain) 21, 22, 240, 244
Friedman Secret Writing Case 227
Friedman, Mr. William F. 2, 12, 13, 16, 19, 20, 24, 29, 30, 38, 46, 234, 257, 258, 298
Friendlich, Sergeant Richard 207, 208, 213
Frizelle, Lieutenant Theobald E. 139, 140
Fulghum, Miss Olivia 201
Funchal digraphic substitution system 106
functions 131
FWA 244, 245

G-2 1, 2, 28, 37, 38, 76, 111, 223
G-2, Assistant Chief of Staff 12, 13, 20, 48
G Branch 10
G period 74, 79
G Section 2
Galvan, Lieutenant Alvaro F. 162
Gammell, Major Lewis W. 257, 258
garbled indicators 266
Garman, Mr. Allan D. 113, 123, 140, 144, 160
GCCS 13, 14, 16—19, 21, 22, 58, 59, 63, 69, 70, 72, 73, 75, 78, 79, 83, 86, 90, 91, 95, 100, 132, 138, 157, 158, 172 174—176, 193, 195, 196, 225, 234, 236, 238, 239, 243, 247, 255, 257, 259—262, 266, 268, 277
GCCS, achievements of 69
GCCS, American Liaison Officer in 292
GCCS, assistance of 183, 186, 192, 193, 201 202
GCCS centers 20
GCCS, chief of 16
GCCS, contributions of 192, 201, 202, 254
GCCS, contribution to 239, 277
GCCS, cooperation of 57, 243
GCCS, Enigma Section 261
GCCS, exchanges with 179, 186, 192, 237, 243, 245, 263, 264, 277, 290, 301
GCCS, Italian Diplomatic Section of 102
GCCS, Japanese diplomatic work at 59
GCCS, keys supplied by 254
GCCS liaison officer 21
GCCS, Liaison Officer at 240
GCCS, liaison with 289
GCCS, London Offices 288
GCCS, Naval Section 21
GCCS, operational procedures developed at 239
GCCS, operational subsection of 269
GCCS operations 20
GCCS, representative of the Signal Security Agency at 292
GCCS, requests from 290
GEB, Port au Prince digraphic substitution system 83, 86, 96
GEC 16, 89, 91-93, 96, 300
GEC—GEE isologs, 89,90
GEC keys 17
GEC solution of 83, 93
GEC, technical description of 17

Doc ID: 6554247

GEC traffic 93, 96
GEC, translations 301
GEC work sheets 17
GED (plain code) 96
GEE 88, 92, 93, 285, 296, 300, 301
GEE additives 84, 89
GEE keys 94
GEE problem 90
GEE, randomicity 93
GEE, solution of 83, 93
GEE, system 88, 244
GEE traffic, solution of 95
GEG, first translation of 96
GEG system 96
general channels 53
General Cryptanalysis (B-3) 9, 10
General Cryptanalytic Branch 11, 24, 82, 130, 232, 258, 270, 280, 284-286, 288, 295, 299
General Cryptanalytic Branch Chief 22
General Cryptanalytic Section (B-III) 55, 130
General Marshall, Memorandum 17
General Staff code 188
General Staff, France, Radio Intelligence Section 221
General Tai Li's code 188
generatrices 267
Geneva 31
geographical location 259
GEQ 234, 236, 238, 240, 246
GEQ indicator system, solution of, report on 240
GEQ, solution of 234
GEQ system 273
GEQ traffic 241
German 131, 139, 140, 222, 223, 300
German (B-2) 3, 4
German Abwehr Enigma (GEQ) 234, 236, 238, 240, 245, 246
German agent 88, 300
German agents in Argentina 226
German Air Force 13, 243, 257, 259
German Army 243
German Army and Air Force traffic, interception of 235
German Army communications 13
German Army traffic 257, 259
German channels 190
German cipher-machine systems 282
German code book, unenciphered 82
German code work 21
German codes 140
German Consulate 85, 245
German cryptographic machine, Enigma 13
German cryptonets 260
German diplomatic agent 82
German diplomatic mission 83
German Diplomatic Section 2, 82, 86, 88, 197, 285
German diplomatic solution 82
German diplomatic systems 17, 21, 82
German Enigma machine 273
German Enigma, Naval 260
German Enigma problem 235, 257
German equipment 77
German Foreign Ministry, location of 87
German Foreign Office 300

Doc ID: 6554247

German Foreign Office cryptographic system, solution of 88
German Government 51, 95, 247
German Hagelin machine directions 303
German installations 77
German Kryha (GEH) 236
German Kryha machine 235
German language 6
German letter traffic, Tokyo-Berlin 245
German machine 91
German-manufactured cipher machine 146
German manufacturers 95
German messages 225
German messages, cribs for 214
German military activities, cessation of 266
German Military Attache 244
German Military Enigma (GEU) 234, 236, 237
German military problem 19
German military systems 17, 19
German military traffic, solution of 17
German models (Enigma) 238
German naval traffic 19
German Navy communications 13
German occupation of North Africa 222
German officer, diary of 222
German one-time pad 244, 285
German, permitted messages 225
German Permutation Cipher Teleprinter, Type 526 234
German problem 83, 213
German recordings 228
German Section 82, 89, 140, 200, 301
German Shanghai letter traffic 244
German signal-intelligence services 94
German sources 301
German spies 87
German stenographic documents 222
German system, solution of 214
German systems 7, 12, 245
German traffic, study of 213
German Teleprinter ciphers (GES, GET) 234, 236, 238, 240, 277
German teletypewriter cipher messages 276
German texts, translation of 230
German Tokyo-Berlin letter traffic 244
German traffic 210, 211, 215
German translations 140
German troop concentrations 77
German Unit 228
German version 145
German version, SZG and SZH 144
Germans, the 40, 83, 85, 88, 94, 95, 213, 214, 225, 226, 260, 267, 303
Germany 44, 78, 177, 178, 222, 223
Germany, fall of 46
Germany, Ludwigshafen 238
Germany, surrender of 220
GES 234, 236, 240
Gesell, Mr. 49
GET 234, 236, 238, 240, 276
Getchell, Dr. 281
GEU 234, 236, 243

Doc ID: 6554247

GEV 244, 245
GEW 244, 245
GEW traffic 246
GEX 244, 245
"Giant, the" 269
Gibbons, Mr. Hughes O. 170-172, 175, 176
Gidlof, Miss Oriole 252
Girhard, Lieutenant C. E. 101
glass plates 274
Glazier, Mr. Sidney 163, 168
Glenn, Captain Thomas H. 112, 124, 125, 131, 133, 139, 143
Glodell, Lieutenant Leroy M. 4, 148, 149, 151, 161, 162, 164; (Captain) 160, 221
Glodell's Unit 157, 158, 161
glossary 287
glossary, Arabic-English, English-Arabic 174
Glossary of Terms ASA 57
Goldstein, Sergeant Ernest 236, 240, 241, 257
Gordon, Lieutenant Cyrus H. 118, 170, 171, 175, 248, 249
Gordon, Miss Louise 206
Gosline, Miss Hazel 181
Goveker, Private Rosalie 191
government 4, 49, 51, 57 142, 190, 203
government, Belgian 130
Government, Brazilian 51
Government,British 51, 247
government, Chinese 196
government, Chungking 180
Government Code and Cipher School 111
government codes, Chinese 187
government, Croatian puppet 180, 193
government, Czechoslovakian in London 180
government, Dutch 247
government, Fascist Republican 108, 116
government, Finnish 247
Government, Free French 123
government, French 247
Government, German 51, 95, 247
government, Greek Royalist 180
government, Haitian 130, 199
government, Italian 110, 247
government, Mexican 147
government, Mussolini 108
Government, Nanking 180, 189
government of Haiti 198
government, Papandreau 192
government, Philippines puppet 180
government, Polish in London 180
government, Portuguese 247
government, Royalist 107
government, Spanish-American 2, 155
government, Swedish 247
government, Swiss 131, 139
government system, Spanish 148
government systems 152, 233
government, Thai 185, 196
government, traffic of the Nanking 185
government traffic, Spanish 8, 149
Government, United States 259
government, Vichy 116, 135, 211
Governmental agency 36, 37
governmental traffic 107
governments 2, 5, 50, 52, 126, 170, 180, 197, 205, 216, 247, 290, 296, 298
governments, Axis 225

Doc ID: 6554247

governments, Central American 148
governments, English-speaking 143
governments, European 215
governments, French 112
governments, Iberian 148
governments, minor European 190
governments of Near and Middle East 176
governments, Spanish-American 152-154
governments, various 177
GRA 192
GRADTAFEL 87
graduate student 171
graduate work 149, 171
grammar 173
grammatical forms 25
grammatical relationships 301
Grand Dutchy of Luxembourg 199
GRB 191, 301
GRE 192
Great Britain 232
Greater East Asia area 58
Greater East Asia Ministry 56
Greece, royalist government of 180
Greenberg, Sergeant Joseph 102
Greek 222, 301
Greek, ancient 190
Greek cryptographic methods 301
Greek descent 190
Greek, modern 190
Greek problem 191
Greek systems 191, 192
Greeks, the 301
Greek traffic 190, 191
Green machines, captured Japanese Army 284
Green Machine, study of 284
Greene, Miss Cordelia 191, 221
Greene, Lieutenant James B. 248
Grey Manufacturing Company 272
Griggs, Dr. Marion 145
grille 264
grilles 77, 224
Grotjahn, Miss Genevieve (Mrs. Feinstein) 48, 235, 248
ground level visibility 204
group, begin spell 143
group, cipher 283
group, code 99, 142, 145, 219
group count 136
group, five-digit 136, 174
group, four-digit 174
group, four-letter 113
group, language 302
group of messages 77
group, overlap 80
group, pentanomic 120
group, plain-code 135
group, prearranged 65
group, research 74
group, spelling 142
group, switch 62
group, textual 66
grouping of subsections according cryptographic method 153
grouping of subsections, language 153
groups 64, 100, 125, 142, 161, 189, 195, 202, 214, 218, 232, 300
groups, additive 89, 90, 93, 122
groups, blocks of 63
groups, cipher 284
groups, code 64, 70, 110, 130, 160, 202, 283, 284, 294
groups, code, high-frequency 283

Doc ID: 6554247

groups, common 165
groups, five-digit 84, 85, 89
groups, five-letter 65, 70
groups for punctuation 143
groups, four-digit 63
groups, four-letter code 25
groups, isolation of 60
groups, literal 82
groups, nontextual 69
groups, relative code 122
groups, sequence of 214
groups, spelling 143
groups, tetragraphic 168, 283
groups, two-letter 25, 55, 62
Guedes code book 303
guessing process 36
guessing words 37
"Guion" cipher, Mexican 150
Gwiazdzinska, Private Marcella 190

"H" book 75
"H" period 72
"H" period traffic 74
Haar, Miss Fairfax 159
Hagelin B-211 247
Hagelin, Boris C. W. 247
Hagelin C-36, 247
Hagelin C-38, solution of 247
Hagelin C-41 247
Hagelin characteristics 245
Hagelin cipher machine, invention of 247
Hagelin, cryptograph, insecure use of 255
Hagelin cryptography FID 252
Hagelin-enciphered running key 252
Hagelin-enciphered text, transposed 252
Hagelin letter-subtractor machine 256
Hagelin machine 167, 235, 247
Hagelin machine ciphers 236
Hagelin machine, Finnish, analysis of 235
Hagelin machine, German, directions for 303
Hagelin machine, statistical approach to 255
[redacted] . . . . EO 3.3b(3) EO 3.3(h)(2) PL 86-36/50 USC 3605
Hagelin messages, Swedish diplomatic 273
Hagelin NEA system 254
Hagelin, Portuguese 254
Hagelin problem 248
Hagelin problems 234, 235
Hagelin report No. 2 255
Hagelin report No. 3 255
Hagelin report No. 4 255
Hagelin Section 167, 240, 250, 253
Hagelin Section, establishment of 247
Hagelin Section, strength of 251
Hagelin solution, bibliography on 247
Hagelin studies 247
Hagelin, Swedish 256
Hagelin systems 256
Hagelin traffic 248
Haggard, Lieutenant 162
Haiti 126, 233
Haitian government 130, 198, 199
Haitian systems 197, 198
Haitian traffic 132, 198, 199
Hallock, Mr. Richard 114, 118, 125; (Lieutenant) 129, 236, 238, 253

Doc ID: 6554247

Hamburg 160
Hampton, Miss Mary Evalyn 200
Hampton, Mr. N. Lloyd 173
Hancock, Miss Margaret 288
hand method 284
hand method of solution 243
hand methods 81, 92, 273
hand operated 272, 274
hand-operated machine 45
hand recovery 243
hand scritching 269
hand solution 268
hand testing 264, 265, 277
hand, work done by 278
handling of documents 292
handling of traffic 47, 290
Hanoi 120
Hanoi code 114
Hanoi cribs 120
Hanson, Mrs. (Miss Sadie Jones) 113
Harding, Miss Rosalie (Mrs. Bash) 113, 148
Harrison, Mr. R. Woodrow 147, 157, 163
Hart, Mr. Humes H. W. 154
Hartstall, Mr. Paul K. 112, 120, 121, 131, 132
Harvard University 171
Hastings, Captain Edward 16
Hawaiian Department 82
Hawkins, Mr. E. J. 48
Hayes, Captain Harold G. 16; (Colonel) 10, 300
Haynes, Lieutenant John 181,182
Hazard, Mrs. Marion 221
"HE" code 27
heading, diplomatic 233
Headquarters Branch, Signal Security Agency 9, 10
Headquarters Building 235
Headquarters, Panama Canal Department 98
Hebern 40
Hebern machine ciphers 236
Hebern-type rotors 285
Helmke, Miss Alvina 140
Helsinki traffic 78
Herther, Mrs. (Miss Annette K. Robinette) 221
Hesse, Mr. Alfred 234, 236, 238, 240, 241, 245
heterogeneous material 141
Hezlep, Captain William H. 204, 206-209
hidden messages 220, 224
higher authority 286
high-frequency code groups 284
high-frequency letters 267
high-security diplomatic machine 13
high-security system 13
high-speed coincidence counting 274
high-speed electronic counting 276
high-speed equipment 271
high-speed RAM methods 218
Hill, Lieutenant Elwood 129, 184
Hill, Miss Mary 62
Hiser, Lieutenant C. H. 101
Historian, ASA 13
historical accounts 24
Historical Background of the Signal Security Agency 24, 40, 51, 82, 147, 298
historical group 215
historical purposes 205
Historical Unit, ASA 24
history, B-III 287
history of liaison with the British 14
History of Portuguese-Brazilian Section 160
History of the Signal Security Agency 40
History, plan of 11
Hitch, Miss Jean 221
Hoesen, Miss Alice Van 120
Hoffman, Miss Rachel 201
holders 31, 46, 297
Holliday, Miss Margaret H. 173
homogeneity of traffic 115
homogeneous block of sheets 90

Doc ID: 6554247

homogeneous block of sheets 90
homogeneous traffic 116
homologs, identification of 42
homologs, solution by 44
Honduras traffic 153
Horsay, Miss Eleanor 221
hostilities, cessation of 50
hotel rooms, conversations in 228
Howard, Lieutenant Lee P. 112, 116, 126, 127
Hsinking 32
HTA 198, 233
HTB 233
HTZ 233
HUA 201
HUD 201
Hungarian 222
Hungarian systems 181, 197, 200
Hungarian traffic 200
Hungary 177
Hunt, Private Burrowes 250; (Sergeant) 236; (Lieutenant) 241
Hunt, Mrs. (Miss Dudley Scovil) 236, 250, 255
Hunter, Miss Janet 122
Hurley, Sergeant George 54, 236, 238
Hurt, Mr. John B. 25, 29, 48
Hyman, Mr. John 206, 248; (Sergeant) 235
Hyslop, Miss Constance 120, 121

"I" messages 75
I period 74, 278
I period key book 66, 74, 75
I Section 2
Iberian governments 148
Iberian groups 157
Iberian systems 157
IBM 73, 87, 210
IBM card reproducer 277
IBM cards 283
IBM Company 272
IBM decoding 87
IBM index 89, 113, 199
IBM letter writing equipment 278
IBM listings 59, 60, 92
IBM message prints 184
IBM method 284
IBM methods 174, 211, 218, 242, 248, 251
IBM procedure 73
IBM processes 92
IBM processing 73, 140, 174, 182, 241
IBM studies 201
IBM tabulator 53
IBM technique 59
IBM teletypewriter tape equipment 272
IBM testing 178
IC cameras 272, 279
IC comparators 271
IC count 273
IC equipment 273
IC film projector 275, 279
IC machinery 273
IC machines 277
IC plate equipment 279
IC plates 242
IC projector 274
IC projector, change of plate gate 276
Iceland, occupation of 85
Iceland, station at 259
ideas, exchange of 281
identical encipherments 39
identical indicators 39
identically enciphered 39
identification 91, 222, 232, 291, 292
Identification Book, System 289, 291
identification, code 231, 233

Doc ID: 6554247

identification, methods of 292
identification, mistakes in 290
identification of homologs 42
identifications 109, 110, 124, 125, 142, 145, 161 165, 168, 176, 183, 184, 186
identities 34, 37
IK 27
illicit station 70
illustrations 173
IMC 204
IMC, Japanese counterpart 210
IMC, Japanese equivalents and 216
IMC synoptic, basic 214
IMS (RA-1) 108
impasse 184
Impero code 104, 108, 110
Impero code reconstruction 101
Impero (ITA) traffic 107
imponderables 15
improvement, cryptographic 66
improvement in interception 241
improvements 243
improvements in M-228 282
impulses, electrical 73
inaccuries 278
inconsistencies 43
increase in needs of Section I 9
increase in personnel 248, 249
increase in security 280 282
increase in strength 9
increased output 179
indecipherable 51, 88
indecipherable system 52
index 89, 141, 168, 169 195, 242
index, additive 89
Index, IBM 89, 199
index, machine 165, 167
index, noun 74
index of coincidence 271, 274
index of coincidence comparators 271
Index of Coincidence Plate Projector 276
index of solved messages 73
index of traffic 160
index, topical 74
Index, XYZ 89
indexes 184, 201, 286
indexes, IBM 113
indexes, machine 198
indexing 191, 200
indexing of traffic 290
indexing procedure 184
indexing system 292
Indexing Unit 56
India-Burma Theater 208
indication keys 85
indicatives, war 212
indicator 32, 41—44, 62, 65, 71, 133, 134, 218, 267, 283
indicator, "A" type 32
indicator construction 249
indicator crib 267
indicator, daily 83
indicator, encipherment of 63, 85, 134
indicator encipherment, solution of 158
indicator, JAS 69
indicator key 66
indicator key chart 66, 67
indicator key, eight-digit 84
indicator key recovery 72, 76, 87
indicator keys 71, 73, 83, 278
indicator keys, daily 85

Doc ID: 6554247

indicator keys, construction of 96
indicator keys, two-day period 95
indicator keys, two-day period 96
indicator pattern 195
indicator recovery 79
indicator research 79
indicator, six-letter 244
indicator subtraction 252
indicator system 45, 135, 303
indicator system, change of 282
indicator system GEQ, solution of, report on 240
indicator system, JBC 56
indicator system, solution of 218, 242, 245, 303
indicator systems 56, 91
indicator tables 129
indicator, tripartite 85
indicators 30, 33, 38, 44, 45, 53, 136, 250, 291
indicators, absolute 256
indicators, cryptanalysis 250
indicators, enciphered 69
indicators, garbled 266
indicators, identical 39
indicators, JN-36
indicators, key 212
indicators, messages enciphered with same 282
indicators, solution of 218
indicators, study of 218
indicators, subtracted, index of 252
indicators, system, solution of 229
Indo-China 137, 232
Indologist 171
inflected forms 301
inflection principle 301
inflectional ending 143
information 6, 12, 14, 30, 38, 57, 63, 76-78, 83, 84, 92, 95, 98, 111, 112, 114, 134, 137, 138, 141, 142, 160, 199, 202, 219, 222, 224, 226, 229, 232, 249, 250, 259, 262, 265, 287, 291, 292, 295, 298
Information and Liaison Branch 10, 11
Information (B-9) 4
information, British 169
information, climatological 215
information, coordination of 230
information, cryptanalytic 15, 91, 290
information, diplomatic 58
information, diplomatic 232
information, dissemination of 289
information, economic 243
information, exchange of 11, 20, 22, 58, 91, 102, 290
information, flow of 21
information, intercept 108
information, interchange of 18, 20, 21
information letter, monthly 21
information, meteorological 204
information, military 232
information of value 25
Information Section 261
information services 4
information, source of 57, 58, 62, 76
information, sources of 164
information supplied by the British 165
information, technical 13, 22, 255
information, technical, exchange of with GCCS and EU 138

Doc ID: 6554247

Information Unit (B-I) 8
information, weather 205
initial letter 25
ink, secret 227
input method, double 265
insecure 64
insecurity of German system 214
insolvable traffic 194
installations, German 77
instruction 173, 236, 241
instruction, cryptographic 61
instruction in Turkish 173
instruction messages, cryptographic 89
instructional material 1
instructions 28, 96, 127, 178, 303
instructions concerning encipherment 17
instructions, cryptographic 95
instructions for circular messages 75
instructional materials 284
instructors 209, 235
insufficient traffic 296
integration 81
intelligence 25, 29, 46, 59, 76, 87, 88, 91, 111, 138, 145, 173, 176, 177, 182, 190, 222, 223, 246, 285, 286, 287, 289, 296
Intelligence agents 299
intelligence, commercial 203
intelligence, cryptographic 60
intelligence, current 91
intelligence, diplomatic 203
Intelligence Division 11, 231
intelligence functions 10
intelligence, important 179
intelligence, military 50, 52
Intelligence Officer in Panama 298
intelligence, production of 1, 28, 47, 133, 180
intelligence, Purple 277
intelligence recovered 92
intelligence recovered from Finnish materials 251
intelligence, source of 285, 300, 302, 303
intelligence value 63, 83, 105, 138, 185, 237, 290
intelligence, vital 92
intentions, Nazi 83
intercept 1
intercept activity 262
intercept centers 261
intercept copies, faulty 238, 241
intercept coverage 205
intercept data 259
intercept facilities 1, 205
intercept material 259
intercept sets, British, release of 260
intercept sources 302
intercept stations, British 70
intercept stations 3, 6
intercept units 209
intercepted 217
intercepted documents 150
intercepted mail 220
intercepted messages 49
intercepted traffic 37, 49, 58, 89, 148, 167, 203, 226, 290
intercepting 84
interception 5, 49, 136, 152, 161, 203, 220, 261, 262, 265, 266, 296
interception, American 109
interception, British 260
interception, facilities for 209

Doc ID: 6554247

interception, improvement 241
interception, inadequate 242
interception of Bulgarian traffic 192
interception of conversations, clandestine 228
interception of German agent 300
interception of German Army and Air Force traffic 235
interception of messages 166
intercepts 29, 32, 88, 98, 105, 192, 209, 217
intercepts of Japanese weather reports 215
intercepts, text of 205, 206
interchange of cryptanalytic information 18
interchange of information 20, 21, 255
interchanges, 1941 11
intercommunication 64
Interior, Italian Ministry of 108
International Aviation Conference 178
International Business Machines Company 272
international conference 296
International Meteorological Code 4, 204
International Meteorological Code, Japanese nonuse of 216
international meteorological conferences 216
interrelationship 201
interrogation of prisoners 94
interruption, cyclic 249
inter-service collective system 217
interval 40
intervals 39, 40, 72, 200
intervals, irregular 66
intervals of broadcast 205
interview 199, 200, 203
interviews 24, 82, 139, 170, 180, 197, 201, 204, 220, 229, 234, 257, 288, 292
introductory course 61
invasion of North African 113, 120
invention 155, 285
invention, of Hagelin cipher machine 247
investigation 83, 194
investigation, Pearl Harbor 13
investigations 49
Invincible (CND) 182
IQA 170
IQB 170
IQC 170
IRA 170, 174, 301
IRA book 302
Iran 170, 177, 301
Iranian codes, compromised 174
Iranian diplomatic systems 301
Iranian systems 302
Iranian traffic 173
Iraq 170, 177
Iraqi systems 174, 179
Iraqi traffic 173
Iraqian cipher 174
Iraqian systems 175
IRB 170, 174, 301
IRC 170, 174, 175, 301
Irish systems 197, 199
Irish traffic 199, 200
irregular intervals 66
"--isati--" 253
isolated stations 217
isolation 122, 123
isolation, group 60
isolation of commercial code traffic 229
isolation of crib messages 261
isolog 137, 192, 195
isologs 71, 74-76, 85-87, 156

Doc ID: 6554247

isologs, GEC-GEE circular 89
Istanbul 242
Istanbul circuit 158
ITA 107, 108
Italian 3, 113, 147, 222
Italian additive encipherment 105
Italian Additive Recovery Unit 105
Italian (B-3) 3,4
Italian Code Recovery Unit 125, 151
Italian Codes and Ciphers 1939-1943 107, 110
Italian commercial system 105
Italian cryptographic habits 101
Italian cryptographic history 102
Italian cryptographic systems 98, 103
Italian diplomatic codes 109
Italian diplomatic correspondence 111
Italian diplomatic problems 13
Italian Diplomatic Section 22
Italian Diplomatic Section of GCCS 102
Italian diplomatic systems 17, 105
Italian diplomatic traffic 98
Italian digraphic substitution encipherment 105
Italian field 100
Italian government 110, 247
Italian governments, two 107
Italian language 6
Italian language specialists 102
Italian messages 214, 225
Italian ministries 108
Italian prisoners of war, letters of 223
Italian problems 100, 107
Italian reports 212
Italian Section 98, 100, 101-103, 106, 107, 109, 132, 294
Italian Section, summary of achievements 111
Italian solution 107
Italian systems 12, 98, 100, 106, 111, 214, 294
Italian traffic 107, 212, 215
Italian traffic, cessation of 212
Italian traffic, resumption of 213
Italian Unit 7, 106
Italian units 104, 106
Italian weather system 212
Italians, cryptographic habits of the 111
Italians, the 99, 108
Italy 44, 213
Italy, capitulation of 213
Italy, Royalist 109
ITD (AR30) 99, 294
ITI (RA) 99
ITT 234, 236

J-6 25, 27
J-7 27
J-8 27
J-9 27
J-10 27
J-11 27
J-12 27
J-13 27
J-14 27
J-15 27

Doc ID: 6554247

J-16 27
J-19 53
J-19 (JAE) 52, 293
J-19 (JAE) termination of 55
J-19 section 54
J-19, solution of 53
J-19 unit 55
J-period 74, 75, 278
J Section 2
JAA 54, 235, 236, 283
JAA-1 46
JAA development sheets 59
JAA messages 277
JAA, solution of 277
JAB 47
Jacobs, Mr. Walter 251, 255, 256; (Corporal) 201; (Sergeant) 22, 280, 285
Jacobson, Mrs. Peyton 80
JAD 47
JAE (J-19) 52, 293
JAE (J-19) termination of 55
Jaffe, Corporal Sidney 119; (Sergeant) 120; (Lieutenant) 131, 132, 134, 145, 208
JAH 293
JAH, exploitation of 233
JAI 293
JAJ 293
JAK 293
JAM 55, 57, 274
JAM, development of 56
JAM, entry into 55
JAM traffic 59
JAO 56
JAP 64
Japan 44, 57, 137, 178, 232
Japan, capitulation of 47
Japanese 34, 35, 49, 50, 52, 220, 222
Japanese "A" Machine 29
Japanese activity in meteorology, concealing of 216
Japanese Admiralty 216
Japanese analogues 46
Japanese Army 243, 291
Japanese Army codes, JE group 284
Japanese Army communications 7
Japanese Army double additive encipherment system 285
Japanese Army machine-cipher system 240
Japanese Army messages 276
Japanese Army problem 11
Japanese Army problems 8, 275
Japanese Army Section 130
Japanese Army systems 1, 10, 11, 74, 295
Japanese Army traffic 276
Japanese (B-1) 3, 4
Japanese "B" Machine 46
Japanese broadcast schedules 217
Japanese characters 64
Japanese cipher-machine systems 282
Japanese Code, breaking of 31
Japanese code clerks 74, 219
Japanese codes 17
Japanese Codes and Ciphers 1919-1929 24
Japanese commercial system 233, 243
Japanese commercial traffic 186
Japanese communications 81
Japanese concealing of meteorological information 216
Japanese counterpart of JMC 210
Japanese cryptanalysis 16
Japanese cryptographic machines 45

Doc ID: 6554247

Japanese cryptography, changes in 277
Japanese delegations 216
Japanese diplomatic communications 7
Japanese diplomatic cryptography 26
Japanese diplomatic enciphered code systems 283
Japanese diplomatic language 61
Japanese diplomatic office 31
Japanese diplomatic problems 54, 58
Japanese diplomatic Red and Purple machines 234
Japanese Diplomatic Section 2, 24, 54, 60, 186
Japanese Diplomatic Section, reorganization of 56
Japanese diplomatic solution, conference on 59
Japanese diplomatic system 15, 17, 21, 22, 24-26, 28, 30, 54, 57, 61, 274
Japanese diplomatic systems 284
Japanese diplomatic traffic 28, 48
Japanese Diplomatic Unit 55
Japanese diplomatic work 21, 22
Japanese diplomatic work at GCCS 59
Japanese Domestic Network 22, 57, 58
Japanese embassies 31
Japanese equivalents and IMC 216
Japanese experts 35, 81
Japanese Foreign office 34
Japanese Government 36
Japanese group 293, 294
Japanese, intentions of 48
Japanese language 8, 25, 48, 61, 115, 128
Japanese Language (B-1) 9, 10
Japanese Language (Section I) 9
Japanese material 24
Japanese messages 49, 225
Japanese meteorological systems 273, 274
Japanese military attaché communications 7
Japanese Military Attaché (JMA) 62, 64
Japanese Military Attaché messages 260
Japanese military attaché problems 78, 79
Japanese Military Attaché Section 118, 181
Japanese military attaché systems 24, 62
Japanese military attaché work 22
Japanese military attachés 64, 76
Japanese Military Cryptanalysis (B-2) 9, 10
Japanese Military Cryptanalysis (Section II) 9
Japanese military field 284
Japanese Navy cipher machine 30
Japanese plain text 35, 49
Japanese prisoners of war, letters of 223
Japanese problems 25, 172, 176
Japanese problems, cryptanalysis of 207
Japanese Purple machine 234, 235, 277, 295
Japanese Red and Purple machines (JAA) 236
Japanese "Red" Machine 29, 234
Japanese Rikugun Letters No. 3 (JRL-3) 63
Japanese Rikugun Numbers, No. 4 63

Doc ID: 6554247

Japanese sections 127
Japanese secret cipher 31
Japanese solution 29
Japanese Subsection, SSA 59
Japanese system 1
Japanese systems 12, 19, 24, 26, 107, 116, 127, 215, 293
Japanese text 37
Japanese, the 26, 28-30, 63, 64-66, 68, 74, 75, 92, 137, 216-219, 226, 260, 284
Japanese traffic 1, 25, 45, 129, 218
Japanese translation 6
Japanese translators 14
Japanese transposition problem 129
Japanese Weather Centrals 216
Japanese weather code, capture of 216
Japanese weather reports 207, 215
Japanese words 219
JAQ 62
JAR 78
Jarmon, Miss Dorothy 221
JAS 62, 64, 69, 77, 78
JAS-1 66, 76
JAS control 69
JAS Conversion Square 278
JAS, cryptographic structure 64
JAS cryptography 66
JAS enciphered indicators 69
JAS, entry 70
JAS indicator 69
JAS messages 70
JAS serial numbers 69
JAS traffic 74, 76
JAT 77
JBA 55, 56, 59, 283
JBB 55, 56
JBC 55-57
JBC indicator system 56
JBC messages, decoding of 60
JBC system 56
JBD 55, 57, 274
JBD, solution of 56
JBE 56
JBG 59
JBH 57
JBH, cryptanalysis of 243
JBH, solution of 243
JD 24
JE English Spelling 27
JE codes, exploitation of 284
jeep, Japanese jet-propelled 92
"Jelly-fish" system 122
JEM 276
JEP 276
JEQ 276
Jerome, Frances M. 48
jet-propelled jeep, Japanese 92
JEV, recovery of 243
JF 24
JG code 25
JH 24
JHC 59, 60
JHE 59
JJA-2 59
JJI 59
JK 62
JKC 59
JL 25
JLA 59
JLD 60
JLL 59
JLM 59
JLR 59
JLS 59
JLT 59
JLV 59
JLW 60
JLX 60
JM 62
JMA (Japanese Military Attaché) 62
JMA personnel 81
JMA Section 80, 81
JMA systems 62-64, 77
JN 62

Doc ID: 6554247

JN-36 216, 217
JN-36 indicators 218
JN-36 key book 219
JN-36 text 218
JN-37 217
JN-37 encipherment 218
JN-37 key book 218, 219
JN-37, solution of 217
JN-37 traffic, coverage of 217
job 264, 268, 269
job, run-checking 264
jobs 61, 263, 265, 266, 274
jobs, number of 269
jobs, priority 265
Johnson, Captain Roy D. 19; (Major) 234, 236, 239, 241, 256, 261-264
Joint Congressional Investigation 31, 48, 50
joint cryptanalytic activities 16
joint work 23
Jones, Lieutenant Clelland D. 126, 127, 133
Jones, Miss Sudie (Mrs. Hanson) 113
Joos, Dr. Martin 186, 236, 249, 280, 281
Joys, Miss Alice 139, 145, 236
JQ 62
JR 62
JRL-3 (Japanese Rikugan Letters No. 3) 62, 63
JRL-4 64
JRN-4 62, 63
JU 24
Just, Mrs. Ethel H. 231
juxtaposition 271, 278
JW 25
JWE-3 219
JWE-5 219
JWE-24 218
K-1 to K-10 27
K-1 code 36
Kalb, Lieutenant Edward C. 208, 209
kana 58, 70
"Kana Nigori, 19" system 240
kana syllables 64
kana symbols 57, 64
kana transposition 243
Keating, Lieutenant L. Clark 220, 221, 231
Keith, Miss Mary 173
Kelly, Lieutenant Vilar 54, 253, 256, 263
Kendrick, Mr. E. A. 18
Kennedy, Miss Caroline 140, 145
Kennedy, Miss Ursula 201
Kepke, Mr. John 250, 253
key 49, 57, 65, 66, 70-72, 74, 76, 89, 94, 178, 193, 227
key, additive 86, 218
key blocks 201
key book 66-69, 72, 75, 76, 79, 216, 218, 253, 254
key book 7 218
key book 8 218
key book 9 218
key book A 67
key book, additive 120
key book B 67
key book C 67, 70
key book D 67, 70
key book E 67
key book F 67
key book G 67, 68
key book H 67
key book I 60, 66, 67, 68
key book J 67
key book, J-period 278
key book, JN-36 219
key book, JN-37 218, 219
key book M (13) 78
key book, obsolete 77

Doc ID: 6554247

key-book page 70
key book, recovery of 83
key book, reconstruction of 253
key book square 74
key books 56, 67, 95
key books 1 to 5 218
key books, captured 218
key books, list of 67
key books, text additive 84
key chart, JAS serial number 69
key charts 71
key, comparison of 275
key, current 28
key distribution 255
key, elements of 266
key-generating unit 282
key chart, indicator 67
key, daily additive 122
key, establishment of period 194
key, indicator 66, 84
key indicators 212
key limitations 201
key, matching 72
key materials 74
key members of the Signal Security Agency 287
key, messages enciphered in same, location of 218
key, nonrepeating 40
key patterns, fitting of 250
key, random 88
key reconstruction, principles 91
key, recovered 56, 89
key recovery 70, 71, 72, 74, 79, 84, 96, 106, 155, 178, 193, 201, 241, 242, 248, 300, 302
key recovery, courses in 73
Key Recovery or Overlap Unit 80
key, safe 299
key recovery, speed of 73
key recovery, two-day-period 87
key recovery units 81
key, resultant 84, 253
key, running 195, 212, 252, 253, 256, 278
key sequence, mixed 65, 129, 135
key sequences 136
key sequences, additive 218
key sheets, pads of 88
key tables, serial number 66
key text, enciphered 252
key, transposition 275
keyboard 46
keyboard, typewriter 73
keyboard typewriter unit 45
keyed columnar transposition 188
keys 55, 84, 85, 94, 96, 129, 130, 145, 154, 179, 201, 219, 242, 300-302
keys, additive 63, 120, 212, 213
keys, analysis of difference between 249
keys, changes in 46
keys, cyclically-repeating 40
keys, daily changing 53, 242
keys, daily, solution of 250
keys, enciphering 122
keys, French 17
keys, GEC 17
keys, GEE 94
keys, indicator 71, 73, 83, 85, 278
keys involving only one odd kick 250
keys, list of 16, 241
keys, method of using 134
keys, Mexican 14
keys, NEA 256

Doc ID: 6554247

keys, on keyboard 73
keys, pages of 219
keys, prediction of 53
keys recovered 53
keys, recovery of 54
keys, reuse of 88
keys, solution of 46, 302
keys supplied by GCCS 254
keys to Swedish traffic 250
keys, two-day indicator 95, 96
keys, wheel-setting, adjustment of 264
Keyword system 95
Keyword system, solution of 83
Keyword traffic 85
kick, keys involving only one odd 250
King, Private First Class Robert 182
Kinney, Mr. David 189
Klein, Captain Maurice H. 62, 80
Klemm, Dr. Frederick 236
Klitzke, Dr. Carl P. 82, 236
KO 27
Koegel, Miss Louise 145
KOOKABURA 248
Koslow, Lieutenant Harry 181
Kropfl, Mr. Ulrich J. 48
Krus, Miss Phyllis 190
Kryha Cipher Machine 83, 235
Kryha, German 235, 236
Kullback, Dr. Solomon 2, 16, 25, 29, 62, 63, 82; (Captain) 4, 6, 16, 17, 147, 234, 240, (Lieutenant Colonel) 9, 10, 79, 82, 245
Kullback's report 17

labor 41, 303
Laboratory Branch 129
lack of able linguists 301
lack of cribs 242, 265
lack of material 121, 220
lack of personnel 102, 152, 182, 263
lack of traffic 56, 120, 169, 194, 240, 261, 262, 301,
lack of trained personnel 171
lack of training 171
lag 222
lag, time 72
Lake Garda 241
Lambert, Miss Wilma J. 244, 263
landings, North African 211
land line communication 192
land type reports 212
Lane, Miss Mary Charlotte 118, 236
language 5, 34, 36, 115, 131, 172, 204
language, Arabic 178
language, basic 5
Language Branch (B-I) 11, 81, 228
language, Chinese, expert in 181
language codes 219
language, Finnish 253
languages, Finno-Ugrian, expert in 250
language, foreign 222, 301
language, French 6, 125, 126, 197
language, German 6
language group 302
language grouping of subsections 153
language, Italian 6
language, Japanese 8, 48, 61, 115, 128
language, Portuguese 6, 161, 163
language, Portuguese, course in 164
language problems, Chinese 186

Doc ID: 6554247

language, Romance 3
language, Scandinavian 253
Language Section Romance 101
language sections, Romance 132
language, Spanish 6, 115, 128, 147, 220
language specialists 220
language study 251
language study in Finnish, first 251
language, technical 76
language, Thai, expert in 189
language, Turkish 173, 179
language, Turkish, studies of 174
Language Unit 132
language units 131, 185, 225, 294
language units, organization by 8
language units, Spanish 159
languages 6, 139, 172, 191, 210, 227, 228, 233
languages, European 222
languages, foreign 231
languages, organization around 103
languages, rare 179, 182
languages, Romance 113, 147, 163, 233
languages, Semitic 171
languages, Slavic 190, 191
languages, Spanish and Portuguese 4
LaSala, Sergeant Donald F. 102
Las Palmas 96
Lathrop, Miss Marion 120
Latin America 12
Lattin, Mrs. G. L. 114, 123
Laudig, Mr. Glenn S. 48
law, basic 39
law, practice of 250
Lawrence, Sergeant B. Roy 48
laws, cryptographic 43
LBA 203, 233
LBB 203, 233
LBC 203
LBZ 233
LEA 178
Lebanese cryptographed traffic 178
Lebanon 138, 177, 179
Lechter, Mr. Max 184
lectures 234, 236, 261
Legalley, Mr. Charles M. 81
legations 178, 179
length 53
Leon, Miss Mary 159
Leonard, Mrs. (Miss Betty Moulton) 159, 292, 294
lessons 173
lessons learned 282
letter 35, 41, 42, 150, 224, 259
letter, cover 227
letter, initial 25
letter, monthly information 21
letter of intent 258
letter, plain-text 43
letter-subtractor machine, Hagelin 256
letter traffic, German Shanghai 244
letter traffic, German Tokyo-Berlin 244, 245
letter traffic (GEN) 245
letter, two digits for one 202
letter writing equipment 278
letters 32, 34, 38, 40, 42, 64-66, 78, 227, 232, 246, 271, 283
letters, cipher 33, 38
letters, cipher text 38
letters, dominant, system of 168
letters, encipherment of 282

Doc ID: 6554247

letters, frequency of 251
letters from civilians to the War Department 223
letters, high frequency 267
letters, missing 34
letters of key 76
letters of key, identical 72
letters of prisoners of war 223
letters passing through Military Censorship 223
letters, plain-text 38
letters, random assortment of 35
letters, solution of 227
Levine, Mr. Jack 235; (Sergeant) 194, 195, 239, 256, 281
Lewis, Sergeant Arthur 234, 235
Lewis, Mr. Frank 79, 82, 235
liaison 58, 78, 81, 104, 130, 131, 208, 209, 259, 281
liaison, Anglo-American 15
liaison, B-III 286
liaison between British and American sections 59
liaison officer 22, 73
Liaison Officer, American 239
Liaison Officer at GCCS 240
liaison officer, GCCS 21
liaison officer, MIS 20
liaison officer, OP-20-G 21
liaison officer, SIS 20
liaison officer, SSA 21
liaison officers 13
liaison, operational 78
liaison reports 288, 292
liaison, slip in 254
liaison, technical 219
Liaison Unit (B-I) 8
liaison with British 11, 21, 138
liaison with British, evaluation of 14
liaison with E Branch 262
liaison with EU 139, 289
liaison with GCCS 289
liaison with GCCS and EU 138
liaison with Navy 208
"Lib-I" system 123
"Lib-2" system 123
"Lib-3" system 123
"Lib-7" system 122
"Lib-8" system 123
Libera, Lieutenant John 191, 195
Liberia 233
Liberian messages 203
Liberian systems 203
librarian 171
libraries 254
Library of Congress 173, 174, 254, 303
library references 300
library, Weather Bureau 215
Ligon, Lieutenant Richard 123
limitation, code group 168
limitations 56
limitations, code 201
limitations, key 201
limitations of plain values 218
limitations, pattern 96
limitations, square 278
line 142
line of additive 84
line symbol 142
lines 84, 86
lines, additive 85, 87, 96
lines, additive combined 86
lines of additives 95
lines, recovered 275
linguistic assistance 81

Doc ID: 6554247

linguistic assistance 81
linguistic deficiencies 172
linguistic difficulty 189
linguistic experts 180, 210
linguistic needs 102
linguistic operations 7
linguistic organization 104
linguistic personnel 192, 193, 302
linguistic personnel, training of 195
linguistic problem 99, 302
linguistic problems 139, 144, 182
linguistic production 251
linguistic phases of work 159
linguistic staff 183
linguistic tasks 172
linguistic training 163
linguistics tests 191
linguists 191, 301
Lipsky, Mr. 281
Lisbon 75, 164, 241, 302
list, discriminant 264
list of equipment 272
list of keys 241
list of recovered daily keys 16
list of short titles 291
list of systems 290
listings, IBM 59, 60, 92
listings of differenences 201
lists, cipher machine 301
lists, priority request 92
literal groups 82
literary Arabic 171
literature, cryptanalytic 288
literature of cryptology 287
Little, Mr. John W. 189
Little, Miss Martha L. 126
Litton, Lieutenant Richard 139
Lloyd, Lieutenant Charles E. 221
loan, personnel on 228
Lobeck, Miss Elmise 173
location, geographical 259
location of German Foreign Ministry 87
location of messages enciphered in same key 218
location of observer 205
location of Weather Unit 209
location, Finnish habits of 250
logarithmic value, charts of 71
logarithmic weighting 283
logged 194
logging 159
logging of messages 142
logging of traffic 193
logging techniques 183
London 12, 17, 31, 100, 114, 138, 146, 175, 237
London, Czeckoslovakian government in 180
London Offices of GCCS 288
London, Polish government in 180
London-Tokyo messages 69
long U 35
Loranco Limited 94
Lorant, Mr. 94, 95
Los Angeles, French Consulate at 127
loss of personnel 103
Lovas, Miss Julia 191
low-echelon systems, traffic in 219
Lowenthal, Private Ruth 190
LUA 199, 233
lucite rods 275, 279
Ludwigshafen, Germany 238
Luxembourg 233
Luxembourg, Grand Duchy of 199
Luxembourg, systems of 197, 199
Luxembourg traffic 198, 199
LUZ 233
Lyons, Captain Ulrich S. 4, 124, 139, 140, 204, 206, 211

Doc ID: 6554247

M-134 40
M-209, converter 247
M-325, converter 40, 282
M-228 282
M-409 282
M (13) key book 78
M Section 2, 4
Maas, Lieutenant Herbert H. 234, 235; (Captain) 22, 140, 238-240, 243
machine 29, 31, 38-40, 42, 45, 46, 50, 53, 84, 90, 91, 94, 95, 244, 245, 266, 269, 277, 280, 301
machine: 5202 239
machine, "A" 26, 29, 31, 32
machine, additive 92
machine, additive generating 91
machine attack 268
machine: Autoscritcher 243
Machine, "B" 31, 32-34, 39, 45-47
machine, basic 245
machine, British Colossus 239
machine, C-38 247
machine, captured 264, 284
machine cipher 159
machine, cipher for field use 247
Machine Cipher Section 57, 234, 237, 239, 240, 244, 246, 261
Machine Cipher Section, contribution of 240, 243
machine-cipher system, Japanese Army 240
machine-cipher system Purple 283
machine cipher systems, Finnish 300
Machine Cipher units 146
machine ciphers 21, 23, 26, 30, 51, 88, 236, 240 251, 261, 278
machine ciphers: Commercial Enigma 236
machine ciphers, cryptanalysis of 235
machine ciphers, enemy 284
machine ciphers: German Abwehr Enigma 236
machine ciphers: German Military Enigma 236
machine ciphers: German Teleprinter 236
machine ciphers: ITT 236
machine ciphers: Japanese Purple 236
machine ciphers: Japanese Red 236
machine ciphers: Swiss 236
machine ciphers: Wheatstone 236
machine, combined-operations cipher 282
machine, Commercial Enigma 234, 238
machine, complication of 245
machine, construction of 271
machine, copy 272
machine cryptanalysis, course in 235
machine cryptanalysis, training ground in 251
machine, cryptographic 13
machine devised by Dr. Joos 186
machine, diplomatic 30
machine, Dragon 239
machine, electronic 270
machine-enciphered messages 37
machine-enciphered traffic 46
machine, Enigma 238, 244-246, 258, 260, 264
machine-generated sequence 91

Doc ID: 6554247

machine, German 91
machine, German Enigma 13, 273
machine, German Kryha 235
machine, German-manufactured cipher 146
Machine, Green 284
"machine gun, the" 265
machine, Hagelin 167, 235, 236, 247, 255
machine, Hagelin, analysis of 250
machine, Hagelin cipher 247
machine, Hagelin letter-subtractor 256
machine, hand-operated 45
machine Hebern 236
machine hours 262
machine index 165, 167
machine index of traffic 161
machine indexes 198
machine IT & T 234
machine, Japanese Purple 235, 295
Machine, Kryha Cipher 83
Machine methods 81, 87, 277
machine methods, development of 268
machine problems, Tunny 239
Machine "Purple" 30, 36, 45, 48, 50, 51, 277
Machine, "Red" 26, 29-31
machine, the "003" 236, 237, 242-244, 246
(See Bombe and also volume IX)
Machine Room 141
machine settings, method of reconstructing 248
machine, solution of 42
Machine, solution of "B" 31
Machine, solution of the "Purple" 31, 58
machine, teleprinter 238
machine, Tunny 239
Machine Unit 80, 81
machinery 260
machinery, cryptographic 281, 284
machinery, IC 273
machinery, maintenance of 273
machinery, operation of 273
machinery, rapid analytical development of 271
machinery, rapid cryptanalytic 76
machinery, request for 271
machines 90, 234
machines, additive 272
machines, American 273
machines, analysis of 282
machines, automatic 45
machines, cipher 29, 234
machines, cipher, analysis of 285
machines, cryptanalytic 285
machines, electromechanical 73, 236
machines, IC 277
machines, Japanese cryptographic 45
machines, Japanese diplomatic Red and Purple 234
machines, M-228, M-325, M-409 282
machines, maintenance of German 94
machines, prototype of new 239
machines, regeneration 279
machines, source of German 95
machines, teletype 210
machines without endplate plugging 282
MacLeod, Miss Marjorie (Mrs. Max-Muller) 118, 236
Madrid 75, 108, 159, 221, 241
Madrid-Tangier messages 75
mail, intercepted 220

Doc ID: 6554247

maintenance crew, bombe 263
maintenance of bombe frames routing of 264
maintenance of machinery 273
maintenance of the "003" 237, 264
maintenance of X 68009 258
Maloney, Lieutenant Clifford J. 207, 208, 219
Maloney, Lieutenant Francis E. 289; (Captain) 228, 231
man hours 73
Mann, Lieutenant E. G. 191
manual 247, 287
manufacturers, German 95
margin of error 271
mariners 204
Marshall, General George C. 11, 50, 259, 260
Marston, Lieutenant E. Dale 113, 235; (Captain) 237, 264, 273 (Major) 234, 237, 257, 263
Martin, Mrs. Julia 292
Marton, Sergeant Edwin 207, 208
Mascotte Commercial Code 160, 168, 303
Masenga, Lieutenant Robert C. 155, 263, 276
Massarsky, Sergeant Irving 54
master additive chart 63
matching of cipher text 283
material 45, 60, 63, 70, 79, 90, 91, 93, 150, 166, 215, 222, 223, 238, 241, 289, 291, 303
material, captured 110, 118, 219
material, classified 210
material, compromised 85, 92, 295, 300, 302, 303
material, crib 262
material, cryptanalytic 16, 77, 242
material, cryptographic 219, 251, 302
material, current 28
material, deciphered 195
material, destruction of 297
material, documentary 292
material, examination of 224
material, exchange of 16, 179
material for key recovery 201
material, heterogeneous 141
material, indexing of 292
material, instructional 1
material, intercept 259
material, Japanese 24
material, lack of 121, 220
material, old used in new systems 302
material, priority 92
material, source 82
material, stenographic 222
material, unenciphered 144
material, useless 298
materials 109, 300
materials, captured 108
materials, code 74
materials, cryptographic 75, 108, 286
materials, foreign cryptographic 107
materials, instructional 284
materials, key 74
materials, uninterrupted flow of 18
materiel, enemy 92
materiel, French 222
mathematical relationship 201
"Mathematical Theory of Related Cipher Alphabets" 284, 285
matrices 135, 136
matrix 52, 178, 283

Doc ID: 6554247

matrix, transposition 274
matrixes 55
Max-Muller, Mrs. (Miss Marjorie MacLeod) 112, 236, 240, 261, 263
McCann, Miss Betty 154, 157
McCartney, Captain Ralph J. 10
McComas, Sergeant Frederick 118, 236
McCormack, Colonel Alfred 20
McCown, Captain Donald 80
McCoy, Mr. Angus 228
McCracken, Lieutenant 106, 107; (Captain) 98, 104, 107
McCurdy, Lieutenant Raymond R. 148, 150, 152, 156, 221
McDonald, Miss Keturah 206
McElwaine, Miss Naomi 203, 231
McFarland, Mrs. George B. 189
McGee, Lieutenant Carl 151, 154
McGee, Mrs. Evalyn 293
McMillan, Miss Nell 221
McReynolds, Miss Charlotte 191
McShane, Lieutenant Rudolph 181
McVittie, Dr. George C. 212, 213
McWhorter, Miss Nancy 149, 154, 155, 234, 236, 238, 240, 241, 263
mechanical functions of X68009 258
mechanical means of scritching 268
mechanical means of sliding crib against intermediate cipher text 239
mechanical tasks 293
mechanical techniques 15
mechanics of the "B" Machine 45
mechanism 30, 38, 265
mechanisms, cipher 39
mechanized procedures, cryptanalytic 282
Mediterranean Theater 208
medium tank, Japanese 92
meeting 257
Memorandum re Finnish traffic 256
Mendelsohn, Dr. Charles J. 82
menu 264
menus 262
menus, methods for making 264
menus, number handled on the 003 265
menus, plugging 264
menus, simultaneous testing of 265
Merano 241
Mertz, Mr. 257
message 33, 36, 57, 62, 84, 88, 90, 95, 135, 138, 145, 156, 176, 201, 244
message, acknowledgment of 226
message, "B" Machine 36
message beginnings, stereotyped 77
message, Code-Instruction 134
message, collective 217
message, corrected 179
message, cryptographic-instruction 55
message, "D" net 242
message, decipher of 47
message, decipherment of 227
message, encode 65
message, English-text 41
message, first read in LBA 203
message, hidden 224
message, new, examination of 231
message number 78, 141

Doc ID: 6554247

message, OWI 255
message part, setting of 267
message, plain-text 249
message print 105, 141, 160, 168, 195
message prints, IBM 184
message, sample 273, 291
message, Swedish 250
message, SYA 178
message, SZD 143
message, test of 232
message, time and place of 211
message, translation of 192
messages 3, 4, 25, 31, 32, 37, 38, 40--43, 45, 46, 50, 53, 59, 60, 64, 70, 71, 74--76, 81, 85--87, 92, 107, 108, 110, 116, 120--122, 126, 127, 130, 134, 136, 137, 141, 146, 154, 156, 162, 164, 168, 179, 186, 189, 192, 218, 219, 227, 229, 233, 240, 242, 245, 246, 253, 266, 267, 271, 278, 283, 300
messages, aligning of 254
messages, BCZ 161
messages, beginning of 35
messages, Brazilian 161
messages broadcast 215
messages, cipher 246
messages, circular 75, 99
messages, code 127, 141, 142
messages, code-instruction 252, 268
messages, contents of 1
messages Costa Rican 148
messages, cryptographic, Buenos Aires ban on 252
messages, cryptographic information 291
messages, cryptographic-instruction 28, 72, 89
messages, current 102, 175, 193
messages, deciphered 26, 71--73
messages, enciphering 26
messages, deciphering of 13
messages, decipherment of 251, 252
messages, decoded 71, 116, 165, 203, 293
messages, decoding of 294
messages, decryptographed 185
messages, decryptographing 292
messages, delayed 218
messages, diplomatic 203
messages, dud 266, 267
messages, enciphered 273
messages enciphered by the Swiss Enigma 237
messages enciphered in same key, location of 218
messages, enciphered, methods of solution 275
messages enciphered with same indicators 282
messages, encoded 136, 141, 178
messages, English 225, 231
messages, English-text 37
messages, Finnish 274
messages, FMS 133
messages, French 116, 124, 127, 128, 225
messages, GEC 301
messages, German 225
messages, German, cribs for 214
messages, German teletype-writer cipher 276
messages, group of 77
messages, Hagelin, method of placing 256
[redacted]
messages, Hagelin, statistical solution of 250

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

Doc ID: 6554247

messages, hidden 220
messages, "I" 75
messages, important 193
messages in CNL 186
messages, in depth 158, 255
messages, intercepted 49
messages, interception of 166
messages, Italian 214, 225
messages, JAA 277
messages, Japanese 49, 225
messages, Japanese Army 276
messages, Japanese diplomatic Purple machine 277
messages, Japanese Military Attaché 260
messages, JAS 70
messages, JBC 60
messages, JBH 243
messages, Liberian 203
messages, logging of 142
messages, London-Tokyo 69
messages, machine enciphered 37
messages, Madrid-Tangier 75
messages, not decoded 49
messages, not translated 49
messages of special importance 184
messages, numbers on Balkan 194
messages, older 105, 215
messages, open code 226
messages, overlapped 91
messages, overlapping of 77
messages, personal 203
messages, placement of 71, 91
messages, plain-text 70, 127, 142, 223-225
messages, POD 165
messages, Portuguese 161, 225
messages, radio service 291
messages, reading of 268,296
messages received 225
messages, repeated 74
messages, secret 26
messages, secret diplomatic 146
message serial number 65
messages, solution of 167, 213, 266
messages, solved 73
messages, Spanish 214, 225
messages, speed handling of 87
messages, superimposition of 211
messages, Swedish diplomatic Hagelin 273
messages, Swedish, method of superimposing 248
messages, Swedish plain-text 247
messages, Swedish, solution of 248
messages, test 234
messages, test of 245
messages, text of 37, 213
messages, Thai 189, 190
messages, translated 3
messages, translation of 231
message, transmittal of 28
messages, TUH 177
messages, Turkish 177
messages, unintelligible 225
messages, unread 91
messages, Washington-Helsinki 251
Meteorological Code, International 4,204,205,210
Meteorological Code, International, Japanese nonuse of 216
meteorological conferences, international 216
meteorological information 204

Doc ID: 6554247

meteorological observer 207
meteorological systems, Japanese 273, 274
meteorological systems solution of 204
meteorological traffic, solution of enemy 206
meteorologist in Air Corps 207
meteorology 216
method 87, 141, 183, 249, 267, 274, 284, 300
method, cryptographic, grouping of subsections in accordance with 153
method, direct 301
method, double input 265
method, experimentation in 183
method for conversion 42
Method for the Solution of the GEQ Indicator System 234, 242
method, hand 284
method, horizontal-vertical 256
method IBM 248, 284
method of analysis, Morgan's 248
method of attack 42
method of attack, organization based upon 103
method of dud solution 266
method of flag analysis 239
method of operation, British 261
method of placing Hagelin messages 256
method of reconstructing machine settings 248
method of solution 242, 250, 284
method of speeding testing process 224
method of superimposing Swedish messages 248
method of using additive cards 134
method of using keys 134
method, overlap 84
method, probable word 211
method, scritching 243
method, undercover 299
methods 46, 200, 261, 264, 299
methods, analytic 61
methods, cryptanalytic 286
methods, deciphering 81
methods, decoding 81, 92
methods for making menus 264
methods for speedy decipherment 252
methods, Greek cryptographic 301
methods, hand 92, 273
methods, high-speed RAM 128
methods, IBM 174, 211 218, 242, 251
methods in use 242
methods, machine 81, 87, 277
methods, machine, development of 268
methods of analysis 242
methods of cryptanalysis of systems 286
methods of Enigma cryptanalysis 238, 241, 257
methods of identification 292
methods of overlapping traffic 134
methods of solution 234, 238, 249
methods of solution, Bombe 267
methods of solution of enciphered messages 275
methods of solution, rapid 268
methods of using film projectors 276
methods, production 71, 87

Doc ID: 6554247

methods, second-storey 251, 296
methods, statistical 251, 252, 256
Mexican ciphers 14, 150
Mexican cipher systems 148
Mexican cipher traffic 149
Mexican code traffic 149
Mexican codes 150, 152
Mexican Diplomatic Section 2
Mexican, etc. (B-4) 3
Mexican government 147
Mexican "Guion" cipher 150
Mexican keys 14
Mexican MXC 155
Mexican traffic 148
Mexican two-alphabet cipher 150
Mexico 159
Mexico City 168
Mexico City circuit 167
Mexico City traffic 166
Meyer, Mr. Luther 191
MI-8 15, 18, 24, 82, 147
MI-8, Chief of 26
MI-8 files 24
MI-8 in New York 62
MI-8 personnel 24
MI-8, Shorthand Subsection 222
Michigan 254
Mickle, Mrs. Olive 292
microfilms 21
Middle East 170
Middle East, governments of 176
Middle East, systems of 172, 177
Middle Eastern countries 174, 179
Middle Eastern diplomatic systems 17
Middle Europe 180
Middle European systems 181, 190
Mihailovic, cipher used by 194
Miles, Major General Sherman 48, 49
military abbreviations 136
military attaché 24
military attaché ciphers, Bulgarian 192
military attaché, communications, Japanese 7
Military Attaché, German 244
military attaché in Rio 300
Military Attaché messages, Japanese 260
military attaché problems, Japanese 78, 79
Military Attaché Section, Japanese 118, 181
military attaché system 159, 187, 188
military attaché systems 63, 77
military attaché systems, Japanese 24, 62
military attaché-work, Japanese 222
military attachés 70, [redacted]
military attachés, Japanese 64, 76
military attachés, Royalist 108
Military Censorship, documents passing through 223
military cipher BUC 193
military cipher, French 135
military ciphers 167, 192
military code, two-part 136
military codes 109
Military Cryptanalysis 236, 273
Military Cryptanalytic Branch 11, 102, 119, 124, 133, 284

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

Doc ID: 6554247

Military Enigma 237, 244
Military Enigma, German 234, 236
military field, Japanese 284
military, French B-211 244
military information 232
military intelligence 50, 52
Military Intelligence Service 20, 57, 58, 229, 232, 303
military machine cipher, French 245
Military Mission, French 135
military operations 20, 109
military operations, planning of 204
military operations, reports on 137
military personnel 164, 172
military systems 19, 297
military techniques 52
military traffic 187
Military Traffic Analysis Branch 290
Millard, Mr. Francis R. 81
Miller, Lieutenant Donald C. 114
Miller, Mr. Kenneth D. 48
Miller, Miss Pauline 201
Minckler, Lieutenant Colonel R. W. 16
Ming Code, Chinese 182, 185
Ming traffic 182
Ministry of the Interior 109
"Minutes of Conference" 16
Miquelon 18
Miquelon code, capture of 113
MIS 92
MIS, Director of 92
MIS liaison officer 20
Miscellaneous Cipher Unit 153, 154
Miscellaneous Diplomatic Section, Officer in Charge 208
Miscellaneous Service Units (B-1) 6
miscellaneous services 290
miscellaneous subsection (B-1) 6
miscellaneous systems 95, 197
miscellaneous traffic 22
miscellaneous writings 286
Missko, Private Margaret 200
missing letters 34
mission 111, 154
Mission, Cipher Security 111
mission of the Agency 229
mission, Sinkov 100
mission, Sinkov-Rosen 11, 12, 13, 15, 17
mission to England 11
missionary 181
missions, German diplomatic 83
missions to England, Mr. Friedman's 12
missions, weather 205
mistakes in routing and identification 290
mixed alphabets 32, 65
mixed key sequence 129, 135
mixed sequences 66, 72--75
Moak, Mr. James 113
modern Arabic terms 174
modern Greek 190
modification 276
modification of equipment 276
modification of RAM equipment 275
Molstad, Captain Perry 6, 248, 249; (Major) 9

Doc ID: 6554247

monitor stations 49
Monmouth, Fort 163
monoalphabetic 39
monoalphabetic substitution 194, 202
monoalphabets 39
Monrovia 86
monographic coincidences 271
monthly information letter 21
Montooth, Miss Martha 149
Moore, Dorothy 80
Moore, Mr. Robert O. 119
morale 61, 222
Moran, Lieutenant William 273
Morgan, Captain G. W. 247
Morgan's method of analysis 248
Morocco 222
Morris, Miss Charlotte 120, 127, 149, 197, 199
Morris, Pfc. William S. 207
Moscow 31
Moscow, attaché in 78
Moss, Mrs. Frances R. 102, 106
motion 258
motions, wheel 242
Moulton, Miss Betty (Mrs. Leonard) 159, 294
move to Arlington Hall 6
multiple exposures 275
Mundinger, Lt. G. H. 82
Munitions Building 103, 115, 119, 148, 206, 209
munitions production 92
Munn, Dr. Katheleen 112
Murdock, Miss Isabel 54, 236
Murray, Miss Mary G. 221
Mussolini, fall of 105, 106
Mussolini government 108
MXA 150, 153, 156, 159, 294
MXB 150, 153, 156, 159, 294
MXC 148, 150, 155
MXD 148
MXE 148, 150, 155
MXG 150
MXH 148
Myers, Sergeant Hugh 207, 208
Myers, Lieutenant Wilbur 162, 163

Nagel, Mrs. Marion 118
name, cover 64
names, appendix of proper 161
names, Russian place 64
names, ship 248
Nanking government, traffic of the 185
Nanking puppet government 180, 189
National Cash Register Company 272
National Military Council in Chungking 188
nations, western, Japanese and 216
naturalized Americans 172
naval attaché 24
naval attaché system 24, 188, 244
naval codes 109, 129
Naval Enigma, German 260
Naval Observatory in Washington 206
naval operations 137, 204
Naval Section GCCS 21
Naval stations, United States 217

Doc ID: 6554247

naval system 19, 121, 216
naval traffic, German 19
Navy 84, 217, 269, 271, 287
Navy Code and Signal Section 30
Navy Codes 24
Navy, collaboration with 58
Navy, communications, German 13
Navy Department Bureau of Ships, assistance of 272
Navy, Italian Ministry of the 108
Navy, liaison with 208
Navy (OP-20-G) 257
Navy system 123
Navy term 272
Navy, the 121, 122, 129, 219
Navy, United States 19, 30
Nazi government of Bulgaria 180
Nazi operations 83
NEA 254
NEA keys 256
NEA, reconstruction of base settings 255
Near and Middle East Section 170, 176, 179, 199
Near and Middle East Unit 132, 197
Near East 170
Near East, countries of 174
Near East, Government of 176
Near East Section .301
Near East, systems of 172, 177
Near Eastern countries 179
Near Eastern diplomatic systems 17
Near Eastern reactions 179
Neff, Lieutenant P. E. 101
negative results 225, 226
negative weighting 277
negotiation 272
negotiations 36, 271
negotiations, diplomatic 108
negotiations with Finland 252
Negro civilians 231
Nelson, Mrs. Antoinette 140
net, "A" 241
net, Japanese domestic 22
net message "D" 242
net, Spanish diplomatic 157, 158
Netherlands Army 54
Netherlands cipher bureau 54
Netherlands East Indies 216
Netherlands Hagelin NEA system 254
neutral capitals 164
New Problems Unit 82
new systems 26
New York 221, 238, 254, 257, 273
New York circuit 166, 168
New York City 227
New York, MI-8 in 62
New York Public Library 254
Newfoundland, station at 259
news reports 120
news, summary of 286
newspaper articles 223
ni 35
night work 44
Nisei, Vint Hill Farms Station 10
Noel, Lieutenant Victor A. 123, 133, 140, 144, 145
nomenclature, standard 287
non-carrying arithmetic 214
Noncommissioned Officer in Charge 4
non-Hagelin systems 253
non-Morse transmission 238
nonrepeating key 40
non-secret Italian commercial code 105

Doc ID: 6554247

nontextual groups 69
norm 5
North Africa 222, 260
North Africa, Armistice Commission in 222
North Africa, German occupation of 222
North African invaision 113, 120
North Africa, operations in 213
North African landings 211
North African Theater 208, 213
North China 182
Northern, Sergeant George 207, 208
notches 238
notches, addition of to rotors 282
notebooks, captured 222
Notes on the RIK-5--JRN-4 62
notes, shorthand 222, 223
noun index 74
Novak, Mrs. (Miss Kathryn Clark) 122
nucleus 176
nulls 283
number, message 141
number, serial 136
number to indicate location 205
numbers 34, 70, 141
numbers, circular 86
numbers on Balkan messages 194
numerals 64
Nummeriermaschine 94, 95
Nummerierwerk 94, 95

oath required by British 13
O'Brien, Miss Ann 126, 127, 149
observation stations 212
observations 78
observations of terrain 222
observations, weather 204, 216, 218, 219
Observatory in Washington, Naval 206
observed weather 215
observer, location of 205
observer, meteorological 207
obsolete system 166
obstacles to solution 284
occupation of Iceland 85
occupation of North Africa, German 222
occupied lands 229
odd and even days 58
odd kick, keys involving only one 250
Office of Censorship 150, 220, 223
Office of Director of Communications Research 16, 17, 46, 258, 298
Office of Director of Military Training 287, 288
Office of Naval Communications 48
Office of Strategic Services 174
Office of War Information 255
officer 221
Officer, British 57
Officer Candidate School 120, 163, 200
officer, GCCS liaison 21
officer, German, diary of 222
Officer in Charge 3, 4, 6, 9, 10, 101, 162, 206, 230, 231, 293
Officer in Charge B-III Control Unit 289
Officer in Charge (B-III) Cipher Section 236, 250
Officer in Charge, B-III-f 54
Officer in Charge Code Unit 104

Officer in Charge
Miscellaneous Diplomatic
Section 208
Officer in Charge
Romance Language Section
101, 113
Officer in Charge, SIS
257
officer in charge, white
231
officer, liaison
20--22, 73
officer, Reserve 206
officers 9, 132, 139,
162, 208, 230
officers, American 13, 14
officers, commissioned
210
officers, control 263
officers in charge 229, 231
officers, liaison 13
Officers, Reserve 101, 103
offices, conversations in
228
official, Spanish 298
"OG" Code 27
Okamoto 31
Oliver, Dr. Revilo P.
149, 151, 160--163
commissions, random 142
O'Neill, Lieutenant J. C.
129, 155, 230
one-part code
83, 152, 161, 174, 182
one-time pad 219
one-time pad (GEE) 300
one-time pad, German
244
one-time pad, random 296
one-time pad system
83, 88, 285
one-time system
78, 88, 93, 302
one-time systems, American
94
OP-20-G
21, 24, 188, 255, 257, 268,
271, 282
OP-20-G, cooperation with
23
OP-20-G, liaison officer 21
open code 150, 219, 220,
223, 226
open code, first solution of
223
open code messages 226
open code, problem in 225
open-code problems 220, 228
open code, testing for
224
open codes 221
opera, pocket volume on
227
operating sections
280, 281, 286
operation 54, 138, 260,
270, 274
Operation and Control of
the 003 237
operation, British 17
operation, British method of
261
operation, cryptanalytic 115
operation No. 98 224
operation of B-III 286
operation of Electromatic
typewriters 272
operation of machinery 273
operation time of the 003 265
operation, turret 263
operational 2
operational activities 281
operational basis 264
operational jobs 263
operational liaison 78
operational procedure 257
operational procedures,
developed at GCCS 239
operational subsection of
GCCS 269

Doc ID: 6554247

operational use 274
operational work 262, 273
operations 4, 7, 10, 19, 103, 107, 112, 115, 161, 219, 230, 231, 262--264, 269, 273, 277, 281, 289, 298
Operations A Building 210, 235
operations, aeronautical 204
operations, Allied 260
Operations B Building 104, 210, 236
operations, Bombe 264
operations British 260
operations, British "E" 13
operations, combining 7
operations, cryptanalytic 7, 295
operations, Enigma 260, 269
operations, GCCS 20
operations in North Africa 213
operations, linguistic 7
operations, military 20, 109
operations, military, planning of 204
operations, naval 204
operations, Nazi 83
operations, reports on 137
operations, reports on military 137
operations, testing 224
operations, Yellow 263
operator 267
operators 206, 209
operators, bombe 263
Orange 240
order, reverse 141
order, wheel 267
Organization 1, 2, 8, 11, 54, 80, 115, 162, 206, 261, 263, 280, 286, 293, 302
organization around languages 103
organization based on method of attack 103
organization, British units 19
organization, Cryptanalytic Branch 10
organization: divided arrangement 156, 157
organization, four-fold 8
organization, linguistic 104
organization, new principle of 5
organization, SIS administrative 103
organizations 18
organizations, special 197
Orient, the 53
oriental countries 172
orientation 206
OSS 300, 303
Ottawa 18, 60, 138
out-of-date cribs 238
output, increased 179
overall priority 290
overlap 73, 158
overlap group 80
overlap method 84
Overlap Unit 71
overlap work 73, 80
overlapped messages 91
overlapping 212, 274
overlapping of messages 77
overlapping traffic 134
overlaps 70, 71, 76, 91, 93, 133, 201, 274, 278
overlaps, recovery from 73
overseas 113, 157, 189, 209, 240
overseas duty 119, 132
Oxford 12

Doc ID: 6554247

P-1 27
PAA 303
packages 78
Packard, Lieutenant Robert F. 54; (Captain) 24
pad additives 158
pad, German one-time 244
pad, one-time 219, 296, 300
pad patterns 300
pad sheets 92
pad system 88
pad system, one-time 93
pads 89, 90
pads, captured 88, 89
pads of additive 89
pads of key sheets 88
pads, reconstruction of 285
page 65, 70, 76, 89, 94, 143
Page, Miss Elizabeth 263
page, key-book 70
page letter 69
page symbols 142
pages 79, 142, 165, 218
pages, BZC 161
pages of keys 219
paginations 184, 188
paginations of BUA 192
paginations processing of 193
pairing 268
Palestine 171
Panama 82, 85, 127, 160, 298
Panama, agent in 89
Panama Canal 88
Panama Canal Department, Headquarters 98
Panama Canal Zone, Quarry Heights 147
Papandreou government 192
papers, technical 287
paragraph 35
paragraph headings 64
Paraguay 153
paraphrased version 36
paraphrasing 36
Paris 31
"Park", the 17, 20
Parker, Miss Alma Earle 263
Parks, Dr. Edd W. 118
partial cribs 74
partial substitution tables 85
Pasadena, California 213
passages 50
passages withheld 49
patience 136, 253
pattern 56, 142, 183, 271
pattern, additive 56
pattern, indicator 195
pattern limitations 96
pattern of blanks 52, 55
patterns, repetition of 142
pattern searches 274
pattern, substitution 166
pattern, transposition 166
pattern, wheel 238, 244
patterns 301
patterns, key, fitting of 250
patterns of blanks 53
patterns, setting of 276
patterns, transposition 283
paucity of text 41
PC-152 (FAC) 302
PC-155 (FAD) 302
PC-146 (FAH) 302
PC-148 (FAV) 302
PEA 303
peace time 204, 212
Pearce, Miss Kathleen 221
Pearl Harbor 78, 148
Pearl Harbor attack 2, 16, 23, 48
Pearl Harbor disaster 49
Pearl Harbor investigation 13, 31, 48
PEB 303
Peebles, Miss Sally 173, 199
Pekare, Miss Bertha 200

Doc ID: 6554247

Peking 31
Pentagon, the 209, 213
pentagraphic code 99
pentagraphic system 168
pentagraphs, sequence of 253
pentanomic code 133
pentanomic group 120
period 34
period 112
period, "E" 70
period, establishment of 194
period, experimental 263
period, G 79
period, I 278
period, J 278
period of division, the 115
periodic changes 66
periods 112
periods, cryptographic 250, 251
periphery of wheels 94
permanent record 286, 287, 291
permission 161
permitted German messages 225
permutation table 64, 160, 163, 232
permutations 33
permutations of the code group 145
permutations, tables of 231
Persian 171, 302
Persian script 174
Persian systems 170, 175
personal diaries, captured 222
personal messages 203
personnel 44, 45, 55, 60, 61, 73, 79, 80, 89, 90, 102, 103, 126, 131, 139, 145, 153--155, 159, 164, 176, 191, 208, 210, 228, 229, 231, 232, 237, 241, 253, 261--263, 273, 280, 281, 292, 301
Personnel (A-1) 3
personnel, addition of 179
personnel, additive recovery 103
personnel, Bell Telephone 263
personnel, British 260, 266
personnel, changes in 229
personnel, clerical 89, 163, 237
personnel, clerical, shortage of 263
personnel, cryptanalytic 81, 237, 260, 263
personnel, cryptographic 297
personnel, destruction of 260
personnel, enlisted 264
personnel, high-grade 243
personnel, increase in 248, 249
personnel, JMA 81
personnel, lack of 102, 152, 168, 182
personnel, less highly trained 264
personnel, linguistic 192, 193, 302
personnel loss 103
personnel, military 164, 172
personnel, new 118, 192
personnel of MI-8 24
personnel, reassignment of 60, 294
personnel, reduction in 132
personnel, rotation of 281
personnel, saving of 302
personnel, Signal Corps 213
personnel, Signal Security Agency 260

Doc ID: 6554247

personnel, shifting of 163
personnel, SIS 29
Personnel Study of Berkeley Street Prepared for Arlington Hall 21
personnel, traffic 194
personnel, trained 171, 179
personnel, training of 195, 237
personnel, transfer of 133, 157
personnel, translator 81
persons, prominent 174
Peruvian code book 303
Peters, Miss Ruth 159
Petersen, Mr. Joseph 54
Pettengill, Dr. Ray W. 82, 236, 245, 261
Pettengill, Mrs. Ray W. 114
Pfeiffer, Lieutenant Paul N. 207; (Captain) 208
Philippine systems 191
Philippines puppet government 180
Philips Export Company 226
Phillips, Dr. Burton 102, 103
Phillips Code 34
Phillips, Captain Edwin R 118
philological knowledge 171
photoelectrical principle of evaluation 271
photograph 108, 167, 284, 296, 297
photograph of British reconstruction of CNB 183
photograph of code book 99
photograph of YOA 192
photographed code books 158, 302
photographic copies 157, 300, 301
photographing 298
photographing of cards 283
photographing of code 299
photographing of data 239
photographs 127
photographs from French consulate 127
photographs from GCCS 201
photographs of British work on POD and POJ 165
photographs of compromised Iranian codes 174
photographs of copies 301
phrase books 182
phrases 34, 37
phrases, common 248
Phynes, Mr. Herman W. 231
"Pibal" type reports 212
pioneer work 113
place names, Russian 64
placing of Hagelin messages 256
placement of messages 71, 91
plain code 178
plain code (GED) 96
plain-code group 135
plain digraphs 62
plain equivalent 142, 219, 226
plain equivalents 64, 141
plain text 3, 34, 35, 37, 38, 41, 42, 45, 57, 72, 75, 84, 85, 107, 136, 141, 150, 156, 191, 202, 203, 226, 248; 251, 253, 275, 278, 300
plain text, captured 253
plain text, commercial 233
plain-text crib 70, 252, 282
plain-text digraphs 24
plain text, diplomatic 233
plain text, English 253
plain text, Finnish, study of 249
plain text, French 126
plain-text frequencies 174
plain text, Japanese 35, 49
plain-text letter 43
plain-text letters 3
plain-text message 249
plain-text messages 70, 127, 142, 223--225, 247

Doc ID: 6554247

plain text mixed with cipher 227
plain text, Portuguese 164
plain text, recovery of 73
plain text, Red Cross 233
plain text, reencipherment of 252
plain-text repetition 38
plain text, Swedish 247, 248
plain-text traffic 116, 232, 233
plain text, transposed 246
Plain Text Unit 154
plain-text values 33, 34
plain-text weather reports 211, 215
plain texts, compromised 246
plan 261
plan of History 11
plan of operation 261
Plan of Organization (B-3) September 1943 10
Planning and Priorities Unit 288, 290
Planning and Priorities Unit, contribution of 289
planning of operations 204
plans 258, 266, 268
plans, postwar 15
plate cameras, IC 279
plate equipment, IC 279
plate projectors, IC 276, 279
plates, glass 274
plates, IC 242
PLB 195
PLC, solution of 195
PLE 195
pledge to British, violation of 13
Pleshkova, Miss Nina 191
PLF 195
plugboard arrangement 39, 46
pluggable endplate 258, 282
pluggable reflector 242, 268
plugging, change in 267
plugging, endplate 237, 238, 243, 244, 264, 267, 268
plugging, endplate, conflicts in 265
plugging menus 264
POA 166, 167, 303
POB 166, 167, 303
POC 166, 303
pocket volume on the opera 227
POD 165, 166, 303
POE 166, 303
POF 165, 166, 303
POG 166
POH 166, 303
POI 165, 166, 303
point of view, British 261
point-to-point circuits 290
POJ 165--167, 303
POK 165, 167, 303
POL 167, 303
police work, code used in 109
policies of B-III 287
policy 6
policy, change in 176
policy of fluidity 163
policy of Research Section 281
Polish 191
Polish code 195
Polish code-recovery problems 195
Polish diplomatic systems 195
Polish government in London 180
Polish group 190
Polish systems 191, 194, 195
Polish traffic 194
political crises 137
politics 92
polyalphabetic cipher 147, 150
polyalphabetic encipherment 186, 203

Doc ID: 6554247

polyalphabetic substitution 278
polyalphabetic substituion cipher 108, 146
polyalphabetic substituion systems 27, 195
POM 303
PON 303
population observations of 222
POQ 162, 167
POR 166, 167, 303
Port au Prince digraphic substitution system (GEB) 83, 86, 96
Porter, Corporal Cecil 162; (Sergeant) 163
ports, Spanish 150
Portuguese 8, 113, 164, 233, 302
Portuguese-Brazilian Section 151, 164, 168
Portuguese-Brazilian systems 157, 163
Portuguese-Brazilian Unit 151
Portuguese cipher systems 167
Portuguese codes 165
Portuguese Codes and Ciphers 1941-1944 160, 169
Portuguese code traffic 149
Portuguese colonial office 167
Portuguese diplomatic code 167
Portuguese government 247
Portuguese Hagelin systems 254
Portuguese language 6, 161, 163, 164
Portuguese language traffic 162
Portuguese messages 161, 225
Portuguese plain text 164
Portuguese problems 163
Portuguese Section 132, 167
Portuguese system 149, 166
Portuguese systems 8, 112, 159-162, 164, 166-169, 294
Portuguese traffic 160 164, 168
Portuguese Unit 164, 166
Portznoff, Dr. Collice H. 102
position 168, 283
position in sequence 204
positions 32, 34, 271, 274, 277
positive results 226
positive weighting 277
possibilities 87
Post Committee on Terminology 287
Post Regulations 210
postwar plans 15
Pottberg, Lorna 80
pouches, diplomatic 297
POV 254
POW 254
powers, European 12
PPD 303
practical cryptanalysis 302
Prather, Mrs. Marvin 229
Prather, Miss Mary Louise 4, 48
preamble 231, 291
prearranged group 65
precision 143
predicted sequences 43
prediction of additives 90
prediction of keys 53
prediction of vocabulary 100
preliminary examination 183
Preliminary Historical Report on the Solution of the "B" Machine 234

Doc ID: 6554247

"Preliminary Report of Trip to England " 19
Prengel, Lt. A. T. 82
President, the 77
Presnell, Miss Dorothy M. 221
Press dispatches 221
press releases 223
presses, German job 94
pressure 91
Price, Miss Jehanne 106
Prime Minister, the 77
princes, Arabian 176, 178
principal Japanese attaché system, the 64
principal problem 81
principle of setting rotor 284
principles, basic 53
print, message 105, 141, 168, 195, 160
printed writings 286
printer 73
printing 94, 210
printing mechanism 245
printing unit 46, 279
prints, IBM message 184
priorities, temporary 290
priority, A-1 259
priority, assignment of 289, 290
priority duds 266
priority, evaluation of 290
priority jobs 265
priority material 92
priority rating 87
priority request lists 92
priority, top 47
prisoners, interrogation of 94
pro forma sheets 219
probability, relative 283
probable word 248
probable word method 211
probable words 249
problem 35, 44, 46, 48, 61, 62, 69, 72, 80, 82, 86, 87, 89, 91, 118, 140, 152, 175, 178, 194, 200, 202, 204, 226, 227, 231, 239, 243-245, 247, 254, 257, 261, 262, 268, 269
problem, cryptanalytic 179, 258, 277
problem, Enigma, the Army's answer 269
problem, FMC 129
problem, GEE 90
problem, German 83, 213
problem, German Enigma 235
problem, German military 19
problem, Greek 191
problem, Hagelin 248
problem, Japanese Army 11
problem, Japanese transposition 129
problem, linguistic 99, 302
problem, method of attack on 211
problem of Balkan systems, principal 193
problem of reconstruction 104
problem of solution 214
problem of transportation 210
problem, open code 225
problem, principal 81, 193
problem, Purple machine 284
problem, security 263
problem, solution of 248
problem, Thai 189
problem, transposition 52
problem, unsolvable 78
problem, weather 209
problems 55, 74, 82, 130, 133, 135, 164, 181, 184, 227, 237, 261, 263, 268, 271, 278, 280, 285

Doc ID: 6554247

problems, additive 55, 57, 132
problems, administrative 287
problems, British 21
problems, Chinese 194
problems, Chinese cryptanalytic 184
problems, Chinese language 186
problems, cipher 8
problems, cipher machine 237
problems, CNH 185
problems, code reconstruction 8
problems, code recovery 140, 302
problems, cryptanalysis of Japanese 207
problems, cryptographic 28, 47, 66, 76, 154, 173, 177, 191, 193, 287
problems, encipherment 131
problems, engineering 48
problems, Enigma 267
problems, Far Eastern 14
problems, French 112, 115, 119, 131, 132
problems, Hagelin 234, 235
problems, Italian 100, 107
problems, Italian diplomatic 13
problems, Japanese 25, 172, 176
problems, Japanese Army 8, 275
problems, Japanese diplomatic 54, 58
problems, Japanese military attaché 78, 79
problems, linguistic 139, 144, 182
problems, new 281
problems of additive recovery 283
problems of code recovery 101, 116
problems of encipherment 101
problems of recovering key 70
problems of solution 284
problems, open-code 220, 228
problems, Polish code-recovery 195
problems, Portuguese 163
problems, principal 83
problems, Rumanian 202
problems, Russo-Polish 138
problems, solution of 210
problems, Spanish 163
problems, Spanish-American 147
problems, special 251, 280
problems, special translation 116
problems, specialized cipher 154
problems, Swiss 119, 140
problems, technical 117
problems, traffic 192
problems, transposition 155
problems, Tunny machine 239
procedure 28, 86, 231, 232
procedure data 237
procedure, German cryptographic 303
procedure, indexing 184
procedure, operational 257
procedures 87, 205, 237, 243, 285, 261
procedures, British 17
procedures, cryptanalytic 236, 259
procedures in Enigma cryptanalysis 236
procedures, mechanized cryptanalytic 282

Doc ID: 6554247

procedures, operational, developed at GCCS 239
process 155, 210, 239
process, algebraic, of combining tables 252
process, conversion 42
process, enciphering 50
process, guessing 36
process of solution 284
processed traffic 167
processes, IBM 92
processing 112, 129, 152, 177, 191, 198, 203, 220, 221, 225, 237, 242, 293, 294
processing, IBM 73, 140, 174, 182, 241
processing of commercial traffic 229
processing of documents 220, 223
processing of German traffic 215
processing of new traffic 213
processing of radio-telephonic conversations 227, 228
processing of recordings 228
processing of telephone conversations 228
processing of traffic 47, 176, 290
processing of weather reports 214
Processing Unit 71, 194
Proctor, Mr. Mortimer 148, 150, 154, 155
production 60, 71, 74, 88, 92, 111, 118, 140, 183, 192, 193, 213, 254, 266, 288
production, aerial 92
production, cryptanalytic 250
production, linguistic 251
production methods 71, 87
production munitions 92
production of CZB 195
production of Hagelin cipher machine 247
production of intelligence 1, 28, 47, 133, 180
production of key 71
production of translations 192
production, speeding up of 73
production stage 153, 154
Production Unit 82
professional scholars 172
professional Semitist 171
Program, Army Specialized Training 172
program, training 1, 60, 173, 191, 208
program, WAC 263
progress 5, 63, 69, 78, 86, 90, 98, 100, 111-113, 118, 126, 136, 138, 142, 146, 148, 150, 161, 165, 180, 187, 188, 193, 213, 241, 245
progress chart 222
progress, cryptanalytic 163
progress of solution 287
progress report 212, 214
progress reports 24, 139, 170, 197, 220, 286
progress reports, exchange of with GCCS and EU 138
progress reports, file of 204
project 37, 157, 237, 258, 273
Project, Beechnut 264
project, bombe 259
project, special 291
Project, Yellow, the 257, 263, 264, 269
projector 272

Doc ID: 6554247

projector and camera, Tetragraph Tester 274
projector, IC film 275
projector, IC plate 276
projectors, film, methods of using 276
projectors, IC film 279
projectors, IC plate 279
projectors, Tetragraph Tester 279
projects 197, 278, 302
projects, cryptanalytic 1
projects, special 273, 289
prominent persons 174
proper names, appendix of 161
Proposed Supplementary Table of Organization, 1 July 1943 9
protection of our systems 254
protocol, matters of, Japanese attention to 216
Prouty, Dr. Charles 62, 79
provisional additive 301
public 50
publication 51
publication of commercial codes 229
publication of OP-20-G 24
publications of Recorders Group 24
Pulakos, Miss Elaine 190
punch controls 272, 278, 279
punch tape, 70-mm. 275
punches 278
punches, 70-mm. 272
punches, tape 272
punctuation 64, 70, 161
punctuation, group for 143
punctuation signs 34, 36
puppet Croatian government code of 193
Purple analogue 45
Purple intelligence 277
Purple Machine 13, 15, 30, 36, 51, 234--236
Purple Machine analog 277
Purple Machine cipher 59
Purple Machine cipher system 54, 283
Purple Machine Cipher Unit 54
Purple Machine, Japanese 295
Purple Machine messages, Japanese diplomatic 277
Purple Machine problem 284
Purple Machine, report on 45
Purple Machine, solution of 31, 45, 46, 48, 50--52

Q2 53
Q3 53
QAA 232
QAZ 233
QGA 233
Quarry Heights, Panama Canal Zone 147
quarters, contiguous 180, 185
Quereau, Mr. Edward 114, 119, 123
questioned documents 150
Quinn, Sergeant Patrick F 114
Quintana, Lieutenant Jose 149
quotations 37

RA 99, 104
RA-1 99, 101, 104, 105,108
Rada, Lieutenant M. E. 101
radar engineer 276
radio 49
radio broadcasts 223
radio communication 192
radio communications 291
Radio Intelligence Section, General Staff, France 221

Doc ID: 6554247

Radio Laboratory, Navy Yard 48
radio service messages 291
radiogoniometry 205
radiotelephone conversations 220, 227, 228
Rafferty, Mr. John R. 114
Ralph, Mrs. Dora 240
RAM 76, 239, 267, 272, 273, 277, 278
RAM, application of 278
RAM, contribution of 278
RAM cryptanalytic machinery 76
RAM development 277
RAM equipment 272--274
RAM equipment, designs for 283
RAM methods, high-speed 218
RAM equipment, modification of 275
RAM Procedure for Placing Cribs in a De-Chi 234
RAM Section 271, 273, 274
RAM studies 201
RAM Subsection 276
RAM tape 242
RAM, theory of 273
Randolph, Mr. Roger S. 20
random alphabets 147
random assortment of letters 35
random, at 38
random cipher square 278
random expectation 89
random (GEE) 89
random key 88
random-mixed sequence 66--68
random omissions 142
random one-time pad 296
random sequence 65
randomicity 90, 200
randomicity of American one-time systems 94
randomicity of GEE 93
range, alphabetical 161
"raob" type reports 212
rapid analytical machinery, development of 271
rare languages 179, 182
Raskin, Lieutenant Saul K. 118, 155; (Captain) 147
rating, priority 87
Ratser, Sergeant Earl M. 248
raw traffic 1, 49, 78, 300, 302
reactions, Near Eastern 179
readability 125, 196, 290
readable 1, 86, 87, 96, 105
readable systems 59, 86
readers 278
readers, tape 272
reading 301
reading of messages 268, 296
reading of stenographic documents 220
reading of traffic 294
Reading Unit 82
reassignment of personnel 60, 294
receivers 209
recommendation 282, 285
recommendations 254, 281, 285
reconstructed 35, 41
reconstructed systems 293
reconstruction 25, 35--37, 42, 43, 45, 46, 64, 68, 73, 76, 82, 96, 100, 122, 128, 129, 137, 160, 163, 165, 174, 183, 196, 202, 217, 300, 301
reconstruction, accuracy of 136
reconstruction, AR 25 code 101
reconstruction, code 5, 8, 70, 301, 302
reconstruction, Impero code 101

Doc ID: 6554247

reconstruction of base settings NEA 255
reconstruction of cipher squares 63
reconstruction of CNB, British photograph of 183
reconstruction of DESAB 96
reconstruction of FIE 253
reconstruction of key book 253
reconstruction of keys 91, 249
reconstruction of machine settings 248
reconstruction of pads 285
reconstruction of repagination 301
reconstruction, partial 102, 114, 145
reconstruction, problem of 104
reconstruction, square 278
reconstructions 99, 109, 110, 144, 167
reconstructions of code 14, 17
reconstructions, partial 143
reconstructors, code 96
record 228, 242
record number of solutions 266
record time 277
Recorder 288
Recorder's Group 285, 287, 288
Recorder's Group, contributions of 287
Recorder's Group publications 24
Recorder's Office, B-III 26
Recorder's Section 107, 185
recording 274
recording apparatus, adjustment of 264
recording a stop 265
recording on films 267
recording, systems of 228
recordings, German 228
recordings of telephone conversations 220
recordings, processing of 228
records 193
records, accounting for 292
Records and Distribution Unit 289
records, permanent 286, 287, 291
records, routing of 292
records, State Department 37
records, translation of Finnish 251
Records Unit 80, 81
recovered 91
recovered code values 125
recovered encipherment 128
recovered, intelligence 92
recovered key 56, 89
recovered keys 53
recovered lines 275
recovered text 100
recovered values 134
recovery 56, 64, 67, 69, 75, 77, 79, 85, 86, 90, 95, 125, 129, 176, 184, 187, 192, 202, 218, 219, 252, 278, 283, 293
recovery, additive 101-103, 105, 149, 157, 195, 200, 283
recovery, book 179
recovery, code 70, 101, 102, 103, 108, 114, 115, 116, 132, 133, 135-137, 144, 145, 149, 152, 156, 164, 175, 185, 186, 189, 193, 198, 199, 202, 203, 294
recovery, from overlaps 73
recovery, hand 243

Doc ID: 6554247

recovery, indicator 79
recovery, indicator key 72, 76, 87
recovery, key 71--74, 79, 96, 106, 155, 178, 193, 201, 241, 242, 300, 302
recovery of alphabets 195
recovery of basic square 285
recovery of code values 102
recovery of endplate plugging and reflector wiring, simultaneous 267
recovery of FBT 113
recovery of French unenciphered codes 124
recovery of JAS Square 278
recovery of JEV 243
recovery of key 54, 71, 84, 248
recovery of key book 83
recovery of plugging 268
recovery of reflector wiring 267
recovery of the "sixes" 48
recovery of two-day period key 87
recovery of values 166
recovery, speeded 87
recovery, square 73
recovery, statistical 283
Recovery Unit 56
recovery units, key 81
recovery work 71, 116
recruiting 172
Red Cross plain text 233
Red cryptograph 45
Red Machine, Japanese 26, 29, 30, 31, 234, 236
Red Machine, modification of 26
reduction of personnel 132
Reed, Mr. C. E. 82
reencipherment of same plain text 252
reference 143
reference catalogs 241
references 77
references, cross 141
references, library 300
reflector 243, 267-269
reflector, development produced by 242
reflector, fixed 258
reflector, pluggable 242, 268
reflector wiring and end plate plugging, simultaneous recovery of 267
reflector wiring, recovery of 267
reflexing circuit 282
regnerating units 272
regeneration machines 279
regimental units 109
registration of documents 292
regular channels 301
Regulations, Post 210
Reischauer, Mrs. Jean 116, 128, 293
Related Problems Unit 82
relations, diplomatic 179
relationship, mathematical 201
relative code groups 122
relative code values 120
relative probability 283
Relay Control, 70-mm. 272
relay bombe 260
relay device 284
relay frame, experimental 258
relay of Buenos Aires messages 252
relay switching system 257
relays 216
relined code 177

Doc ID: 6554247

remote operation of Electromatic typewriters 272
remote stations, difficulty of hearing 217
removal of encipherment from weather reports 205
reorganization 1, 3, 5, 6, 11, 58, 115, 117, 119, 130, 132, 153, 198
reorganization of 1943 7, 10
reorganization of Japanese Diplomatic Section 56
repaginated code 161, 177
repaginated version 158
repagination 105, 167, 301
repagination, reconstruction of 301
repaginations 185, 192
repeated messages 74
repeated sequences 43
repeated sequences, search for 41
repeated version 249
repetition 88
repetition, cyclic 3
repetition of patterns 142
repetition, plain-text 38
repetitions 84, 200
repetitions, causal 38
repetitions, search for 275
repetitions, three-digit 135
report 26, 48, 62, 125, 136, 147, 148, 160, 175, 209, 222, 301
report forms, Japanese weather 216
report, Major Kullback's 17
"Report of Technical mission to England" 12
"Report on 'E' Operations of the GC & CS" 19
"Report on IBM Operations" 19
"Report on 'ISSOS' and 'ISK' Sections" 19
report on Purple Machine 45
report on relative coverage 290
report on solution of GEQ indicator system 240
Report on solution of the Finnish 0000 and 17 systems 256
Report on solution of the Swedish Hagelin traffic 256
"Report on Visit to the Intercept Station at Cheadle and War Office Y Group" 19
report: Personnel Study of Berkeley Street Prepared for Arlington Hall 21
report: "Preliminary Report of Trip to England" 19
report, progress 212, 214
report, Sinkov-Rosen 12, 13
report, special 223
report: "Special Historical Report on the Solution of the 'B' Machine." 24
report, stereotypic 74
reporting, court 221
reports 19, 49, 78, 82, 127, 137, 138, 215, 217, 228, 239
reports, analysis of 261
reports, broadcasting of from Dakar 210
reports, German broadcasting of weather 215
reports, Italian 207, 212
reports, Japanese weather 207, 215
reports, JN-36 217
reports, land type 212
reports, liaison 288, 292
reports, MI-8 24
reports, negative 224
reports of Captain Fried 21
reports of Captain Seaman 21
reports of spies 87

Doc ID: 6554247

reports of the Swiss Section 139
reports on espionage 150
reports on weather conditions 213
reports, "pibal" type 212
reports, plain-text weather 211, 215
reports, progress 24, 112, 170, 197, 220, 286
reports, progress, exchange of with GCCS and EU 138
reports, progress, file of 204
reports, "raob" type 212
reports, ship type 212
reports, solution of 205
reports, special 217
reports, weather 4, 205, 206, 214, 218
reports, weather, broadcast of 204
reports, weather, Russian 211
reports, weather, solution of 206
representative, American 111
representative, diplomatic 147
representatives 298, 299
representatives, Axis 225
representatives of the Signal Security Agency at GCCS 292
reproducer, IBM card 277
reproduction 277
Republican Fascist government 107, 108, 110
request 37, 260
request for action, MIS 92
request for machinery 271
requests for traffic 290
requests from GCCS and EU 290
request lists, priority 92
research 40, 60, 71, 78, 79, 89, 90, 119, 122, 147, 157, 159, 163, 208, 233, 234, 237, 239, 245, 251, 257, 263, 271, 287, 302
research activities 265
research and development 51
Research Cipher Sections 140
research, continuous 289
research contracts 272
research, cryptanalytic 139, 189, 200
research, Enigma 267
research group 55, 71, 74, 90, 243, 244, 251, 267
research, indicator 79
research on discriminants 261
research on new systems 117
research paper 285
research, preliminary 131, 132, 145, 190
research purposes 238
Research Section 91, 280, 285
Research Section, B-III 55, 201
Research Section, B-III, contributions of 281
Research Section, contributions of 283, 284
Research Section, policy of 281
research specialists 280
research, specialized 281
Research staff 201, 282
Research staff B-III 284, 285
research techniques 73
Research Unit (B-III) 56, 57, 79-81, 183, 187, 193, 194
research work 300
researches on Czech systems 195

Doc ID: 6554247

Reserve Officer 12, 82, 101, 103, 206
resetting of wheels 91
resources 139
responsibility 176, 290
responsibility, allocation of 22, 289
responsibility, division of 19
resultant 150
resultant additive 85, 87
resultant additive key 84
resultant additives 86
resultant key 84, 253
resultant text 73
results, British 17
results, negative 225, 226
results of American work on Italian problems 13
results of British study 14
results, positive 224, 226
results, satisfactory 159
resumption of Italian traffic 213
retards 217
reuse of additives 89
reuse of keys 88
reuse of lines of additive 84
revelations of British 13
reverse order 141
revision 8
rewire of 003 frames 267
Rhodes, Lieutenant Commander 160
Rhodes, Mrs. Phyllis 155
Rice, Dr. James V. 147, 149, 152, 164, 201, 202
Rickhart, Dr. Margaret J. 102, 106
Riegl, Miss Viola 191
RIK-2 64
RIK-5 62
RIK-International 63
Rikugun 63, 64
Rikugunken 63
Riley, Miss Norma 154
Rio de Janeiro 86, 147
Rio, military attaché in 300
RIP--37 24
ROA 202
Roberts, Lieutenant Laurence P. 180-182, 184-186
Roberts, Miss Virginia 240
Robertson, Miss Lena 80
Robinette, Miss Annette K. 221
robot heads 272
ROC 202
Rochester, New York 273
ROD 202
rods, lucite 275, 279
ROE 202
ROF 202
ROG 202
Romance language 3
Romance Language Code Recovery Section 139
Romance Language Code Recovery Unit 151, 230, 202
Romance Language Section (B-III-a) 101, 113, 132, 202,
Romance language sections 132
Romance language traffic 160
Romance languages 113, 147, 163, 233
Rome 31, 110, 111, 147, 237, 241
Rome, German station in 213
Rome-Washington circuit 111
room turret 264
Rosebro, Miss Mary Neely 240, 244, 263
Rosen, Mr. Leo 48; (Lieutenant) 11, 12, 16, 257; (Captain) 257, 258
Ross, Miss Alda 159
Ross, Lieutenant Gordon W. 155, 157, 159; (Mr.) 160
rotary bombe technique 259
rotary electrical cryptographic elements 44

Doc ID: 6554247

rotary type Bombe 257
rotary commutator 32, 40
rotation in use of tables 158
rotation of personnel 281
rotation, use of systems in 25
rotor, setting of 284
rotors 40
rotors, addition of notches 282
rotors, Hebern-type 285
rotors, solution of 282
Rotter, Miss Helen 173
route transposition 129, 253
routine affairs 289
routine exchange 16
routing 232, 289
routing maintenance of bombe frames 264
routing, mistakes in 290
routing of records 292
routing of traffic 3, 6
Rowlett, Mr. Frank B. 2, 16, 29, 48, 53; (Lieutenant) 116, 154, 234, 248; (Captain) 249, 258 (Major) 6, 9, 59; (Colonel) 10, 22, 24, 132, 203, 245, 257, 261, 300
rows 65, 70, 75
Royalist government 107
royalist government of Greece 180
royalist government of Yugoslavia 180
Royalist Italy 109
Royalist military attaches 108
Rudolf Mosse Commercial Code 83, 96
Rumania 203
Rumanian problems 202
Rumanian systems 181, 197, 201
Rumanians, the 202
Rumanian traffic 201-203
run 265
run checking 263
run-checking job 264
running key 256, 278
running key, Hagelin-enciphered 252
running-key substitution 188, 253
running-key system 253
runs 265
runs, checking of 263
Rupp, Captain C. A. 251
Russell, Captain Franklyn F. 181, 182, 229
Russell, Sergeant Willis 114
Russia 177, 232
Russian codes 78
Russian, knowledge of 191
Russian place names 64
Russo-Polish problems 138
Russian systems 12, 78
Russians, the 203
Russian traffic, study of for training purposes 211
Russian weather reports 211
Rutledge, Dr. Leslie A. 118, 180, 184-186, 253, 256
Rutledge, Mrs. L. A. (Lieutenant Praxythea Coroneas) 190

safe key 299
safes, combination 297
Safford, Commander L. S. 48
Saigon 217
Salem, Lieutenant Joseph R. 118, 170, 171, 173, 175-177 208
Salt Gabelle 181
sample message 273, 291

Doc ID: 6554247

San Francisco
177, 178, 303
San Francisco Conference
178, 179, 192, 290
Santa Isabel 159
Santiago traffic 127
satellites, Axis 190
Saudi Arabia 170, 175
177, 178
Sauerwein, Jr., Mr. Henry A.
102, 103, 228
Sayre, Lieutenant George M.
126, 127, 149
Scandinavian language 253
scanning 277
scarcity of translators 49
"Scarlet" 64
schedules, broadcasting,
Japanese 217
Scherer, Miss Betty
236, 241, 263
scholar, classical 190
scholars, professional 172
school, B-I 61
School, Officer Candidate
163
Schukraft, Major R. E. 4
Schwab, Miss Anita 80
Schwartz, Lieutenant Benjamin
171, 173
science of climatology 211
science of cryptanalytics 285
scientific advance 92
Scovil, Miss Dudley
(Mrs. B. Hunt) 250, 255
script, Persian 174
scritching 243, 268
scritching, hand 269
scritching, mechanical means of
268
Seaman, Lieutenant John N.
247--249, 255, 256,
(Captain) 20, 21, 236,
250; (Major) 22, 112
Seaman, Dr. William M. 80
search 36, 253, 254
search for cribs 276
search for repeated sequences
41
search for repetitions 275
searches, pattern 274
Second Phrase Code, Bentley's
185, 187
Second Signal Service Company
3
"second-storey" methods 251
296
"second storey" work 298
secondary encipherment 167
secrecy, pledges 13
secret 47, 50
secret agents 76
secret Chinese system, most
186
secret cipher, Japanese 31
secret code 216
secret codes 182
secret communications
13, 31, 225, 282
secret communications, most
144
secret diplomatic code, most
177
secret diplomatic messages
146
secret ink 227
Secret Ink and Photographic
Laboratory (D Section)
3
secret messages 26
Secret Project X 68009
258
secret service agents 106
Secret Service, British
301
Secret Switching System
Project X68003 257
secret systems 12
secret text 227
Secret Writing Case,
Friedman 227
Secretaire General 136
Section I (Japanese Language)
9

Doc ID: 6554247

Section II (Japanese Military Cryptanalysis) 9
Section III, decline in requirements 9
Section III (General Cryptanalysis) 9
Section IV (Tabulating Machinery) 9
Section A (Administrative) 3
Section, Administrative 4
Section B (Cryptanalytic) 3, 6
Section C (Cryptographic) 3, 4
Section Cryptanalytic 4--6, 8, 10
Section D (Secret Ink and Photographic Laboratory) 3
Section E 5, 6
Section G 2
Section I 2
Section J 2
Section M 4
section, single 112
section, special 3
sections, British diplomatic 17
sections concerned with the 003 267
sections, operating 280
secure system 31, 52, 295, 296
security 30, 49, 51, 52, 83, 172, 214, 244, 259, 280, 283, 296
security, Allied 211
Security Branch 255
Security Division 282
security, increase in 280, 282
security of communications 26
security of espionage agents 299
security of our own communications 273, 285
security of systems 281
security problem 263
security reasons 12
security requirements 66
security, signal 287
security traffic, highest 88
Seele, Lieutenant Keith C. 133, 140, 144
Seidenglanz, Lt. Leonard J. 82
Sells, Miss Margaret 181
Semimonthly Report 286
Semitic languages 171
Semitist, professional 171
sentences 37
separate systems 170
separation of codes 153
separation of units 156
sequence 3, 35, 41, 53, 77, 224, 253
sequence, additive 108
sequence, cipher 30
sequence, key 65
sequence, machine-generated 91
sequence, mixed 66, 75
sequence, mixed key 129, 135
sequence of groups 214
sequence, position in 204
sequence, random 65
sequence, random-mixed 67
sequence, single-mixed 67
sequence solution 91
sequence, standard 66, 67
sequences 41, 46, 53, 79, 91, 136
sequences, additive 105
sequences, additive key 218
sequences, basic 43, 44
sequences, cipher 40
sequences, cyclic 41, 43
sequences, cyclically-repeating 40
sequences, key 136
sequences, mixed 72--74
sequences, predicted 43
sequences, random mixed 66, 68

Doc ID: 6554247

sequences, reconstructed basic 44
sequences, repeated 43
sequences, search for repeated 41
sequences, standard 66
sequences, symmetric 43
sequences, transposition 188
Serbian 222
serial number 136
serial number chart 66
serial number key chart, JAS 69
serial number key tables 66
serial number, message 65
serial numbers 71
serial numbers, JAS 69
series 141
series, consecutive 194
Series, Cryptanalytic 169
series of encipherments 168
service units 3, 6, 116, 280
services 5, 23, 280
services, information 4
services, miscellaneous 290
setting, clip 267
setting of a message part 267
setting of patterns 276
setting, rotor 284
setting, wheel 264
settings 39, 44, 92
settings, machine, method of reconstructing 248
settings of wheels 30, 91, 239, 245, 266
settings, reconstruction of 255
Shaffer, Miss Sophie 190
Shanghai 31, 32, 245
Shapiro, Mr. Hyman 207
sheets 300
sheets, crib 241
sheets, homogeneous block of 90
sheets, loose, captured 222
sheets, pad 92
sheets, pro forma 219
Sherer, Miss Betty 140
shift, swing 114
shifting 39, 43
shifting of personnel 163
shifting starting points 86
ship names 248
ship type reports 212
shipment, largest from GCCS 17
shipping firms 58
short course 163
shortage, traffic 59
shortcuts 243
shortening of work day 210
shorthand notes 222, 223
Shorthand Subsection, MI-8 222
shorthand textbooks 222
short title 64, 146
short titles 59, 60, 289
short titles, assignment of 291
short titles, list of 291
Siegel, Mrs. Helen 112, 119, 126, 128, 129, 131, 132, 281, 293
Sigafoose, Miss Clara 159
SIGCUM 280
SIGFOY, Converter M-325 40
Signal Corps 28
Signal Corps personnel 213
Signal Intelligence Service 1--3, 5, 11, 15, 16, 18, 24--26, 29--31, 36, 37, 48, 50, 63, 98, 103, 148, 160, 234, 247, 249, 257, 258
Signal Intelligence Service, Chief 12, 13, 16, 257
Signal Intelligence Service contribution to British 13
Signal Intelligence Service, expansion of 149

Doc ID: 6554247

Signal Intelligence Service fundamental task 28
Signal Intelligence Service, liaison officer 20, 21
Signal Intelligence Service, time of establishment 28
signal intelligence services, American 52
signal intelligence services, German 94
Signal Reserve 100
Signal Security Agency 1, 19, 22, 23, 59, 62, 69, 72, 79, 81, 84, 88, 90, 91, 94, 109, 111, 115, 117, 130, 131, 135, 136, 141, 144, 153, 156, 169, 176, 178, 188, 197, 209, 211, 221, 226, 238, 239, 243, 246, 248, 249, 258--263, 268, 270, 271, 273, 277, 278, 287, 288, 292, 295, 298, 299-301, 303
Signal Security Agency, achievements and failures of 287
Signal Security Agency, British contributions to 14
Signal Security Agency, files of 229
Signal Security Agency Headquarters Branch 9
Signal Security Agency, key members 287
signature 233, 259, 283, 291
signatures 86
signs, special 161
Silber, Dr. Gordon R. 106, 107
Silverstein, Lieutenant Maurice 152
similarities, cryptographic 39
similarity 5
Simonds, Lieutenant Stanley H. 119, 199
simplified code 178
Singapore, cipher section in 14
single-frame model of Dudbuster 266
single-mixed sequence 67
Sinkov, Dr. Abraham 2, 29, 48, 58, 62, 63, 98, 100, 147; (Captain) 11, 12, 16, 101, 102, 257; (Major) 4, 103; (Lieutenant Colonel) 13, 79, 245
Sinkov, Mrs. Delia A. 147, 148
Sinkov mission to GCCS 11, 13, 15, 17, 100
Sinkov-Rosen report 13
SINODEFENS 183
SIS (See Signal Intelligence Service)
Sittler Commercial Code 199
six wheel, the 29
"sixes", the 32-35, 37
skill 136, 180
skill, cryptanalytic 156
skills 103
Skinner, Lieutenant John 54
skips 32
SLA 193
Slavic languages 190, 191
slide-testing cipher 92
sliding crib against intermediate cipher text, mechanical means of 239
Slovak 191
Slovakian cipher (SLA) 193
Slovakian systems 191
Smadbeck, Lieutenant Louis 155
Small, Mr. Albert W. 22, 48, 53, 98, 235, 269, 280
SMFSA 272
Smith, Miss Helen 122
Smith, Miss Margaret 263
Smith, Mr. William S. 113, 115, 117, 118; (Lieutenant) 117, 118, 122, 129, 183; (Captain) 112,230, 240

Doc ID: 6554247

Smithson, Mrs. Nelle 288
Snodgrass, Miss Catherine 184
Snow, Miss Belinda 207, 211, 215
Snyder, Mr. Samuel S. 22, 24, 29, 48, 53, 54, 59, 60, 62, 63, 79, 80, 82, 98, 243, 281
Solar code book (CLA) 303
solenoid banks 272
solution 1, 2, 4, 8, 25, 28, 40, 42, 44, 51, 52, 55, 67, 71, 72, 74, 78, 82, 84--86, 88, 91--93, 96, 98, 105--107, 108, 111, 112, 114, 120, 129, 133, 135, 136, 142--144, 146, 148, 150--152, 154, 155, 161, 162, 166--169, 174, 175, 177, 178, 183, 184, 187--189, 200, 201, 203, 210, 211-213, 218, 230, 235, 239--242, 246, 252, 254, 260, 262, 264--269, 286, 295, 299, 303
solution and analysis of the Hagelin letter-subtractor machine 256
solution, arithmetic of 91
solution, Belgian 198
solution, bibliography on Hagelin 247
solution, Bombe methods of 267
solution, British 63
solution by cryptanalytic means 295
solution by homologs 44
solution, cipher 149
solution, dud 266
solution, emergency 7
solution, Enigma 13, 269
solution, German diplomatic 82
solution, hand 268
solution, independant 111, 196
solution, Italian 107
solution, Japanese 29
solution, method of 238, 242, 243, 249, 250
solution, obstacles to 284
solution of Analin Fabrik Commercial Enigma traffic, methods of 234
solution of "B" Machine 31, 44, 47, (See Solution of the "Purple" Machine)
solution of BUC 193
solution of ciphers 5, 132, 277
solution of CNL encipherments 185
solution of codes enciphered by additives 116
solution of CZB 194, 195
solution of daily keys 250
solution of dud messages 267
solution of enciphered messages, methods of 275
solution of encipherments 7, 231
solution of FIE 256
solution of Finnish 0000 and 17 systems, Report on 256
solution of Finnish systems 252
solution of Finnish transposition system 256
solution of FIR-2 256
solution of FMS 133
solution of French messages 211
solution of GEB 96
solution of GEC 83, 93
solution of GEE 93, 95
solution of GEQ 234
solution of GEQ indicator system, report on 240
solutions of German Abwehr Enigma 238
solution of German Kryha traffic 235

Doc ID: 6554247

solution of German military traffic 17
solution of German system 214
solution of German teletypewriter cipher, solution of 277
solution of Hagelin C-38 247
solution of Hagelin message by statistical methods 250, 256
solution of Hagelin cryptogram, first 251
solution of indicator system 218, 245, 303
solution of Irish traffic 199
solution of Italian cryptographic systems 98
solution of J-19 53
solution of JAA 277
solution of JBD 56
solution of JBH 243
solution of JN-37 217
solution of keys 46, 302
solution of keyword system 83
solution of letters 227
solution of messages 266
solution of meteorological systems 204
solution of meteorological traffic 206
solution of Nanking Government codes 189
solution of open code, first 223
solution of PIC 195
solution of problems 210
solution of "Purple" Machine 13, 31, 45, 46, 48, 50, 52, 57, 58
(See also Solution of the "B" Machine)
solution of reports 205
solution of rotors 282
solution of SLA 193
solution of special jobs from GCCS 237
solution of Swedish Hagelin traffic, Report on 256
solution of Swedish messages 248
solution of system indicators 229
solution of TUE 178
solution of two-period cillies 267
solution of weather reports 206
solution of weather traffic 207
solution of wheel settings 30
solution, problem of 214
solution, problems of 284
solution, process of 284
solution, progress of 287
solution, rapid methods of 268, 284
solution, statistical 255, 283
solution, time and effort needed for 296
Solution Unit 58
solution work 29, 241
solutions 28, 45, 263, 281, 283, 285, 302
solutions, American 100
solutions, record number of 266
solved 86
solved messages 71, 73
solved systems 6, 293
Somerville, Massachusetts, letter of citizen of 227
Soong, Dr. T. V. 183
sorting 140, 198, 210, 232
sorting of traffic 6, 183, 193, 233, 265
source, British 94
source material 82
source of German machines 95
source of information 57, 58, 62, 76

Doc ID: 6554247

source of intelligence 300, 302, 303
sources, foreign intercept 217
sources, German 301
sources, intercept 302
sources of climatological data 216
sources of information 164, 230
sources of intelligence 285
sources of material 24
sources, traffic 290
South Africa 96, 232
South America 83, 227, 232, 300, 302
South American 303
South American (B-7) 4
South American cities 158
South American code books 303
South American diplomatic systems 17
South American group 157
South American Section 112, 148--152, 154, 155, 164
South American Section, dissolution of 149, 221
SPA 148, 150, 151, 157
SPA tape system 302
Spain 2, 41, 159, 232
Spain, Sergeant Harold 120, 121
Spaniards, the 215
Spanish 8, 222, 233, 294, 302
Spanish Additive Unit 151, 152, 156--158
Spanish-American 154
Spanish-American cipher systems 153, 156
Spanish-American codes 153, 156
Spanish-American countries 2
Spanish-American governments 152--155
Spanish-American problems 147
Spanish-American Section, division of 151
Spanish-American systems 147, 159
Spanish-American traffic 148
Spanish and Portuguese languages 4
Spanish code 150
Spanish Code Recovery Unit 151--153, 155-157, 159
Spanish codes 17
Spanish colonial system 159
Spanish consular offices 158
Spanish diplomatic and consular code 298
Spanish diplomatic net 157, 158
Spanish diplomatic systems 17
Spanish embassies 157
Spanish emissaries 302
Spanish Government 8
Spanish government codes 299
Spanish government system 148
Spanish government traffic 149, 152
Spanish, graduate work in 149
Spanish group 293, 294
Spanish language 6, 115, 128, 147, 220
Spanish language code systems 159
Spanish language units 159
Spanish messages 214, 225
Spanish official in Panama 298
Spanish ports 150
Spanish problems 163
Spanish Section 132, 159

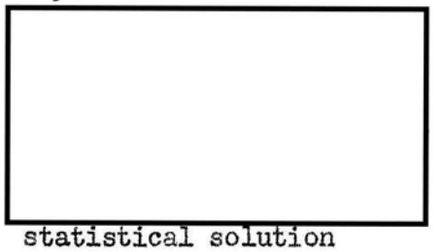
Doc ID: 6554247

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

Spanish-speaking countries 230
Spanish systems 7, 112, 116, 147
Spanish, systems using 293
Spanish texts, translation of 230
Spanish traffic 129, [redacted]
Spanish translation 6
Spanish weather conditions 214
SPB 158, 159, 294
SPC 159
SPD 159
SPE 158
special assignment 280
special camera with lucite rods 279
special circular system 76
special course 61
Special Examination Unit 220, 223, 226--228
Special Examination Unit, contributions of 227
Special Examination Unit, first head of 221
"Special Historical Report on the Solution of the 'B' Machine" 24
Special Machinery for Security Applications 272
special problems 82, 251, 280
special projects 273, 291
special section 3
special signs 161
specialists 73, 281
specialists, French 114, 139
specialists, Italian language 102
specialists, language 220
specialists, research 280
specialization 293
specialized research 281
specialized training courses 285
speed message handling 87
speed, need for 290
speeded recovery 87
speeding of testing process 224
speeding production 73
speeding the work 86
spell group, begin 143
spelling encipherments 185
spelling groups 142, 143
spelling tables 27
spies, German 87
"spot decoding" 137
Sprengle, Lieutenant William 273
SPSIB-3, file on the 003 in 257
square 72, 74
square 10 x 26 77
square, basic, recovery of 285
square, cipher 65--69, 71, 72, 76
square, conversion 71, 72, 74, 77, 83
Square, Conversion, No. 28 278
square, key book 74
square, new type of 72
square No. 8 68
square, random cipher 278
square, reconstruction 278
square recovery 73
square, structure of 72
square Vigenere 67
squares, cipher 75
squares, conversion 66, 71, 75, 78, 243
squares, enciphering 275

Doc ID: 6554247

squares, list of
67, 68
squares, types of
67, 68
SSA (See Signal Security
Agency)
staff 206, 276
staff, cryptanalytic
185
staff, GCCS 18
staff studies 286
staff supervision 1
staffs, British 19
Staley, Dr. Ruth
140, 145
Stallknecht, Mrs. Anne Henry
200
standard nomenclature 287
standard sequence 66, 67
starting point 33
starting points, shifting
86
starting points, testing of
277
State Department 38
State Department files 38
State Department records 37
station 84, 124, 141, 148,
151, 162, 205, 209
station, Dakar 211
station, German in Rome
213
station, Iceland 259
station, illicit 70
station, Newfoundland
259
station, Vint Hill Farms
259
stations
87, 99, 217, 229, 237
stations, British intercept
70
stations, Canadian 217
stations, coastal 212
stations, European 107
stations, intercept 3, 6
stations, monitor 49
stations, observation 212
stations, remote and isolated
217
stations, U. S. Army
217
stations, U. S. Naval
217
statistical analysis
251
statistical approach to
Hagelin machine 255
statistical approaches
283
statistical calculation
38



EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

statistical solution
255, 283
statistical solution of
Hagelin messages 250
Statistical Solution of
Messages Enciphered by
the Tunny Machine 234
statistical studies 241
statistical tests 34
status of the systems 125
Stenographic (B-5) 3, 4
stenographic documents
220, 221
stenographic documents,
German 222
stenographic material 222
stenographic systems 222
stenography, expert 221
Stephens, Miss Elizabeth
54
Stephenson, Lieutenant O. W.
101
stepping 32, 94
stepping apparatus 259
stepping of rotors 282
steps 32
stereotyped message
beginnings 77
stereotypes 71
stereotypic report 74
Stevens, Miss Elizabeth
24

Doc ID: 6554247

Stevens, Captain Geoffrey G. 16; (Major) 20, 21, 59, 259
Stibitz, Mr. 257
Stifler, Miss Martha (Mrs. Waller) 189
Stockholm 247
stops 265, 267
stops, Bombe 264
stored traffic 89
Stowbridge, Lieutenant Richard W. 207
Strachey, Mr. Oliver 18
Strategic Services, Office of 174
strip additive 122
strip of additive 157
strip system, daily 121
strength 9, 114, 176
strength of commercial unit 230, 231
strength of subsection dealing with Middle European systems 191
strength of Weather Unit 208
student, graduate 171
students 164, 235, 236
students, classes of 61
studies 247, 283
studies, climatological 219
studies, continuation of 101
studies, cryptanalytic 38
studies, frequency 232
studies, Hagelin 247
studies, IBM 201
studies, RAM 201
studies, staff 286
studies, statistical 241
studies, technical 248
Studies, TICOM 94
study 39--42, 44, 46, 50, 55, 56, 62, 69, 70, 72, 74, 77, 79, 88-90, 98, 100, 101, 107, 123, 129, 147, 154, 177, 194, 197, 238, 246, 247, 257, 262, 267, 273, 278, 280--282, 285, 290, 296, 301, 303
study, cryptanalytic 178
study in Finnish language, first 251
study, language 251
study of Brazilian systems 151
study of codes 152
study of Finnish plain text 249
study of Green Machine 284
study of indicators 218
study of messages 71, 215
study of systems 125
study of traffic 158, 291
Sturgis, Mr. Cyrus C. Jr. 48
subject matter 76, 138, 223
subjects 156
subsection of GCCS, operational 269
substitution 123, 146, 243
substitution, autokey 57
substitution cipher, polyalphabetic 108, 146
substitution ciphers, digraphic 178
substitution, digraphic 65, 83, 135, 178, 188
substitution encipherment 114, 118, 144, 188, 195, 214
substitution, monoalphabetic 194, 202
substitution pattern 166
substitution, polyalphabetic 278
substitution, running-key 188
substitution, simple 158
substitution systems 154
substitution system, aperiodic 57
substitution system, polyalphabetic 195
substitution system, Port au Prince digraphic (GEB) 83, 86, 96
substitution tables 85, 155, 165
substitution tables, digraphic 184, 192, 195

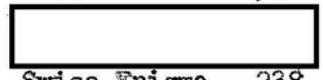
Doc ID: 6554247

substitution tables, recovery of 102
substitution with disguised running key 253
substitutions, solution of digraphic 101
subtracted indicators, index of 252
subtraction, indicator 252
subtractor 67
success 1, 2, 7, 9, 18, 42, 47, 48, 50, 52, 73, 186, 198, 218, 228, 233, 239, 244--246, 261, 262, 265, 269, 273, 275—277, 284, 285, 295, 296, 301
success, cryptanalytic 8, 300
success (GEC) 93
success of training program 173
suggestions 183
Sukunakarazu 35
summaries of cryptanalytic work 286
Summary Annual Report of the Army Security Agency 287
summary of achievements of the Italian Section 111
summary of news 286
Summey, Miss Virginia 221
superenciphered text 252
superencipherment 46, 53, 252
superimpose 70
superimposed 86
superimposed encipherments 184
superimposition 39, 85, 211
supervision 48, 121, 186, 290
supervision joint 185
supervision of experts 273
supervision, staff 1
supervisor 113, 119, 124, 129, 132, 159, 184, 293, 294
supervisor, Negro 231
supervisors 191
Supply Branch 175
supposition 89
suppression of duplicate encipherments 39
Surgeon General 12
surrender of Bulgaria 193
surrender of Germany 220
survey, engineering 258
survey, general 168
surveys 286
suspect correspondents 225
suspected documents, testing of 224
suspension of Axis communications 225
suspician 224, 297
suspicious document 223
Svensson, Major E. H. F. 4
SWA 273
Swears, Lieutenant Clinton C. 206; (Major) 204
Swedish 247
Swedish cipher tables 249
Swedish diplomatic Hagelin messages 273
Swedish diplomatic systems 17
Swedish engineer 247
Swedish government 247
Swedish Hagelin B-211 245
Swedish Hagelin traffic, Report on solution of 256
Swedish message 250
Swedish messages 248
Swedish plain text 247, 248
Swedish tables compromised 249

Doc ID: 6554247

Swedish traffic, keys to 250
Swift, Mr. Gustavus F. 24, 80, 114, 118
Swift, Miss Katharine L. 112, 128, 131, 292, 293
swing shift 114
Swiss 146
Swiss ciphers 140
Swiss code 145
Swiss code recovery 140
Swiss codes 131

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605



Swiss Enigma 238
Swiss Enigma, messages enciphered by 237
Swiss government 131, 139
Swiss machine cipher (SZD) 236
Swiss problems 119, 140
Swiss Section 140, 144, 146
Swiss Section, reports of 139
Swiss systems 125, 132, 133, 139, 140, 143, 146, 184
Swiss systems, cryptanalysis of 118
Swiss, the 141
Swiss traffic 131
Swiss Unit 124, 139, 140, 143
Swiss Unit, separation from French Code Recovery Unit 124
Swiss Unit, strength of 140
switch group 62
switches 46, 259
switching system 257
Switzerland 142, 145
SYA 178
SYB 178
syllabary 26, 62, 178
syllabary codes 24
syllabary, two-letter 25
syllables 34
syllables, kana 64
symbol, line 142
symbols, kana 57, 64
symbols, page 142
symmetric sequences 43
symmetrical standard alphabets 65
symmetry, direct 66
Synopsis of Cryptanalytic Machines 234
synoptic 204, 214, 218
synoptic, basic 212
synoptic, basic IMC 214
synoptic forms employed by the Japanese 216
synoptic, normal 204
synoptics 217
Syria 138, 177, 179
Syria, native of 171
Syrian cipher systems 178
Syrian descent 171
Syria's declaration of war 178
system 16, 30, 31, 38, 41, 46, 47, 50, 53, 55, 56, 66, 75, 77, 79, 84, 86, 88, 90, 93, 95, 96, 99, 106, 134, 135, 143, 147, 157, 165, 166, 169, 185, 192, 202, 203, 217, 219, 237, 240--242, 262, 291, 300, 301
system, "88.." 63
system, additive 135
system, Afghan 174
system, altered 64
system, aperiodic substitution 57
system, auxiliary 53
system, Brazilian 149, 160
system, capture of 226
system, changes in 28, 68, 69
system, Chinese 184, 186
system, cipher 146, 150, 155, 162, 168, 184, 196

Doc ID: 6554247

system, code 190
system, companion 195
system, compromised 113, 118, 120
system, cross-reference filing 232
system, cryptographic 5, 50, 84, 296
system, cryptography of 69
system, current 28, 133
system, daily strip 121
system, diplomatic 50, 158, 178, 187, 203
system, discriminant allocation 265
system, "Eel" 122
system, Egyptian 174
system, elements of 66
system, enciphered 219
system, enciphered code 158, 184, 203, 296
system, Ethiopian 179
system, FCD 135
system, "FELIX" 96
system, FIB 255
system, "Fido" 123
system FIE 253
system, Finnish transposition, solution of 256
system, "Floradora" 83
system "Fraco" 123
system, Free French 121, 133
system, Funchal digraphic substitution 106
system, GEE 88, 93, 244
system, GEG 96
system, GEQ 273
system, German Foreign Office cryptographic 88
system, German one-time pad 285
system, GEW 245
system, Hagelin NEA 254
system, high-security 13
System Identification Book 289, 291
system indecipherable 52
system, indexing 292
system, indicator 45, 135, 218, 229, 240, 242, 245
system, indicator, change of 282
system, indicator, solution of 303
system, Italian 98, 105, 212, 215, 294
system, Japanese 1
system, Japanese attaché 64
system, Japanese commercial 233, 243
system, JBC 56
system, "Jelly-fish" 122
system, JRN-4 63
system, Keyword 83, 95
system, "Lib-1" 123
system, "Lib-2" 123
system, "Lib-3" 123
system, "Lib-7" 122
system, machine-cipher, Japanese Army 240
system, military attaché 77, 159, 187, 188
system, minor 188
system, naval attaché 188
system, naval 121, 123, 216
system of dominant letters 168
system of handling and checking 292
system, one-time 302
system, one-time pad 78, 83, 88, 93
system, one-time, true 88
system, pad 88
system, pentagraphic 168

Doc ID: 6554247

system, polyalphabetic substitution 195
system, Port au Prince digraphic substitution 83, 86
system, Portuguese 149, 166
system, principal 16
system, "Purple" Machine cipher 54, 58
system, relay switching 257
system, RIK-International 63
system, running-key 253
system, Saudi-Arabian 178
system, secure 52, 31
system, simple 227
system, solution of German 214
system, solution of keyword 83
system, SPA tape 302
system, Spanish colonial 159
system, Spanish government 148
system, special 188
system, special circular 76
system, switching 257
system Thai 180
system, Tokyo 201
system, transportation, solution of 253
system, transposition 55, 133, 135, 283
system, TUB 174
system, Tunny 238
system, Turkish cipher 177
system, two-digit commercial 177
system, unreadable 146, 203
system Vichy additive 134
system, Vichy-Hanoi 120
system, Yugoslavian (YOB) 194
systems 2, 4, 52, 58--61, 100--102, 110, 114, 121, 122, 126--128, 141, 142, 145, 146, 154, 170, 173, 177, 182, 193, 194, 203, 205, 218, 226, 233, 244, 252, 253, 278, 289, 291, 292, 301, 303
systems, additive 57, 121
systems, air attaché 186
systems, American 78, 94
systems, analysis of 28, 246
systems, analysis of our own 282
systems, Arabic 170
systems, attaché 24, 25
systems, attacks on 282
systems, Balkan 181, 192, 193
systems Brazilian 8, 151, 160--163, 167--169
systems, British 15
systems, Bulgarian 191
systems, captured 137
systems, Chinese 181, 189, 191, 194
systems, Chinese digit 187
systems, Chinese diplomatic 17
systems, Chinese Foreign Office 188
systems, Chinese, solution of encipherment of 180
systems, Chungking 186, 187
systems, cipher 152, 154
systems, clandestine 83
systems, code 152, 154, 193
systems, colonial 166, 167
systems, colonial additive 120
systems, commercial 57, 59
systems, compromised 125, 293
systems, Croatian 191

Doc ID: 6554247

systems, cryptanalytic relations between 286
systems, cryptographic 51, 139, 153, 193, 286
systems, cryptographic, foreign 291, 295
systems, Czech 191, 194, 195
systems, description of 24, 78, 289
systems, diplomatic 19, 20, 23, 55, 62, 166, 219, 233, 290, 297, 299
systems, earlier 28
systems, Egyptian 175
systems, enciphered 105
systems, enciphered code 118, 183, 189
systems, English 170
systems, Enigma 284
systems, exploitation of 28
systems, Far Eastern 180
systems, FIA, Buenos Aires version of 254
systems, financial 187
systems, Finnish 249, 252, 256
systems, Finnish machine cipher 300
systems, foreign 11
systems, foreign cryptographic 1
systems, Free French 122, 123, 137, 138
systems French 19, 22, 113, 114, 128, 132, 147, 170, 294
systems, French colonial additive 119
systems, French diplomatic 17
systems, French Mission 122
systems, German 7, 12, 245
systems, German cipher-machine 282
systems, German diplomatic 17, 21, 82
systems, German military 17, 19
systems, government 152, 23[illegible]
systems, Greek 191, 192
systems, Hagelin 256
systems, Haitian 198
systems, history of the cryptanalysis of 286
systems, Hungarian 181, 197, 200
systems, Iberian 157
systems, increasing complexity of 26
systems, indicator 56, 91
systems, Iranian 301, 302
systems, Iraqi 174, 175, 179
systems, Irish 197, 199
systems, Italian 12, 98, 100, 103, 106, 111
systems, Italian diplomatic 17, 105
systems, Japanese 12, 19, 24, 26, 107, 116, 127, 215, 293
systems, Japanese Army 1, 10, 11, 74, 295
systems, Japanese cipher-machine 282
systems, Japanese digraphic substitution 26
systems, Japanese diplomatic 15, 17, 21, 22, 24—26, 28, 30, 54, 57, 61, 284
systems, Japanese meteorological 273, 274
systems, Japanese military attache 24, 62
systems, JMA 63, 64, 77
systems, Liberian 203
systems, list of French code 124
systems, major 177
systems, meteorological, solution of 204
systems, methods of cryptanalysis of 286

Doc ID: 6554247

systems, Mexican cipher 148
systems, Middle East 172, 177
systems, Middle Eastern diplomatic 17
systems, Middle European 181, 190
systems, military 19, 297
systems, military attaché 63
systems, miscellaneous 95, 197
systems, naval 19
systems, naval attaché 24, 244
systems, Near East 172, 177
systems, Near Eastern diplomatic 17
systems, new 26
systems, non-Hagelin 253
systems of Afghanistan 175
systems of Belgium 197
systems of communications 11
systems of Eire 197
systems of encipherment 111
systems of Haiti 197
systems of Luxembourg 197, 199
systems of recording 228
systems of Rumania 197
systems, old material used in new 302
systems, Persian 170, 175
systems, Philippine 191
systems, Polish 191, 194, 195
systems, Polish diplomatic 195
systems, polygraphic substitution 27
systems, Portuguese 8, 112, 159--162, 164, 166, 168, 169, 294
systems, Portuguese-Brazilian 163
systems, Portuguese cipher 167
systems, Portuguese Hagelin 254
systems, protection of our 254
systems, readable 59, 86
systems, reconstructed 293
systems, research on 117
systems, Rumanian 181, 201
systems, Russian 12
systems, Saudi Arabian 175
systems, secret 12
systems, secure 295, 296
systems, security of 281
systems, security of our own, increase in 285
systems, separate 170
systems, Slovakian 191
systems, solution of 1, 8, 112, 161
systems, solved 6, 153, 293
systems, South American diplomatic 17
systems, Spanish 7, 112, 116, 147
systems, Spanish-American 147, 159
systems, Spanish-American cipher 153, 156
systems, Spanish diplomatic 17
systems, status of 125
systems, stenographic 222
systems studied 173
systems studied in B-III 280
systems, study of 125
systems, substitution 154
systems, Swedish diplomatic 17
systems, Swiss 118, 125, 132, 133, 139, 140, 143, 146, 184
systems, Syrian cipher 178
systems, teletypewriter 284
systems Thai 189, 191
systems, transposition 28
systems Turkish 170, 172, 174, 175, 177, 302
systems, unknown 121, 123, 185, 278, 302

Doc ID: 6554247

systems, used in rotation 25
systems using French 293
systems using Spanish 293
systems, Venezuelan 147
systems, Vichy 122, 137
systems, Vichy French enciphered code 118
systems, weather 7, 23, 293
systems, weather, Japanese 216
systems, Yugoslavian 191
SZA 141, 143, 145, 146
SZB 141, 143, 145, 146
SZC 141, 143, 145, 146
SZD 143, 146, 236, 237, 240
SZD, A Swiss Machine Cipher 234
SZG 144
SZH 144
SZM 118, 144, 184
SZN 118, 144, 184
SZP 146
SZQ 144
SZR 145, 146
SZS 146

table 212
table 13 x 26 69
table 26 x 26 69
table, additive 120
table "B" 27
table, code 68
table, permutation 64, 160, 163, 232
tables 59
tables, additive 158
tables, cipher 193
tables, compromised 252
tables, deciphering 192
tables, digraphic substitution 184, 192, 195
tables, distribution 42, 43
tables, frequency 71
tables, indicator 129
tables, key 66
tables of permutations 231
tables of probable weather 215
tables, rotation in use 158
tables, spelling 27
tables, substitution 85, 102, 155, 165
tables, Swedish cipher 249
tables, transposition 165
Tabulating Machinery Unit (A-2) 3, 4; (B-4) 6, 9, 10; (B-8) 4
tabulations 48, 271
tabulator, IBM 53
Tai Li's Code, General 188
TANGENSTAFEL 86
Tangier 75
tank, Japanese medium 92
tape 88
tape, 70-mm, first use of long 276
tape, additive, one-time 158
tape equipment, teletype-writer 272
tape punches 272
tape, RAM 242
tape readers 272
tape system, SPA 302
tape, teletypewriters, equipment 278
tapes 158
tapes, compromise of 158
Tascabile, RA 104
Taylor, Sergeant Carisle C. 114; (Lieutenant) 293; (Captain) 293
Taylor, Miss Delia A. (Mrs. Sinkov) 48, 82, 148, 150

Doc ID: 6554247

Taylor, Miss Erma 159
Taylor, Lieutenant James C 128
Taylor, Lieutenant Colonel Telford 20
teamwork 47
technical consultation 23
technical data 14, 78, 92
technical description of GEC 17
technical difficulties 228
technical direction 2
technical director 103
Technical Director, B-III-a 189
technical expert 206
technical information 22, 255
technical information exchange of with GCCS and EU 138
technical knowledge 19
technical language 76
technical liaison 219
technical papers 255, 285, 287
technical problems 117
technical reports 239
technical staffs 280
technical studies 248
technique 53, 135, 136
technique, British 17, 19
technique, IBM 59
technique, rotary bombe 259
techniques 7, 38, 73, 74, 79, 247, 271, 275
techniques, American 15
techniques, charting 183
techniques, cryptanalytic 5, 33, 51, 71, 134, 180
techniques, development of 72, 283
techniques, Finnish 300
techniques, Hagelin, development of 247, 248
techniques, logging 183
techniques, mechanical, electrical, and electronic 15
techniques, military 52
techniques of aligning messages 254
techniques of cryptanalysis, modern 295
techniques, research 73
Teheran, Conference in 77
telegrams 78, 223
telegrams, exchange of 22
telegraphic Chinese 182
telegraphic expense 29
telegraphic texts, Turkish 173
telephone conversations 220, 228
telephony, automatic 46
teleprinter ciphers, German 234, 236, 240
teleprinter machine 238
teletype 213
teletype facilities 210
teletype machines 210
teletypewriter cipher, German, solution of 277
teletypewriter cipher messages, German 276
teletypewriter, cipher, SIGCUM 280
teletypewriter systems 284
teletypewriter tape equipment 272, 278
Templeman, Miss Gloria 173
temporary duty 19
Tenneis, Miss Mary Margaret 200
Tenney, Mr. Raymond P. 180--182, 185
Terminology, Committee on 287, 288
terms 288
terms, coinage of in GCCS 83

Doc ID: 6554247

terms, cryptographic 288
terms, definitions of 287
terms, modern Arabic 174
terrain, observations of 222
territories, conquered 57
test 269
test jobs 262
test messages 234
test of 5202 276
test of message 232, 245
Tester, Tetragraph 271
testing, hand 277
testing hypothesis 89
testing, IBM 178
testing of menus, simultaneous 265
testing of starting points 277
testing of suspected document 224
testing process, method of speeding 224
tests 226, 265, 271, 273
tests, analytical 34
texts, cipher 267
tests, coincidence 274
tests, linguistics 191
tests, statistical 34
tetragraph 168
Tetragraph Tester 271, 272, 274
Tetragraph Tester camera 275, 276, 279
Tetragraph Tester projector and camera 274
Tetragraph Tester projectors 279
tetragraphic chart 64
tetragraphic code chart 70
tetragraphic code groups 283
tetragraphic groups 168
tetranomic code 133, 144
Tetratester 271
text 33, 35-37, 42, 135, 271, 283
text additive book, basic 84
text additive key books 84
text, cipher 29, 53, 56, 57, 76, 239, 246, 249, 252, 253, 275, 276, 278
text, code 65
text cryptographic 43
text, elements of 73, 277
text, enciphered code 65
text, enciphered key 252
text encipherment 83
text, English 36, 47
text, French plain 126
text, Japanese 37
text, Japanese plain 49
text, JN-36 218
text, key 73
text of intercepts 205
text of messages 213
text, paucity of 41
text, plain 57, 73, 75, 85, 107, 116, 127, 136, 141, 150, 156, 202, 203, 225--227, 232, 233, 248, 251, 253, 275, 278, 300
text, plain-code 84
text, plain, reencipherment of 252
text, plain, Swedish 248
text, plain, transposed 246
text, reading of 224
text, recovered 100
text, resultant 73
text, resulting 177
text, secret 227
text, superenciphered 252
text, transcribing of 231
text, transposed Hagelin-enciphered 252

Doc ID: 6554247

text using the same key 275
textbooks 211
textbooks, shorthand 222
texts, cipher 200
texts, code 73
texts, German 230
texts of intercepts 206
texts, plain, compromised 246
texts, Spanish 230
texts, Turkish telegraphic 173
textual data, comparison of 277
textual group 66
THA 180
Thai code 189
Thai, encipherments of 190
Thai government 196
Thai language, Dictionary of 189
Thai language, expert in 189
Thai messages 189, 190
Thai officials 189
Thai problem 189
Thai Systems 189, 191
Thai, the 189
Thailand 189
Thailand puppet government 180
Thailand, system used by 180
THC 190
the "003" (K68003) 236, 237, 242--244, 246, 257, 262, 265, 268, 269 (See Bombe and volume IX.)
the 003, attachments 265
the 003 capacity 265, 266
the 003 equipment 269
the 003 equipment, cost of 265
the 003 frames, rewire of 267
the 003, installation of 262
the 003, maintenance of 264
the 003 sections concerned with 267
the 5202 239, 271, 276, 284
Theater, China-Burma-India 207, 219
Theater, India-Burma 208
Theater, Mediterranean 208
Theater, North African 208, 213
theaters 207
theft of cryptographic documents 298
Theory and Analysis of a Letter-Subtractor Machine 247
theory and application of cryptanalytic methods 286
theory of additive recovery 283
theory of RAM 273
Thielmann, Mrs. Marjorie 149, 150, 152
Thompson, Lieutenant James R. 206
Thornett, Captain E. B. C. 21, 57, 59
three-letter code groups 25
three-wheel Enigma machine 258
TICOM Studies 94
Tilby, Captain P. W. 21
Tiltman, Colonel 69, 78; (Brigadier) 249, 259
time 209, 269, 278, 303
time and place of message 211
time, cryptanalytic-machine 23
time, expenditure of 295
time in weather reports 205
time lags 72
time, record 277
time required for solution 296

Doc ID: 6554247

time, saving of 302
timesaver 73, 92
title, short 64, 146
titles 80
titles, short 59, 60, 289, 291
T/O's 5
Tokyo 37, 64, 70, 72, 74 75, 91, 200, 216, 219
Tokyo-Berlin circuit 92
Tokyo-Berlin German letter traffic 244, 245
Tokyo, Foreign Office in 31
Tokyo-Kabul circuit 60
Tokyo-Kuibishev circuit 60
Tokyo system 201
Tokyo-Vatican City circuit 60
Tokyo, War Office in 76
tool, cryptanalytic 277
tools, 301
top priority 47
topical index 74
tour of duty 132
TOYOHATA station, coverage of 217
trade-control bodies 57
traffic 1, 2, 5--7, 31, 35, 48 56--58, 64, 67, 69, 70-- 72, 76--78, 84, 85, 87 91, 96, 98, 99, 106, 109-- 111, 113, 118, 122, 133, 134, 137, 138, 141, 143-- 146, 153, 156, 158, 161 166--168, 179, 180, 188 190, 191, 194, 203, 209-- 211, 214, 225, 230, 232 233, 235, 237-239, 243, 245, 249, 254, 259, 260, 280, 286, 289, 293, 300-- 302
traffic, ability to read 294
traffic, accumulated 140
traffic, accumulation of 169
traffic, amount of received 177
traffic, Analin Fabrik Commercial Enigma, Methods of solution 234
Traffic Analysis 10, 261, 262
Traffic Analysis and Control Branch 10, 11
traffic analysts 262
Traffic and Indexing Unit 54
Traffic and Systems Coordinator 289
traffic, Argentine code 149
traffic, assignment of 117
traffic, attack on 13, 19
Traffic (B-6) 3, 4
traffic, back 59, 241
traffic, backlog of 49, 101
traffic, Belgian 132, 197--199
traffic, Berlin-Lisbon 241
traffic, body of 144
traffic, Brazilian 160
traffic, Brazilian code 148, 149
traffic, Buenos Aires 127
traffic, Bulgarian 192
traffic, BZF 169
traffic, cessation of 266
traffic, Chilean code 149
traffic, Chinese 182
traffic, clandestine 225, 226
traffic, code 152, 153
traffic, Colombian 147
traffic, Colombian cipher 149

traffic, colonial 166
traffic, commerical 57, 198, 230, 231
traffic, Commercial Code 233
traffic, commercial, processing of 229
Traffic Coordination Section 233
Traffic Control 10
traffic, Costa Rican 148
traffic, cryptanalysis of weather 207
traffic, current 63, 87, 102, 104, 144, 169, 186, 187, 210, 241, 244, 262, 264, 265
traffic, Dakar 211
traffic, decoded 159
traffic, decoding of 115
traffic, decrease in volume 193
traffic, diplomatic 2, 197, 205, 206
traffic, distribution of 290
traffic, Dominican cipher 149
traffic, editing of 174
traffic, exchange of with GCCS and EU 138
traffic, exploitation of 233
traffic, FBM 120
traffic, FFE 135
traffic, file of 202
traffic, filing of 193
traffic, Finnish 249, 250, 255, 300
traffic, Free French 121
traffic, French 4, 112, 115, 128, 130, 137, 199, 211
traffic, French government 130
traffic from Berlin 246
traffic, GEC 93, 96
traffic, GEQ 241
traffic, German 210, 211, 215
traffic, German Air Force 257, 259
traffic, German Army 257, 259
traffic, German Army and Air Force, interception of 235
traffic, German military 17
traffic, German naval 19
traffic, German, study of 213
traffic, GEW 246
traffic, governmental 107
traffic, Greek 190, 192
Traffic group 71
traffic, "H" period 74
traffic Hagelin 248
traffic, Haitian 132, 198, 199
traffic handling 47, 209, 290
traffic, handling of weather 210
traffic Helsinki 78
traffic, highest-security 88
traffic, homogeneity of 115, 116
traffic, Honduras 153
traffic, Hungarian 200
traffic, Impero (ITA) 107
traffic in CNG 185
traffic in commercial codes 229
traffic in depth 120
traffic in low-echelon systems 219

Doc ID: 6554247

traffic in SZR 146
traffic, index of 160
traffic, index of Brazilian five digit 161
traffic, indexing of 290
traffic, insolvable 194
traffic, insufficient 296
traffic, intercepted 37, 49, 58, 87, 89, 148, 167, 203, 226, 290
traffic, Iranian 173
traffic, Iraqi 173
traffic, Irish 199, 200
traffic, Italian 107, 212, 215
traffic, Italain diplomatic 98
traffic, JAM 59
traffic, Japanese 1, 25, 45, 129, 218
traffic, Japanese Army 276
traffic, Japanese commercial 186
traffic, Japanese diplomatic 28, 48
traffic, JAS 74, 76
traffic, JAT 77
traffic, JN--37, coverage of 217
traffic, Keyword 85
traffic, lack of 56, 120, 169, 194, 240, 261, 262, 301
traffic, Lebanese cryptographed 178
traffic, letter, German Shanghai 244
traffic, letter, German Tokyo-Berlin 244, 245
traffic, letter (GEW) 245
traffic, logging of 193
traffic, Luxembourg 198, 199
traffic, machine-enciphered 46
traffic, machine index of 161
traffic, Mexican 148
traffic, Mexican cipher 149
traffic, Mexican code 149
traffic, Mexico City 166
traffic, military 187
traffic, Ming 182
traffic, miscellaneous 22
traffic of the Nanking Government 185
traffic, new 100, 291
traffic new, processing of 213
traffic overlapping of 134
traffic personnel 194
traffic, plain-text 116, 232, 233
traffic, Polish 194
traffic, Portuguese 160, 164, 168
traffic, Portuguese code 149
traffic, Portuguese language 162
traffic problems 192
traffic, processed 167
traffic, processing of 47, 176, 290
traffic, QAA 232
traffic, raw 1, 49, 78, 300, 302
traffic, raw American 78
traffic, requests for 290
traffic, responsibility for 22
traffic, Romance language 160
traffic routing 3, 6
traffic, Rumanian 201--203
traffic, Russian, study of for training purposes 211

Doc ID: 6554247

traffic, Santiago 127
traffic, secret 175
Traffic Section 131, 199
traffic shortage 59
traffic, solution of 105
traffic, solution of enemy meteorological 206
traffic, solution of weather 207
traffic, sorting of 6, 183, 193, 265
traffic sources 290
traffic, Spanish 129, 157
traffic, Spanish-American 148
traffic, Spanish government 149, 152
traffic, stored 89
traffic, study of 158
traffic, Swedish, keys to 250
traffic, Swiss 131
traffic, SZD 240
traffic, translating 164
traffic, Turkish 173
traffic, types of 148
traffic, unenciphered 209
Traffic Unit 80, 131, 132, 194
Traffic Unit (B-6) 5
traffic, unreadable 168, 198
traffic, Venezuelan cipher 149
traffic, Vichy French 207
traffic, volume of 49, 83, 172, 213, 217, 226, 265, 296
traffic, Washington 127
traffic, weather 208, 212, 293
trained personnel 179
trained personnel, lack of 171
training 2, 8, 60, 79, 118, 164, 172, 208, 239, 241, 260, 261, 263, 268
training, academic 163
training, ASTP 172, 182
training, course of 211
training courses, specialized 285
training, cryptanalytic 61
Training, Director of 131
training for an emergency 1
training function of SIS 28
training ground for machine cryptanalysis 251
training in cryptanalysis 101
training, linguistic 163
training of linguistic personnel 195
training of new personnel 237
training program 1, 60, 173, 191, 208
training, purposes of 182
Training Section 60
training, study of Russian traffic for 211
transactions 229
transcribing of radiotelephone conversations 220
transcribing of stenographic documents 220
transcribing of text 231
transcription 173, 174, 228
transfer 154, 162
transfer of personnel 157, 164
translate 182
translated 35, 120
translated messages 3, 49
translating traffic 164
translation 4, 6, 8, 47, 76, 86, 87 106, 114—116, 120, 126, 132, 134, 137, 141, 143, 145, 146, 149, 156, 157, 159, 161, 162, 165, 167, 169, 174, 175, 193, 203, 237, 250

Doc ID: 6554247

Translation and Intelligence Unit 261
translation, first Bulletin 28
translation, French 6
translation, Japanese 6
translation (Nisei) 10
translation of DESAB, first 96
translation of Finnish materials 251
translation of FMB, first 122
translation of GEC, first 96
translation of German texts 230
translation of messages 231
translation of radiotelephone conversations 220
translation of shorthand notes 222, 223
translation of Spanish texts 230
translation of YOA messages 192
translation problems 116
translation purposes 302
translation services 179
translation, Spanish 6
translation stage 156
Translation Unit 82, 125, 151--157
Translation Unit, French 116, 126, 127
translations 1, 25, 28, 44, 60, 91, 100, 102, 111, 127, 144, 161, 177, 187, 189, 198, 202, 249, 293
translations, accuracy of 110
translations, British 193
translations, French 140
translations, German 140
translations of Balkan messages 193
translations of GEC 301
translations of German Kryha traffic 235
translations, POB 166
translations, production of 192
translator 29, 113, 200, 302
translator personnel 81
translators 35, 71, 73, 81
translators, Japanese 14
translators, scarcity of 49
Translators Unit, Aids-to- 80, 81
transmission 77, [redacted] 177, 205, 226
transmission, costs of 229
transmission, non-Morse 238
transmission of documents 22
transmittal of message 28
transmitters 217
transportation, problem of 210
transportation system, solution of 253
Transposed Cipher Unit 126
Transposed Cipher Unit, French 129,130
transposed code 134
transposed code Chinese 187
Transposed Code Section 135
transposed Hagelin-enciphered text 252
transposed plain text 246
transposition 28, 52, 55, 57, 95, 99, 108, 123, 133, 135, 136, 168, 253, 281
transposition cipher 178, 195

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

Doc ID: 6554247

transposition, columnar 129
transposition, double 179, 194
transposition encipherment 137, 187
transposition encipherment, French 130
transposition encipherments 129, 188
transposition, kana 243
transposition key 275
transposition, keyed columnar 188
transposition matrix 274
transposition of elements 99
transposition pattern 166, 283
transposition problem 52
transposition problem, Japanese 129
transposition problems 155
transposition, route 129
transposition sequences 188
transposition system 55, 133, 135, 283
transposition system, Finnish, Solution of 256
transposition system, Free French 121
transposition systems 28
transposition tables 165
transpositions 33, 154
Travis, Commander Sir Edward 263
treaty, commercial 36
Tribble, Miss Margaret 200
trigraph 41
trigraphic code 64, 143
trigraphic code, enciphered 144, 175
trigraphic coincidences 271
trigraphic designations 291
trigraphic Foreign Office code 188
trigraphic groups 283
trigraphs, sequence of 253
Tripartite Agreement 44
troop concentrations, German 77
troops, morale of 222
TRUJILLO 99
Trujillo, Ciudad 99
TUA 170, 174, 175, 302
TUB 170, 174, 175
TUC 170, 177
TUD 170, 175
TUE 170, 175, 176, 178, 302
TUF 170
TUG 170, 177, 178
TUH 177
TUI 170
TUJ 170, 175
TUK 170
TUL 170 . . . . .
[redacted]
Tunny system 238
Turing, Mr. 259
Turkey 138, 170, 177, 232
Turkish 171, 172, 175, 222, 302
Turkish cipher system 177
Turkish delegation 177
Turkish embassies 178
Turkish, expert in 171
Turkish, instruction in 173
Turkish language 173, 179
Turkish, language studies of 174
Turkish legations 178
Turkish messages 177
Turkish systems 170, 172, 174, 175, 177, 302
Turkish systems, descriptions of 78

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605

Doc ID: 6554247

Turkish telegraphic texts 173
Turkish traffic 78, 173
Turkish two-part code 174
Turks, the 177
turnover, wheel 238, 265
turret operation 263
turret room 264
"twenties", the 32, 34
two-day-period key recovery 87
two-letter code groups 25, 26
two-part code 109, 111, 145, 161, 174
two-part code book 157
two-period cillies 267, 268
Tyndall Field, Florida 207
types of squares 68
typescript 286
typewriter keyboard 73
typewriter unit, keyboard 45
typewriters 144
typing 191, 231
typing of shorthand notes 222
typing of YOA 192
typists 3, 191

U, long 35
U-type codes (JU) 24
"UJ" Code 27
Ullman, Miss Gertrude E. 147, 149, 154, 234, 236, 238, 240, 241, 263
ulterior assistance 296, 298
uncooperative attitude of Japanese delegations 216
undercover method 299
Underwood, Dr. Dale 24, 80
unenciphered 99
unenciphered code 64, 96, 120, 123, 126, 168, 198, 202
unenciphered code book German 82
unenciphered codes 113, 122, 124, 141, 182
unenciphered groups 214
unenciphered indicators 212
unenciphered material 144
unenciphered messages 116
unenciphered traffic 209
unidentified code groups 294
United Nations 109, 229
United Nations Conference on International Organization 188
United States 254, 257, 282
United States, armed forces of 297
United States Army 40
United States Army Converter M-209 247
United States Army stations 217
United States Coast Guard 160, 242, 246
United States Consular Service 181
United States, defense of 50
United States Government 36, 259
United States Naval stations 217
United States, the 14, 19, 35, 76, 157, 176, 227, 260
United States Weather Bureau in Washington 211, 219
units, service 280
universities, American 171, 219

Doc ID: 6554247

University, American, in Cairo 171
University, Harvard 171
University, Yale 171
unknown systems 278, 302
unread messages, exploitation of 91
unreadable system 146, 203
unreadable traffic 198
unsolvable problem 78
U. S. M-138-A cipher device 127
U. S. State Department cryptographic materials 77
useless material 298
users of systems 297
Utley, Lieutenant John H. 149--152

Vaccination Antityphoidiques 136
value, intelligence 63, 83, 93, 290
values 134, 165, 166
values, cipher-text 34
values, code 70
values, plain-text 33, 34
Vandenberg, Mrs. Mary B. F. 123, 140
Vanderhoof, Sergeant Mary B. 122
van Hoesen, Miss Alice 120
variants 65, 69, 142, 194, 195, 202, 275
variations 302
vault 287
V-E Day 232, 285
Venezuela 2, 152, 159
Venezuelan ciphers 150
Venezuelan cipher traffic 149
Venezuelan systems 147
Vergine, Sergeant George 236, 251, 255, 256
Verkuyl, Colonel J. J. 54
version 36, 301
Vichy 120
Vichy additive system 134
Vichy codes 137
Vichy DX code 122
Vichy France 2
Vichy French digit codes 114
Vichy French enciphered code systems 118
Vichy French Government 116, 135, 211
Vichy French traffic 207
Vichy-Hanoi system (FBM) 120, 122
Vichy systems 122, 137
Vigenere 67
Vint Hill Farms Station 10, 209, 220, 259
violation of pledge to the British 13
Virtanen, Dr. Reino 250, 253, 254
visibility 204
visit 58, 78
vocabulary 25, 26, 64, 142, 187
vocabulary, prediction of 100
Vogel, Captain Edward J. 220--223, 225, 227, 228
volume, limited 169
volume, traffic 49, 83, 172, 213, 217, 265, 296
vowel-consonant 141
vowels 29
vulnerability of machines without endplate plugging 282
VZA 159, 294
VZB 150

WAC program 263
Waggoner, Mr. Thomas A. 82, 89

Doc ID: 6554247

Waldeck, Miss Edna 183, 184
Walker, Miss Louise 154
Walker, Miss Marjorie 173
Wall, Dr. Walter 140
Waller, Mrs. (Miss Martha Stifler) 189
Waltz, Mr. Maurice 54
War Department 11
War Department, letters to from civilians 223
War, duration of 280
War, end of the 214
War, factors in winning of 21
War in Europe 2
War indicatives 212
War, Italian Ministry of 108
War Office in Tokyo 76
War, the 2, 3, 11, 13, 15, 23, 48, 52, 57, 64, 67, 76, 87, 92
Warner, Mrs. Elizabeth 182
Warsaw 32
Washington 16, 22, 31, 37, 49, 82, 98, 100, 147, 175, 178, 179, 237, 251, 252, 300
Washington, Chinese Mission in 183
Washington circuit 161, 164, 167
Washington Evening Star 48
Washington Helsinki messages 251
Washington, Naval Observatory in 206
Washington traffic 127
Washington, United States Weather Bureau in 211
Washington, Weather Bureau in 206, 209
Watson, Mrs. Dorothy K. 200, 220, 228
Watz, Mr. Maurice 235
Weather (B-10) 4
Weather Bureau library 215
Weather Bureau, United States 206, 209, 211, 219
Weather Central, Army 209, 210, 213, 215, 219
Weather Centrals, Japanese 216
weather concessions 216
weather conditions 204, 211, 213
weather conditions, Spanish 214
weather information 205
weather missions 205
weather observations 204, 216, 218, 219
weather, observed 215
weather problem 209
weather report forms, Japanese 216
weather reports 4, 205, 206, 214, 216
weather reports, broadcast of 204
weather reports, Japanese 207, 215
weather reports, plain-text 211, 215
weather reports, Russian 211
weather reports, solution of 206
Weather Section 215
weather system, Italian 212
weather systems 7, 23, 293
weather systems, Japanese 216
weather, tables of probable 215
weather traffic 208, 212, 293
weather traffic, cryptanalysis of 207

Doc ID: 6554247

TOP SECRET CREAM

weather traffic, handling of 210
weather traffic, solution of 207
weather types, continuity of 205
Weather Unit 206—208, 210, 212, 213
Weather Unit, location of 209
Weather Unit, strength of 213
Weeks, Mrs. Clara 159
Weidman, Dr. Robert H. 132, 139, 140, 236
weighting 277, 283
Welchman, Mr. W. G. 260, 263
Wenger, Commander J. N. 30
Western form 174
western nations, Japanese and 216
Wheatly, Lieutenant LeRoy 273, 276
Wheatstone 236
wheel 238
wheel, break 32
wheel break pattern 244
wheel, cipher 29
wheel, continuously moving 282
wheel, control 30
wheel, fourth 260
wheel motions 242
wheel order 267
wheel setting 30, 245, 264, 266
wheel-setting keys, adjustment of 264
wheel, the "six" 29
wheel turnover 265
wheel-turnover pattern 238
wheel wiring 244, 246
wheels 30, 244, 248, 267
wheels, adjacent 242
wheels, cipher 30
wheels, cyclic 276
wheels, periphery of 94
wheels, resetting of 91
wheels, setting of 91, 239
white officer-in-charge 231
WI 27
Wilder, Sergeant Oscar, Jr. 48
Williams, Mr. 257
Williamson, Miss Letitia 163
willingness of British to cooperate 12
Willis, Miss Harryett 119
Win (CNC) 182
wires 269
wiring 245
wiring, reflector 267
wiring, wheel 244, 246
withheld passages 49
Wolff, Dr. 300
Wonder, Mr. Charles W. 157
Wood, Miss Kathryn 132
Wood, Miss Nellie F. 183, 184
Woods, Miss Margaret 154
word, frequently-used 25
word, probable 248
words 34, 62
words, artificial 29
words, frequencies of 251
words, Japanese 219
words, probable 249
words, skeletons of 33
work 35, 43—45, 54, 56, 57, 63, 74, 75, 79, 82, 86, 89, 92, 96, 100, 105, 106, 112, 143, 191, 228, 230, 234, 237, 238, 245, 252, 253, 262, 265, 270, 276, 278, 281, 285, 287, 289, 290, 294, 295, 297

TOP SECRET CREAM

Doc ID: 6554247

work, checking of 289
work, clerical 48
work, cryptanalytic 78, 286, 292
work day, shortening of 210
work, difficulty of 222
work done by hand 278
work, early 62, 82, 98
work, exploratory 82, 247
work, graduate 171
work in French 113
work in Spanish, graduate 149
work, joint 23
work, night 44
work on GEW 246
work, operational 262, 273
work, overlap 73, 80
work, pioneer 113
work, recovery 71, 116
work, research 300
work, "second storey" 298
work sheet 4
work sheets 59, 85, 129, 130, 240, 300
work sheets, GEC 17
work sheets, GEW 244
work, solution 29, 241
work, speeding the 86
workers 36
working day, 24-hour 290
world 83, 87
World War I 51, 82, 98, 221, 222, 298
World War II 1, 51, 98
Worth, Miss Josephine 80
Wright, Mrs. Edith 80
Wright, Mrs. Inez 163
Wrigley, Captain Edward J. 206; (Major) 204
writing, code 35
writings, miscellaneous 286

X-27 (FAM) 302
X-38 (FAN) 302
X68003 ("003) 236, 237, 242--244, 246, 257, 259 (See also volume IX)
X68007, engineering survey 258
X68009 258, 259
X68128 265
X68129 265
"X" code 99
XA 27
XB 27
"XYZ Index" 89

"Y" (AR 38) 101
Y-1 105
Yale University 171
Yardley, Mr. Herbert O. 18, 26, 51; (Captain) 298
Yellow Project, the 257, 263, 264, 269
Yellow operations 263
YO 26
YOA 192--194, 301
YOB 194
Yugoslav YOA book 301
Yugoslavia 180, 191, 194
Yugoslavian code 192, 196
Yugoslavian system YOB 191, 194

Zimmerman, Mrs. Katherine 80

Doc ID: 6554247

APPENDICES

Doc ID: 6554247

TOP SECRET CREAM

EVOLUTION OF THE GENERAL CRYPTANALYTIC BRANCH

In 1941 the cryptanalysis of all foreign systems other than those of the Japanese Army was carried on in various parts of the Signal Intelligence Service. There was a J (Japanese) Section, directed by Mr. F. B. Rowlett; a G (German) Section, directed by Dr. Kullback; an I (Italian) Section, directed by Captain Sinkov; an M (Mexican) Section, directed by Mr. Frank Bearce; a school under Sergeant Kretlow; a Machine Section, under Mr. Kropfl; and a Bulletin and Distribution Section under Miss Louise Prather. This organization was not rigid, for the top cryptanalysts freely consulted among themselves and worked together on problems as the need arose. Indeed, as late as August 1942 the table of organization of what was then called B Branch existed only in slips pinned to a bulletin board in Major Boud's office in the Munitions Building. The organization was then much the same as that of 1941, except that Lieutenant Bearce was now in charge of the French Section and a "South-of-the-Border" section had been formed under Lieutenant Glodell. When the Signal Intelligence Service moved early in July 1942 to Arlington Hall, B Branch already existed as such, but included: B-1, an amorphous section those principal job was the translation of the production of the two cryptanalytic units, the publication and distribution of the Bulletin, instruction in Japanese, and information; B-2, which was charged with code recovery and the solution of additive encipherments of code; B-3, whose mission was the solution of ciphers and code encipherments other than additive; and B-4, the IBM unit. The main problems of B-2 were Italian, Spanish, (including Spanish American), Portuguese (including Brazilian), German, and French.

Serious effort had also begun on Japanese Military Attache systems and by June 1942 the problem of meteorological encipherments was undertaken. In B-3 the main problems were the famous J-19 transposed code, Hagelin encipherments, and the Japanese Purple Machine ciphers. The organization of B-3 in January 1943 is presented in Tab 4. Captain John N. Seaman had been attached to Colonel Boud's office in the summer of 1942 and had more recently been in charge of the group working on Hagelin problems; when Captain Frank B. Rowlett went to the Training Branch in 1942, Captain Seaman became OIC of B-3.

On 1 September 1943 the organization of B Branch was completely revised; B-2 was set up to deal exclusively with the Japanese Army systems and B-3 undertook the mission which it has had ever since. The organization at that time is shown in Tab 7.

More recent changes in organization are revealed in the Annual Report, Signal Security Division, Fiscal Year 1943; the Annual Report Signal Security Agency, Fiscal Year 1944; and the Summary Annual Report, Signal Security Agency, Fiscal Year 1945.

TOP SECRET CREAM

Doc ID: 6554247

SECRET

PLAN OF ORGANIZATION

SIGNAL INTELLIGENCE SERVICE

1 March 1942

SECRET

OIC
Lt. Col. Harold Boud

TECHNICAL ASSISTANT
1st Lt. Frank B. Rowlett

B-1
JAPANESE
Major L. H. F. Svensson

B-2
GERMAN
Captain Solomon Kullback

B-3
ITALIAN DIPLOMATIC
Major Abraham Sinkov

B-4
FRENCH
Lieutenant H. . . Pearce

B-5
STENOGRAPHIC
Miss Louise Prather

B-6
TRAFFIC
Major A. L. Schukraft

B-7
SOUTH AMERICAN
Lieutenant L. L. Glodell

B-8
ITALIAN
Lieutenant Robert H. Adams

SECRET

2

354247

WORK SCHEDULE MAY 18- MAY 30 1942

(THIS SUPERCEDES PREVIOUS SCHEDULE ISSUED MAY 13th)

Beginning Monday May 18 and until further notice the following Schedule will be in effect for the Japanese Army Codes Section:

Day Shift:	Night Shift:
Mary Joseph DUNNING	Lt. Elbert MOSES
Lt. Charles FERGUSON	
PFC. James FULD	Pvt. David AVRACH
Lt. Rodger HARRISON	Pfc. Morton BARROW
Lt. John C MERRITT	Miss Jean COCROFT
Mr. Franklin PORTER	Pfc. William FLEISCHMAN
Lt. Chester RAY	Sgt. James GUSTON
Lt. Morris SEIBERT	Pfc. Cameron HOSMER
Mrs. Delia SINKOV	Miss Louise LEWIS
Mr. A.W. SMALL	Pfc. Victor ROSE
Mr. Maurice WALTZ	Sgt. Paul SEBESTYEN
Miss Harryet WILLIS	Pfc. Rubin WEISS
Lt. Victor YOUNG	
Hours: 8:15-5:00	Hours: 4:30-12:30
Lunch: 45 min.	Supper: 30 min.
	Saturday: 1:00 PM- 9:00.

* *

The above shift in plans is made necessary by the rapid expansion of the section. It is hoped to switch shifts at the end of two weeks.

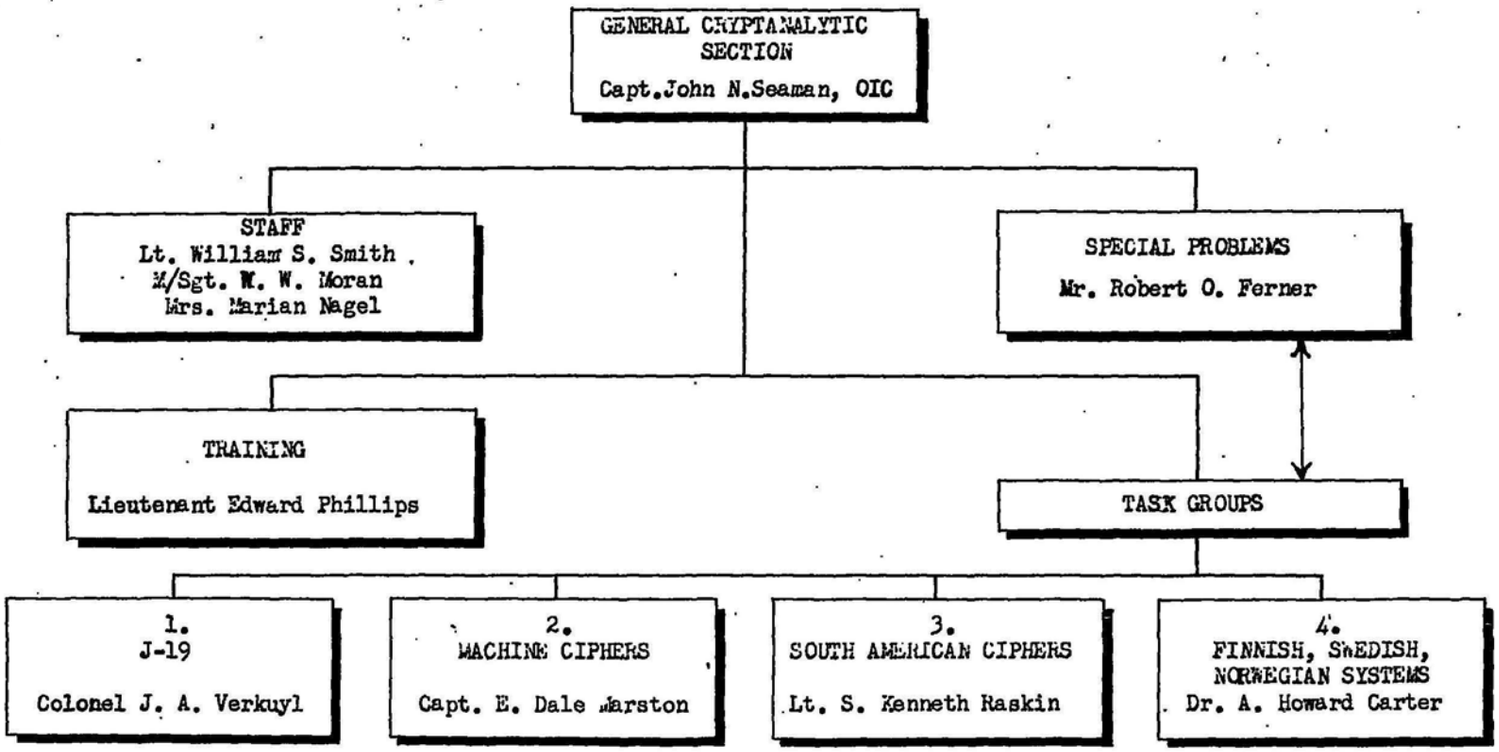
* *

✓ Japanese lectures will start promptly at 4:30 each day, so the night shift is asked to be here promptly.

* *

~~SECRET~~

PLAN OF ORGANIZATION
General Cryptanalytic Section, B-3
January 1943



~~SECRET~~

D: 6554247

~~SECRET~~

IN REPLY REFER TO

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

SPSIS-2

5

February 17, 1943.

MEMORANDUM TO: Mr. Friedman.

In connection with our conversation of the other day, the following is submitted as a statement of the functions and organization of B Section:

1. The solution of all military and diplomatic and certain specified commercial codes and ciphers and the translation of the messages written therein of all actual and potential enemy governments and such governments as directed. Also the solution of all open codes and any other visible forms of secret writing including shorthand submitted to it by other agencies of the army. The operation of an IBM service for SSB.

2. The organization of B Section is as indicated by the accompanying chart.

3. The functions of the subsections of B Section are as follows:

(a) B-I. The recording and indexing of all messages received from E Section; the decryptographing of all messages in known systems; the translation of all decryptographed messages; the reading and study of all shorthand and open code material submitted by other agencies of the army; the preparation of a daily bulletin of solved and translated messages and its delivery to G-2 and the Navy; the operation of a library and a collateral information service; the recording, accounting for and proper dissemination of all classified collateral information in documentary form; and the operation of a Japanese language school for translators.

(b) B-II. The solution of all codes indicated in paragraph 1 including additive enciphered codes but excluding codes enciphered by means other than additive.

~~SECRET~~

~~SECRET~~

IN REPLY REFER TO

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

(c) B-III. The solution of all ciphers indicated in paragraph 1 including codes enciphered by means other than additive.

(d) B-IV. The operation of the IBM service indicated in paragraph 1.

4. The functions of the Technical Committee, consisting of the subsection heads and other selected persons, are to study the over-all operation of the section and make appropriate recommendations to the Officer in Charge of B Section.

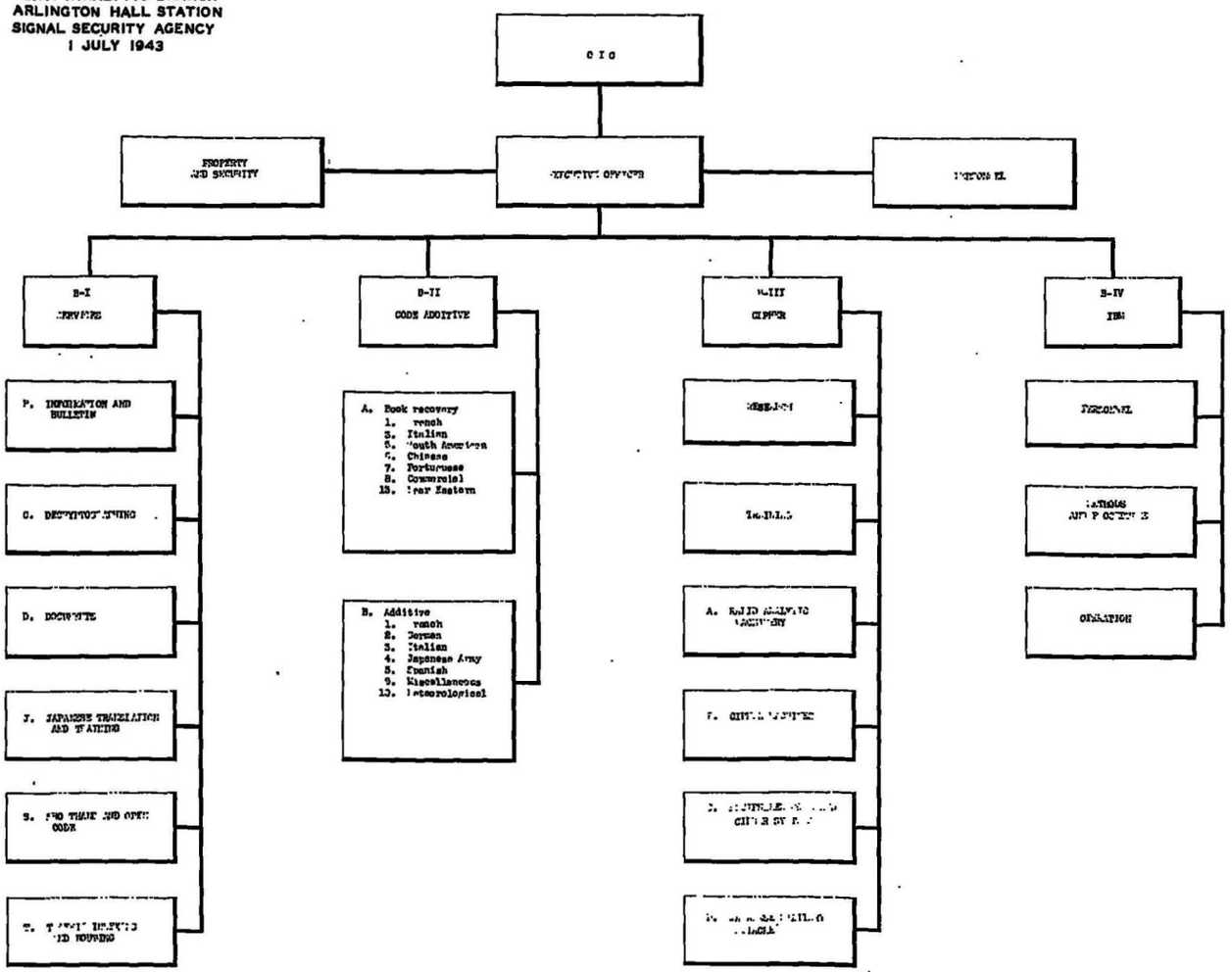
5. The functions of the Coordinators, one for each government whose codes and ciphers are under study, are to coordinate the activities of the various language groups where they cross subsection lines and make appropriate recommendations to the Officer in Charge of B Section.

6., In connection with all of its functions and as part of the execution thereof, B Section conducts in-service training for its personnel in accordance with its requirements.

Harold Doud,
Lt. Col., Signal Corps.

~~SECRET~~

B
CRYPTANALYTIC BRANCH
ARLINGTON HALL STATION
SIGNAL SECURITY AGENCY
1 JULY 1943



SECRET

PLAN OF ORGANIZATION
CENTRAL CRYPTANALYTIC BRANCH
B-III

GENERAL CRYPTANALYTIC SECTION
Major Frank B. Rowlett

SEPTEMBER 1945

ADMINISTRATIVE

TRAINING: Lt/Col Daniel M. Corbin

RECORDER: Dr. Albert Howard Carter

RESEARCH: Mr. Robert O. Ferner, CIC

SPECIAL EXAMINATION: Captain E. J. Vogel

B-3-a
Major Gordon T. Fish

1. ITALIAN
   Capt. F. Duke
2. SPANISH-PORTUGUESE
   Lt. J. V. Haggard
3. CHINESE-THAI
   Lt. L. P. Roberts
4. PLAIN TEXT
   Lt. J. J. Apollony
5. NEAR EASTERN
   Lt. J. A. Salem
6. SPECIAL PROBLEMS
   Lt.G. E. McCracken

B-3-b
Major E. J. Wrigley

2. GERMAN
   Lt. Leonard J. Seidenglanz
9. SPECIAL PROBLEMS
   Lt. F. L. Coudert
10. WEATHER
    Lt. William H. Hezlep

B-3-c
Captain E. Dale Marston

1. RAM
   Captain E. Dale Marston
   a. OPERATIONS
      Lt. L. Wheatley
   b. MAINTENANCE
      Lt. L. W. Moran
2. MACHINE CIPHERS
   Capt. Ray Johnson
3. MISCELLANEOUS CIPHERS
   Lt. James C. O'Neill
4. JAPANESE DIPLOMATIC AND JAPANESE MILITARY ATTACHE
   Mr. Samuel B. Snyder
   c. CODES — Miss Elizabeth Stephens
   d. ADDITIVE — Lt. Karl Elmquist
   t. TRAFFIC — Sgt. John Richardson
   a. JMA — Lt. Donald McCown
   b. PURPLE — Lt. L. Phelps

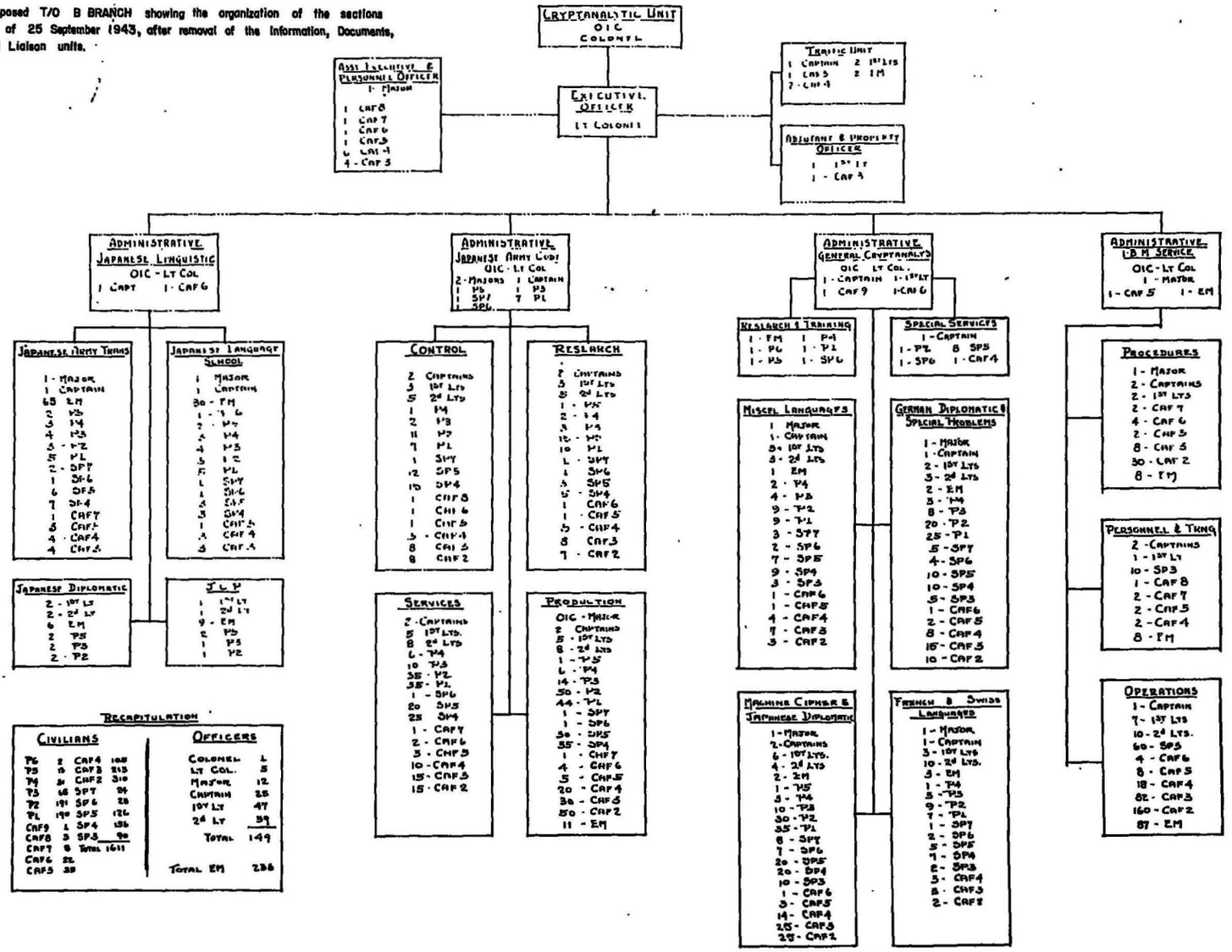
B-3-d
Major William Edgerton

1. ADDITIVES
   Captain J. J. Carroll
2. SWISS AND BELGIAN CODES
   Capt. Thomas H. Glenn
3. OTHER ENCIPHERED CODES
   Lt. Elwood Hill
4. TRAFFIC
   Miss Ruth Adams
5. DECRYPTOGRAPHING
   Miss Katharine L. Swift

SECRET

SECRET

Proposed T/O B BRANCH showing the organization of the sections as of 25 September 1943, after removal of the Information, Documents, and Liaison units.

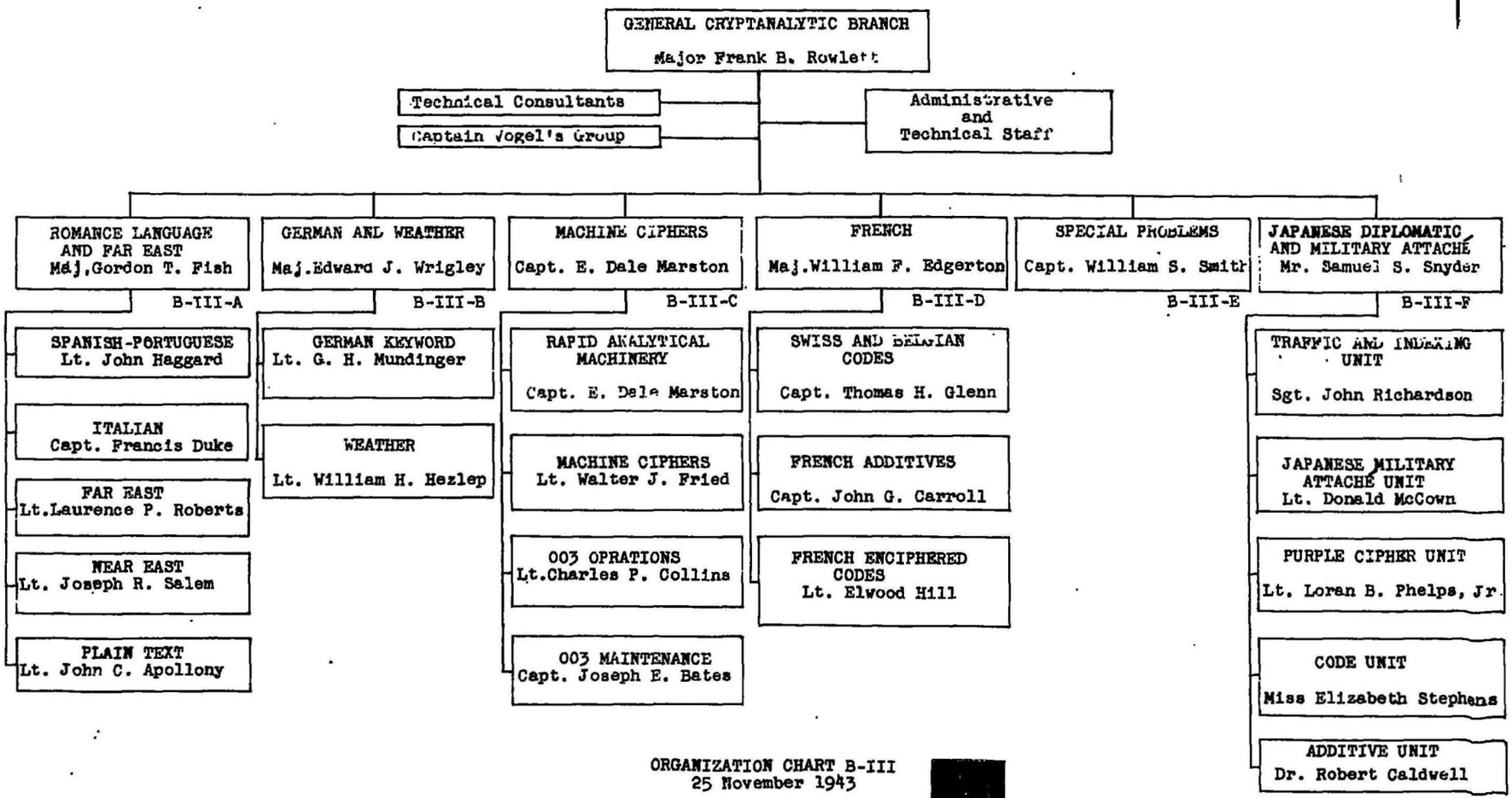


RECAPITULATION

CIVILIANS				OFFICERS	
P6	2	CAF 4	108	COLONEL	1
P5	10	CAF 3	213	LT COL.	3
P4	31	CAF 2	310	MAJOR	12
P3	68	SPT	94	CAPTAIN	25
P2	191	SP6	28	1ST LT	47
P1	192	SP5	126	2D LT	39
CAF 9	1	SP4	136	TOTAL	149
CAF 8	3	SP3	90		
CAF 7	8	TOTAL 1611			
CAF 6	22				
CAF 5	38			TOTAL EM	236

SECRET

~~SECRET~~



ORGANIZATION CHART B-III
25 November 1943

~~SECRET~~

~~SECRET~~

B
CRYPTANALYTIC BRANCH
ARLINGTON HALL STATION
SIGNAL SECURITY AGENCY
17 APRIL 1944

APPROVED:
W. Preston Corderman
W. PRESTON CORDERMAN
COLONEL, SIGNAL CORPS
COMMANDING

ADMINISTRATIVE

1 Colonel	1 CnF-14
1 Lt. Col.	2 CnF-9
1 Major	1 CnF-8
1 Captain	1 CnF-7
3 1st Lts.	2 CnF-6
4 2nd Lts.	10 CnF-5
11 Officers	14 CnF-4
	14 CnF-3
12 Enlisted	46 Civilians
Total Personnel	69

B-I

1 Lt. Col.	2 P-6
1 Major	8 P-5
8 Captains	25 P-4
30 1st Lts.	35 P-3
46 2nd Lts.	35 P-2
	30 P-1
86 Officers	1 SP-8
	23 SP-7
	32 SP-6
	50 SP-5
	50 SP-4
	1 CnF-13
	1 CnF-9
	2 CnF-8
	2 CnF-7
	3 CnF-6
	15 CnF-5
	5 CnF-4
	15 CnF-3
254 Enlisted	387 Civilians
Total Personnel	641

B-II

1 Colonel	3 P-6
1 Lt. Col.	8 P-5
2 Majors	55 P-4
15 Captains	80 P-3
31 1st Lts.	100 P-2
40 2nd Lts.	110 P-1
90 Officers	8 SP-8
	100 SP-7
	100 SP-6
	250 SP-5
	125 SP-4
	1 CnF-14
	4 CnF-9
	4 CnF-8
	4 CnF-7
	4 CnF-6
	845 CnF-5
	80 CnF-4
	150 CnF-3
80 Enlisted	1306 Civilians
Total Personnel	1444

B-III

1 Lt. Col.	1 P-7
4 Majors	3 P-6
9 Captains	6 P-5
16 1st Lts.	45 P-4
20 2nd Lts.	50 P-3
	50 P-2
50 Officers	65 P-1
	2 SP-8
	10 SP-7
	15 SP-6
	8 SP-5
	110 SP-4
	4 CnF-14
	1 CnF-13
	3 CnF-9
	3 CnF-8
	3 CnF-7
	3 CnF-6
	155 CnF-5
	30 CnF-4
	80 CnF-3
65 Enlisted	781 Civilians
Total Personnel	896

B-IV

1 Lt. Col.	3 P-6
1 Major	12 P-5
4 Captains	15 P-4
18 1st Lts.	30 P-3
18 2nd Lts.	33 P-2
	1 SP-8
42 Officers	25 SP-7
	20 SP-6
	20 SP-5
	25 SP-4
	1 CnF-13
	1 CnF-9
	2 CnF-8
	2 CnF-7
	2 CnF-6
	134 CnF-5
	18 CnF-4
	20 CnF-3
13 Enlisted	466 Civilians
Total Personnel	523

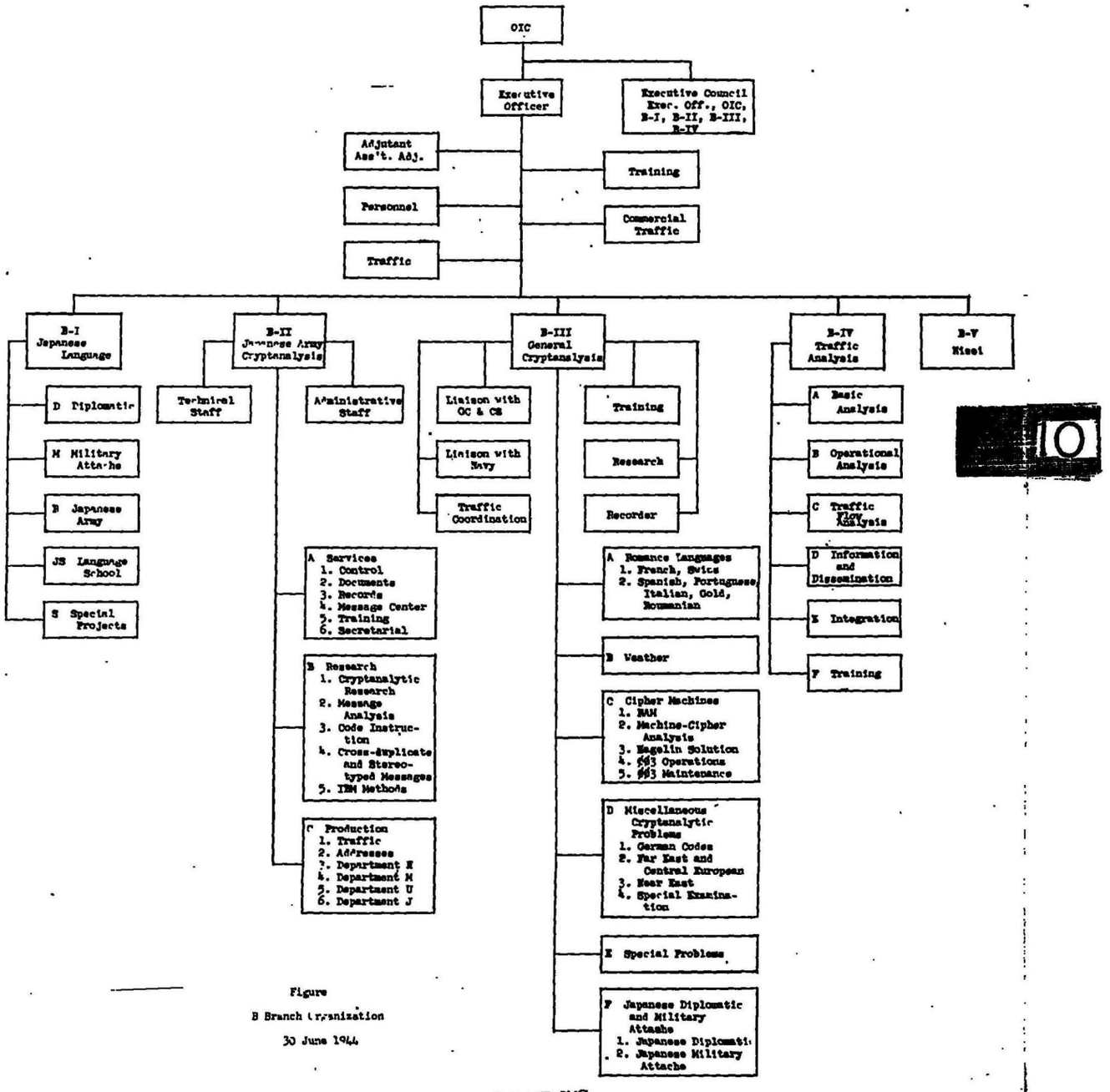
B-V

1 Major	
1 Captain	
2 1st Lts.	
4 Officers	
*	
Total Personnel	4

RECAPITULATION

MILITARY	CIVILIAN
2 Colonels	1 P-7
5 Lt. Cols.	8 P-6
10 Majors	28 P-5
36 Captains	118 P-4
130 1st Lts.	141 P-3
161 2nd Lts.	240 P-2
	220 P-1
343 Officers	13 SP-8
	178 SP-7
	220 SP-6
	283 SP-5
	411 SP-4
	3 CnF-14
	2 CnF-13
	11 CnF-9
	12 CnF-8
	12 CnF-7
	12 CnF-6
	484 CnF-5
	128 CnF-4
	324 CnF-3
369 Enlisted	3488 Civilians
Total Personnel	4234

* 43 Enlisted Personnel from B-I located at Vint Hill and assigned to that Station.



Figure

B Branch Organization

30 June 1944

Doc ID: 6554247

SECRET

B-III

Lt. Colonel Rowlett

19 August 1944

Reorganization

1. In accordance with a directive from the Commanding Officer, Signal Security Agency, a reorganization of the Agency will become effective 21 August 1944.

2. On the above date the undersigned becomes Chief of the Intelligence Division.

3. Effective the 21 August 1944 and until further notice, the Intelligence Division will consist of five branches. A brief description of these five branches follows:

a. Japanese Language Branch, abbreviated title, B I. Officer in Charge:- Lt. Colonel Verner C. Aurell. Composition:- This branch will consist of the present Section B I plus the present Section B V.

b. Military Cryptanalytic Branch, abbreviated title, B II. Officer in Charge:- Lt. Colonel S. Kullback. Composition:- The present Section B II.

c. General Cryptanalytic Branch, abbreviated title, B III. Officer in Charge:- Lt. Colonel Frank B. Rowlett. Composition:- The present Section B III.

d. Traffic Analysis and Control Branch, abbreviated title, B IV. Officer in charge:- Major Robert T. Walker. Composition:- The present Section B IV plus the Control Section of the present E Branch.

e. Information and Liaison Branch, abbreviated title, I & L. Officer in Charge:- Major J. H. Frier. Composition:- The present Information and Liaison Branch less the Production Trends Section.

4. Under the new organization the office of the Division Chief is not an office of record and, consequently, many of the functions now performed by the Office of the Chief of B Branch will devolve upon chiefs of the five branches set up as above. These functions will include personnel and supply.

5. The branch chiefs will be authorized direct correspondence

SECRET

on technical matters with other branches of SSA or offices within SSA and with field signal intelligence establishments. They will be authorized to authenticate their own telegrams and correspondence.

6. On the other hand, all matters involving policy, new procedures, the transfer of personnel, and matters which require coordination between other branches of the Intelligence Division, or with other branches and offices of the SSA will be authorized only by the Division Chief. In such cases, the coordination will be secured by the branch of origin and will bear on the face of the document a written indication of the concurrence of the other branch or branches concerned prior to submission to the Chief, Intelligence Division.

7. The sole purpose of this reorganization is to increase the efficiency of the derivation of intelligence from radio intercept by avoiding any possible duplication of effort by bringing closer together all activities concerned with the production of signal intelligence. In accomplishing this end, it is desired that there be no interruption in existing procedures, that there be no movement of personnel or equipment, and that within branches there be as few changes as possible in the responsibilities and duties of the branch personnel. Certain changes will of necessity have to be made if the full benefit of the reorganization are to be realized but these changes will be made slowly, based upon the experience of the new alignment and with a minimum of interruption to existing procedures.

8. The organization described above will be tried out for a period of approximately six weeks upon the conclusion of which recommendations will be made by the Chief, Intelligence Division to the Commanding Officer, Signal Security Agency concerning any changes which it may be desired to incorporate in the permanent reorganization. It is desired that all five branch chiefs keep this in mind during the entire period and that they submit to me not later than 12 September their comments and recommendations concerning the new organization.

/s/ Harold G. Hayes

Harold G. Hayes
Colonel, Signal Corps
SPSIB, Ext. 311

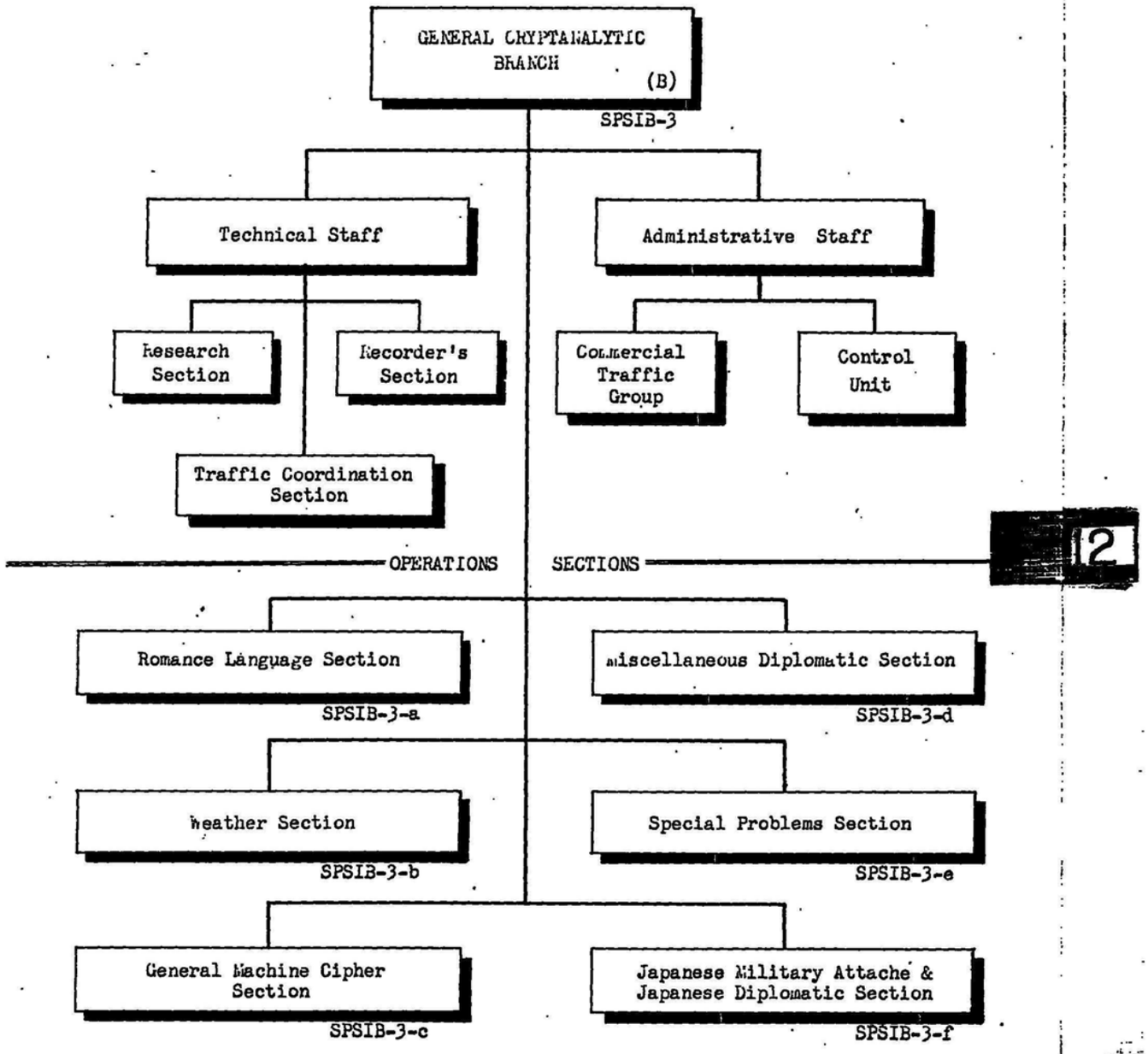
SECRET

Doc ID: 6554247

~~SECRET~~

ORGANIZATION OF GENERAL CRYPTANALYTIC BRANCH

21 August 1944



2

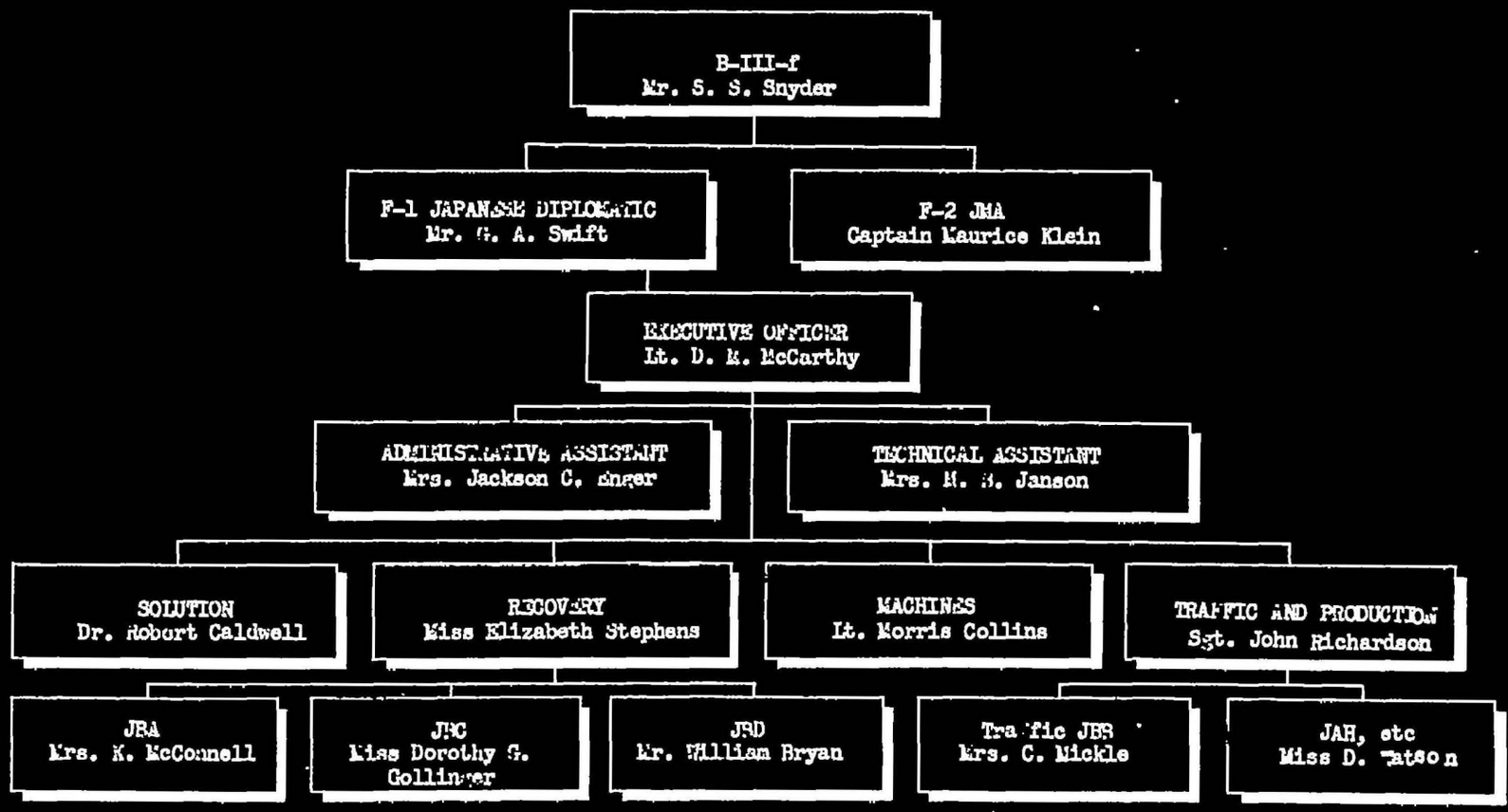
~~SECRET~~

SECRET

PLAN OF ORGANIZATION

JAPANESE DIPLOMATIC SECTION

Spring 1944

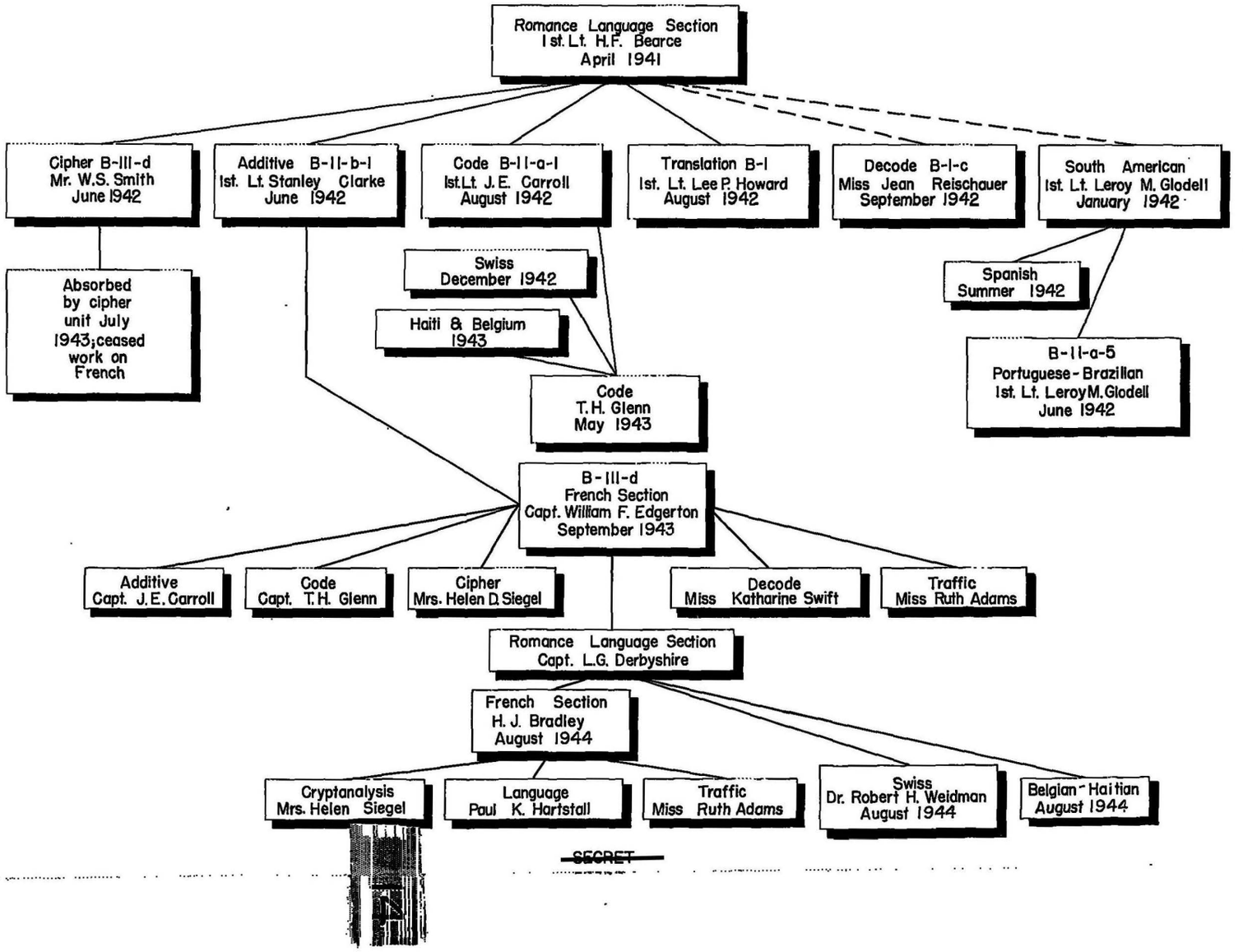


SECRET

Doc ID: 6554247

~~SECRET~~

EVOLUTION OF THE ROMANCE LANGUAGE SECTION
1941 TO 1944



~~SECRET~~

SECRET

COUNTRY	July Rec.	July Pub.	August Rec.	August Pub.	September Rec.	September Pub.	October Rec.	October Pub.	November Rec.	November Pub.	December Rec.	December Pub.	January Rec.	January Pub.	February Rec.	February Pub.	March Rec.	March Pub.	April Rec.	April Pub.	May Rec.	May Pub.	June Rec.	June Pub.	Total Rec.	Total Pub.
Afghanistan	66	$	66	$	$	$	$	$	$	$	$	$	63	$	80	$	64	$	49	$	65	6	76	5	593	11
Albania	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	1	$	2	$	3	1
Argentina	see South America				187	74	116	56	67	37	49	12	132	53	188	69	468	96	821	94	749	89	581	68	3404	642
Belgium	437	7	587	66	328	82	223	114	288	18	$	$	$	$	$	3	261	6	341	$	537	2	1883	$	3953	225
Bolivia	see South America				23	14	32	3	48	7	42	2	186	51	66	11	121	21	295	47	293	7	413	15	1429	178
Brazil	see South America				516	69	544	68	584	22	596	21	914	32	945	49	925	35	1693	36	1668	33	1171	28	8876	379
Bulgaria	167	$	196	$	8	$	$	$	$	$	$	$	$	$	$	$	$	$	243	$	382	$	423	1	976	1
Burma	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	1	$	$	2	$
Chile	see South America				429	339	442	164	413	162	377	47	665	116	577	113	819	147	1845	128	826	114	968	154	6341	1418
China (combined)	$	46	$	232																						
Chungking	see China (combined)				2521	112	2146	82	2404	77	1628	76	961	82	849	53	1488	73	1862	98	1984	161	2298	74	17559	838
Nanking	see China (combined)				$	$	$	$	$	$	$	$	14	$	187	$	455	$	1128	3	1812	$	1869	$	5873	$
Colombia	see South America				22	2	67	6	68	3	56	7	148	15	142	29	583	28	859	36	769	15	938	78	3374	249
Costa Rica	see South America				$	$	$	$	$	$	$	$	$	$	$	$	$	$	243	4	313	1	295	$	854	5
Croatia	13	$	37	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	31	$	81	$
Cuba	see South America				34	21	41	3	34	7	36	1	32	7	36	8	619	17	1147	17	1267	13	1146	9	4386	103
Czechoslovakia	226	$	449	$	$	$	148	$	$	$	$	$	$	$	$	$	$	$	134	$	49	$	132	$	463	$
Denmark	363	$	287	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	119	$	128	$	125	$	372	$
Dominican Republic	see South America				118	78	158	85	141	45	75	24	118	36	84	12	327	21	335	11	451	28	853	45	2668	363
Ecuador	see South America				293	88	146	2	148	5	122	1	292	7	422	9	521	2	587	12	721	18	833	58	3995	194
Egypt	78	$	112	$	8	$	8	$	4	4	5	$	3	$	16	$	163	1	132	1	282	4	118	$	595	16
Esthonia	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	2	$	1	$	$	$	3	$
Ethiopia	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	17	$	9	$	24	$	79	$
Finland	476	343	638	156	265	129	182	39	221	18	118	185	224	82	486	61	833	134	462	77	598	83	394	68	5843	1796
France	6362	586	8838	742	3674	586	3679	1697	3934	1194	3585	1295	6818	1391	8395	1246	14428	1588	12615	1665	11978	2368	9954	2632	74972	15596
Germany	8969	2265	8328	2741	2415	3685	11592	1661	3162	1613	2664	1698	21857	547	24747	992	24421	655	21885	739	18751	421	13632	474	144246	11798
Greece	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	698	8	486	15	336	32	1672	75
Greenland	22	$	46	$	38	$	$	1	$	$	$	$	$	$	$	$	$	$	148	$	183	$	114	$	393	1
Guatemala	see South America				6	$	12	$	2	$	3	$	2	$	$	$	$	$	56	$	94	3	288	$	586	3
Haiti	see South America				$	$	$	$	165	$	$	$	$	$	$	$	$	$	77	3	187	3	87	1	487	11	483	18
Honduras	see South America				$	$	$	$	$	$	$	$	$	$	$	$	$	$	43	$	23	1	74	$	178	1
Hungary	175	$	196	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	181	$	386	11	695	6	1822	17
Iberia	2865	276	2782	1251	see Spain and Portugal																					
Iceland	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	487	$	588	$	429	$	1424	$
Iran	174	14	229	26	116	73	91	71	133	124	138	133	175	89	253	$	446	4	391	1	352	94	477	73	2474	542
Iraq	16	4	45	3	11	8	12	14	13	23	4	2	6	3	89	$	69	$	57	$	62	$	112	$	373	78
Ireland	161	$	327	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	254	$	228	$	216	$	684	$
Italy (including Badoglio)	2718	215	2828	413	526	148	98	37	93	28	79	29	158	26	116	21	374	143	124	48	133	66	237	185	1938	643
New Mussolini govt.	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	224	136	398	178	296	227	916	535
Japanese	185693	4222	147385	7478	6546	3672	16841	3463	8789	3498	13478	3554	16147	3896	18437	4419	23422	3972	24915	4699	31465	6242	26678	3925	169918	44538
Latvia	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	8	$	18	$	1	$	19	$
Liberia	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	21	$	13	$	14	$	48	$
Lithuania	$	$	$	$	6	$	$	$	$	$	$	$	$	$	$	$	$	$	2	$	2	$	6	$	16	$
Luxembourg	$	$	$	$	8	2	$	$	$	$	$	$	5	1	15	3	21	3	21	2	15	$	55	1	149	12
Mexico	see South America				366	263	322	114	383	83	358	54	628	146	473	182	1891	142	1857	143	1968	169	1993	173	11397	1449
Netherlands	2571	$	2582	$	$	$	$	$	$	$	$	$	$	$	$	$	1539	$	1977	963	1289	1662	1733	1443	6118	3468
Nicaragua	see South America				31	$	$	$	4	$	$	$	8	$	5	$	161	3	244	1	363	1	281	3	1639	34
Norway	$	$	$	$	$	$	$	$	$	$	258	$	217	$	237	$	238	$	536	1	639	2	363	$	2679	$
Panama	see South America				18	18	$	$	11	4	8	$	35	13	36	12	67	16	299	1	23	7	631	8	1431	74
Paraguay	see South America				$	$	$	$	$	$	$	$	14	$	8	$	45	2	68	$	85	2	49	2	261	6
Peru	see South America				112	51	114	22	99	25	186	44	244	79	238	77	466	84	634	153	548	94	548	138	3181	729
Philippines	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	19	$	1	$	22	$
Poland	733	4	965	6	$	$	$	$	$	$	$	$	28	$	4	$	$	$	565	18	836	$	462	$	1827	18
Portugal	see Iberia				468	42	489	306	521	149	473	117	1666	138	1229	121	1276	223	2368	298	1669	292	1566	163	14373	1743
Rumania	378	$	354	4	126	$	$	1	$	$	$	$	$	$	$	$	$	$	83	$	46	1	$	$	633	2
Salvador	see South America				$	$	$	$	1	$	$	$	$	$	3	$	165	11	159	$	172	8	179	2	679	21
Saudi Arabia	1	$	$	$	2	$	67	63	44	34	9	$	$	$	2	$	3	$	1	$	2	$	$	$	136	99
Slovakia	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	$	11	$	98	$	15	13	124	13
South America	4657	396	5511	997	see the several countries																					
Spain	see Iberia				339	167	497	164	398	153	525	163	866	179	1694	137	2663	891	1821	283	1853	172	1249	164	14257	1797
Sweden	1338	12	2482	1	399	$	515	$	723	$	642	$	1877	$	1353	$	1272	$	2517	$	2598	$	2378	3	13436	3
Switzerland	1878	335	2242	457	961	439	814	562	1138	376	1158	152	1482	135	1451	183	2119	174	2695	185	2615	254	2381	281	16664	2617
Thailand	$	$	$	11	65	5	164	26	116	21	157	2	291	14	224	55	289	97	217	74	187	188	292	11	1897	433
Turkey	732	12	684	39	321	44	446	74	351	169	279	155	383	78	899	8	1267	16	1284	13	1558	76	1953	68	8661	677
Uruguay	see South America				38	29	18	2	33	1	13	$	64	3	39	5	97	$	168	1	139	6	169	3	762	58
Venezuela	see South America				92	98	127	12	84	12	183	6	287	52	189	55	1117	38	1817	85	1226	63	1338	97	5272	452
Yugoslavia	322	17	518	37	21	288	718	$	$	$	189	$	$	$	$	9	$	1	459	$	418	$	312	2	2921	212
Total	221829	8776	188989	14614	21863	14829	33886	8535	24171	7832	27225	7844	55316	7191	63432	7934	84866	8827	92698	9771	94116	11997	85791	16696	576966	89467

Figure . The production of B-III throughout the year, showing the number of messages received and the number published for each government or governmental group. The figures do not include a great number of messages decryptographed but not published. The totals given in the column farthest to the right are for the ten months from September through June because of the new system of accounting inaugurated in September. Further, the great rise in figures for April is largely due to the fact that plain text was systematically counted for the first time in that month. The figures become increasingly more accurate as the system of accounting was perfected; those for the first six months of 1944 are far more reliable than those for 1943.

*The figures given are totals for the several French governmental groups (Vichy, Giraudist, etc.), whose systems sometimes overlay. **The figures for Japan include Army traffic for July and August of 1943, the province of B-I and B-II. In the later period also, they reflect the contribution of B-I in translation and code reconstruction.

SECRET

554247

TOP SECRET

PROCESSING OF DIPLOMATIC TRAFFIC

TOP SECRET

Doc ID: 6554247

TOP SECRET

PROCESSING OF DIPLOMATIC TRAFFIC
40 GROUP UNITS

September 1944

SECTION AND NATIONAL GROUP	NO. TRIS.	TOTAL RECEIVED	DUPLICATES	ORIGINALS	NOT PROCESSED AT ALL	NOT DECIPHERED OR DECODED						DECODED OR DECIPHERED	NOT TRANSLATED OR SUMMARIZED						TRANSLATED OR SUMMARIZED
						Total	System Unsolved	Book key or indicator incompletely solved	Text Incomplete	Backlog	Lack of Personnel		Total	Low Intelligence	Held for Parts	Held for British Translation	Lack of Personnel	Backlog	Incomplete Text	
B III-A																				
Spain	3	2,981	1,276	1,765	-	1,115	28	1,685	2	-	-	596	40	33	-	7	-	-	-	556
Argentina	4	760	344	416	-	30	-	4	-	26	-	386	172	172	-	-	-	-	-	214
Bolivia	2	162	32	130	-	75	3	72	-	-	-	55	-	-	-	-	-	-	-	55
Chile	2	814	305	505	-	70	35	-	-	35	-	435	270	270	-	-	-	-	-	165
Colombia	2	538	225	313	-	34	-	34	-	-	-	279	98	98	-	-	-	-	-	181
Cuba	3	32	-	33	-	1	1	-	-	-	-	32	29	29	-	-	-	-	-	3
Dominican Republic	1	239	22	217	-	28	-	28	-	-	-	189	141	141	-	-	-	-	-	48
Ecuador	4	571	250	321	104	33	3	26	1	3	-	184	109	109	-	-	-	-	-	75
Guatemala	1	31	4	27	-	27	27	-	-	-	-	-	-	-	-	-	-	-	-	-
Haiti	1	37	2	35	-	-	-	-	-	-	-	35	25	20	-	-	-	5	-	10
Mexico	8	724	155	569	-	172	43	76	-	53	-	397	169	169	-	-	-	-	-	228
Nicaragua	2	4	1	3	-	3	3	-	-	-	-	-	-	-	-	-	-	-	-	-
Peru	2	402	103	299	-	1	-	-	-	1	-	298	143	143	-	-	-	-	-	155
Panama	1	39	-	39	-	-	-	-	-	-	-	39	39	39	-	-	-	-	-	-
Paraguay	1	3	-	3	-	3	3	-	-	-	-	-	-	-	-	-	-	-	-	-
Uruguay	3	70	12	58	-	2	2	-	-	-	-	56	37	37	-	-	-	-	-	19
San Salvador	1	1	-	1	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-
Venezuela	2	258	97	161	-	1	-	1	-	-	-	160	97	97	-	-	-	-	-	63
Tot. Span. Lang.	43	7,663	2,828	4,835	104	1,596	148	1,327	3	118	-	3,135	1,369	1,357	-	7	-	5	-	1,766
Portugal	17	2,649	1,325	1,324	-	321	30	1	1	143	146	1,003	507	404	-	3	2	98	-	496
Brazil	7	1,625	668	957	-	438	1	322	-	-	115	519	342	261	-	-	-	81	-	177
France	32	19,037	10,476	8,561	-	2,574	1,953	616	1	4	-	5,987	1,660	1,589	37	-	2	1	31	4,327
Belgium	3	574	32	542	-	294	196	-	-	-	98	248	165	165	-	-	-	-	-	83
Switzerland	15	7,335	3,716	3,619	-	1,961	26	1,734	7	193	1	1,658	311	126	1	-	184	-	-	1,347
Italy	8	940	493	447	158	137	-	14	-	123	-	152	18	18	-	-	-	-	-	134
Luxembourg	1	5	-	5	-	-	-	-	-	-	-	5	3	3	-	-	-	-	-	2
Rumania	6	1,526	216	1,310	-	1,310	1,310	-	-	-	-	-	-	-	-	-	-	-	-	-
TOTAL B III-A	132	41,354	19,754	21,600	262	8,631	3,664	4,014	12	581	360	12,707	4,375	3,923	38	10	188	185	31	8,332
B III-C																				
Finland	3	345	174	171	-	171	171	-	-	-	-	-	-	-	-	-	-	-	-	-
Netherlands	2	1,557	298	1,259	-	826	99	727	-	-	-	433	-	-	-	-	-	-	-	433
Norway	1	720	-	720	720	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Sweden	2	2,024	825	1,199	-	1,199	1,199	-	-	-	-	-	-	-	-	-	-	-	-	-
Germany	2	1,136	498	638	-	638	638	-	-	-	-	-	-	-	-	-	-	-	-	-
TOTAL B III-C	10	5,782	1,795	3,987	720	2,834	2,107	727	-	-	-	433	-	-	-	-	-	-	-	433
B III-D																				
Germany	4	39,135	6,809	32,326	30,180	47	-	47	-	-	-	2,099	506	182	-	-	-	324	-	1,593
Hungary	1	1,059	453	606	-	588	582	6	-	-	-	18	-	-	-	-	-	-	-	18
Total B III-D-1	5	40,194	7,262	32,932	30,180	635	582	53	-	-	-	2,117	506	182	-	-	-	324	-	1,611
Bulgaria	2	1,151	622	529	-	273	273	-	-	-	-	256	228	-	-	54	-	174	-	28
China	18	4,696	909	3,787	2,844	196	115	53	5	23	-	747	560	552	8	-	-	-	-	187
Croatia	2	82	25	57	-	57	57	-	-	-	-	-	-	-	-	-	-	-	-	-
Czechoslovakia	3	495	25	470	-	359	299	60	-	-	-	111	96	96	-	-	-	-	-	15
Greece	3	1,333	826	507	80	-	-	-	-	-	-	427	10	5	-	5	-	-	-	417
Philippines	1	4	-	4	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Poland	6	1,221	227	994	-	925	452	473	-	-	-	69	1	1	-	-	-	-	-	68
Slovakia	1	30	3	27	-	27	27	-	-	-	-	-	-	-	-	-	-	-	-	-
Thailand	1	279	50	229	-	3	-	3	-	-	-	226	60	52	-	-	-	8	-	166
Yugoslavia	2	189	41	148	-	137	69	68	-	-	-	11	-	-	-	-	-	-	-	11
Total B III-D-2	39	9,480	2,728	6,752	2,928	1,977	1,252	657	5	23	-	1,847	955	706	8	59	-	182	-	892
Afghanistan	1	51	14	37	-	18	-	18	-	-	-	19	13	6	-	-	7	-	-	6
Egypt	1	40	8	32	-	8	-	8	-	-	-	24	7	7	-	-	-	-	-	17
Ethiopia	2	25	-	25	-	15	-	15	-	-	-	10	4	4	-	-	-	-	-	6
Ireland	2	44	3	41	-	41	33	8	-	-	-	-	-	-	-	-	-	-	-	-
Iraq	3	46	14	32	-	1	-	-	1	-	-	31	8	8	-	-	-	-	-	23
Iran	1	626	275	351	-	39	-	29	10	-	-	312	189	90	-	88	11	-	-	123
Saudi Arabia	2	41	4	37	-	37	1	36	-	-	-	-	-	-	-	-	-	-	-	-
Turkey	8	2,758	1,135	1,623	-	109	14	8	87	-	-	1,514	720	717	3	-	-	-	-	794
Total B III-D-3	20	3,631	1,453	2,178	-	268	48	122	98	-	-	1,910	941	832	3	88	18	-	-	969
TOTAL B III-D	64	53,305	11,443	41,862	33,108	2,880	1,922	832	103	23	-	5,874	2,402	1,720	11	147	18	506	-	3,472
B III-F - Jap. Dip.	22	51,178	32,451	18,727	-	3,132	2,323	618	128	63	-	15,595	6,555	1,600	321	800	2,561	1,273	-	9,040
B. Adm. T.																				
Denmark	1	25	18	7	7	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Greenland	2	15	-	15	15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Iceland	2	9	1	8	8	-	-	-	-	-	-	31	20	20	-	-	-	-	-	11
Ireland	1	34	3	31	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Liberia	1	18	1	17	17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Lithuania	1	4	2	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
TOTAL B. Admin.T	8	105	25	80	49	-	-	-	-	-	-	31	20	20	-	-	-	-	-	11
Special																				
KI	5	1,365	609	756	159	-	-	-	-	-	-	597	412	412	-	-	-	-	-	185
ZY	10	14,399	885	13,514	-	13,514	13,514	-	-	-	-	-	-	-	-	-	-	-	-	-
ZZ	6	18,267	5,174	13,093	-	13,093	13,093	-	-	-	-	-	-	-	-	-	-	-	-	-
TOTAL SPECIAL	21	34,031	6,668	27,363	159	26,607	26,607	-	-	-	-	597	412	412	-	-	-	-	-	185
Totals B III Sect.																				
B III-A	132	41,354	19,754	21,600	262	8,631	3,664	4,014	12	581	360	12,707	4,375	3,923	38	10	188	185	31	8,332
B III-C	10	5,782	1,795	3,987	720	2,834	2,107	727	-	-	-	433	-	-	-	-	-	-	-	433
B III-D	64	53,305	11,443	41,862	33,108	2,880	1,922	832	103	23	-	5,874	2,402	1,720	11	147	18	506	-	3,472
B III-F	22	51,178	32,451	18,727	-	3,132	2,323	618	128	63	-	15,595	6,555	1,600	321	800	2,561	1,273	-	9,040
B. Admin. T	8	105	25	80	49	-	-	-	-	-	-	31	20	20	-	-	-	-	-	11
Special	21	34,031	6,668	27,363	159	26,607	26,607	-	-	-	-	597	412	412	-	-	-	-	-	185
GRAND TOTAL	257	185,755	72,136	113,619	34,297	44,084	36,623	6,191	243	667	360	35,237	13,764	7,675	370	957	2,767	1,954	31	21,473
% of Intercepts		100.00	38.81	61.17	18.46	23.7	19.7	3.3	0.13	0.35	0.18	18.9	7.4	4.1	0.20	0.52	1.5	1.05	0.02	11.5
% of Originals	-	-	-	100.00	30.19	38.8	32.2	5.4	0.21	0.59	0.32	31.01	12.11	6.76	0.32	0.84	2.44	1.72	0.0	18.88
PLAIN TEXT	-	21,916	1,697	20,219	-	-	-	-	-	-	-	-	20,275	20,265	-	-	-	-	-	24

Doc ID: 6554247

TOP SECRET CREAM

THE FIRST TRANSLATION OF A B-MACHINE MESSAGE

Except in cases of great emergency, it is not until the cryptanalysts realize that a basic system is on the way to solution that they venture translations in that system. The reason this three-part message, translated 14 June 1940, could be submitted several months before the so-called first "Purple" Machine messages of 27 September 1940, was that the system began to break down at the moment of this translation. At this point, it was realized beyond a doubt that, in a matter of a few months, all the messages in this system could be read. The solution of this message might be said to be somewhat forced in that several obvious letters of the text were assumed.

TOP SECRET CREAM

From: Rome (Japanese Ambassador)
To: London
June 6, 1940.

Received from Berlin as #95.

Rela to London as #71. Sent to Tokyo as #328 (?), May 30th.

Part 1 of 3.

* * * The Foreign Minister of the Netherlands formally stated to the Japanese Minister ~~at~~ The Hague that the Netherlands Government would ~~(could ?)~~ not see as acceptable any country's protection of the Netherlands East Indies and that the Netherlands Government were determined to refuse any offer of protection or intervention of any kind or which may be made by any country.

The Japanese Government believes that the Netherlands Government is determined to remain true to the above quoted statement in spite of the * * * for which the Japanese Government cannot help feeling deepest sympathy. But it must, however, be appreciated by the Japanese Government that * * *. The Japanese Minister at The Hague under instructions from his government proposed to the Foreign Minister of the Netherlands that the matters to be discussed * * *. The Japanese Government is anxious to be informed as soon as possible ~~of the~~ (that ?) Netherlands Government * * * in the response to the proposal and * * * to make these instructions known and to propose that the complete negotiations should be conducted in Batavia and that the East Indies Government be instructed to that effect by the Netherlands Government.

#7610

Trans. 6/14/40 (7)

From: Rome (Japanese Ambassador)
To: London
June 6, 1940.

Received from Berlin as #95.

Relay to London as #71. Sent to Tokyo as #328 (?), May 30th.

Part 2 of 3.

* * * between Japan and the East Indies in the matters of trade enterprises, * * * the traditional friendship between the two * * * public opinion of both countries * * * by situations which bring calumny and propaganda * * * international relations * * *. The Japanese Government is only too anxious * * * the questions between * * * of the East Indies * * *. The Japanese Government shares with the Netherlands Government. * * * feel that the proposal of the Japanese Government * * * initiative for these proposals on the questions of trade enterprises underway. * * * to the effect that the Netherlands Government would not adopt any change in the measures of the export to Japan of all the East Indies products needed in Japan.

#7611

Trans. 6/14/40 (7)

From: Roma (Japanese Ambassador)
To: London
June 6, 1940.

Received from Berlin as #95.

Relay to London as #71. Sent to Tokyo as #[illegible]8 (?), May [illegible]th.

Part 1 of 2.

[illegible] to the promotion of friendly sentiment between * * * Firm in the belief that the Netherlands Government shares with the Japanese Government the desire not only to keep this fostered friendship undisturbed under any circumstances but also to continue increasing friendly relations between them, the Japanese Government proposes to the Netherlands Government * * * permit within the limits of the present emergency the trade between Japan and the East Indies * * * the Netherlands Government be good enough to give the Japanese Government an answering Japanese memorandum above answer * * * continuing the export to Japan of the undermentioned products and goods of the East Indies and to instruct the government there * * * to act accordingly:

Rubber	Scrap Iron
Mineral Oil	Chrome Ore
Bauxite	Lead
Nickel Ore	Cinchona
Manganese Ore	Molybdenum
Wolfram Ore	

Note: This is the first translation of "B" machine messages.

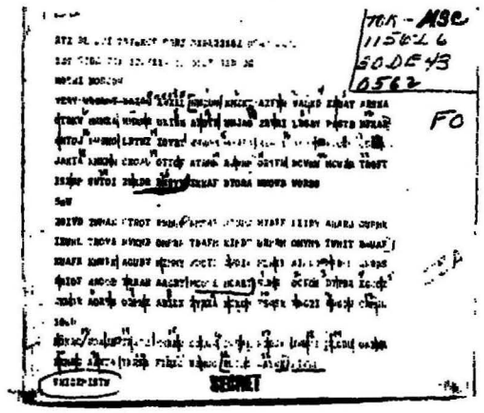
7612

Trans. 6/14/40 (7)

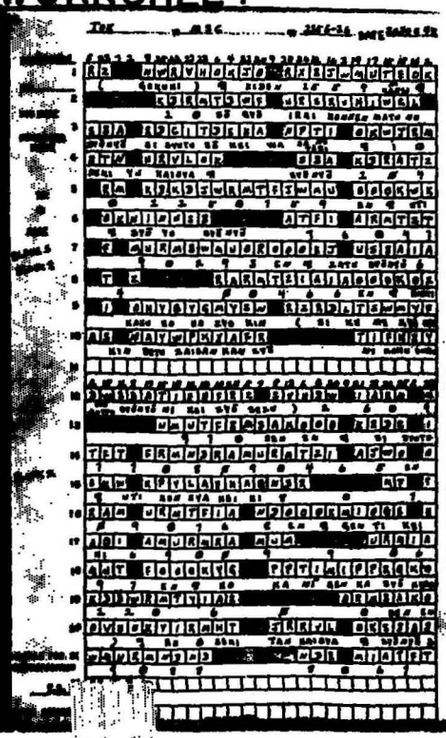
INTERCEPT

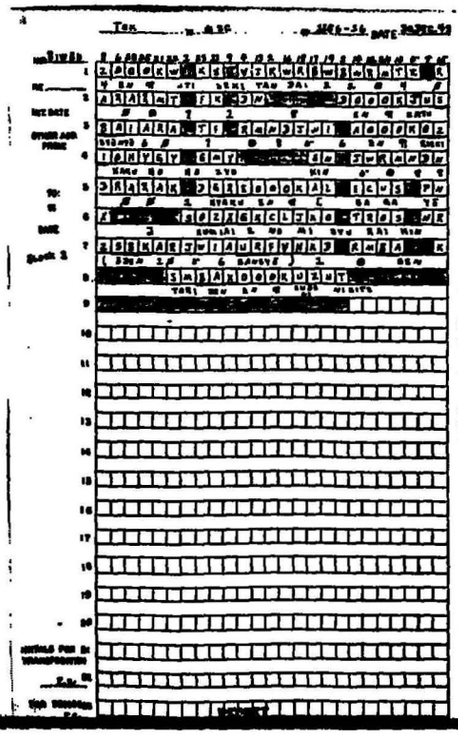
5. The JAA process.--The JAA operation is summarized in the following illustrations. The first series shows the cryptanalysis of the messages: the matrix with its blocks, the decodement, and translation; the rules for the use of blanks in the two types of encipherment; and the digraph-to-code chart. The second series illustrates problems of key recovery.

The top photograph shows an intercepted JAA message. The traffic unit has designated the serial and worksheet numbers, the date, and the origin and destination. (The message is sent ready to be transposed and decoded.) The message is marked into groups of forty (JAA letters), which constitute a block. A full block is rectangular in form, 25 cells wide, and 16 deep. Each block has a different numerical key. The message is written into the matrix and the plain is obtained from values on the digraph and trigraph charts. Finally, the translated message is shown on the last photograph on the page.

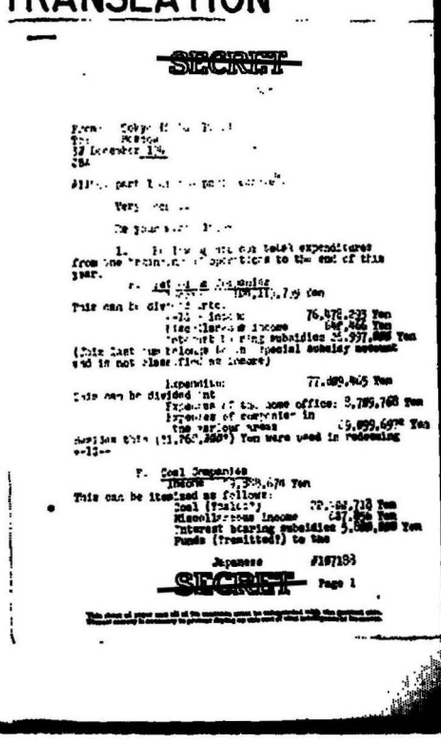


WORKSHEET





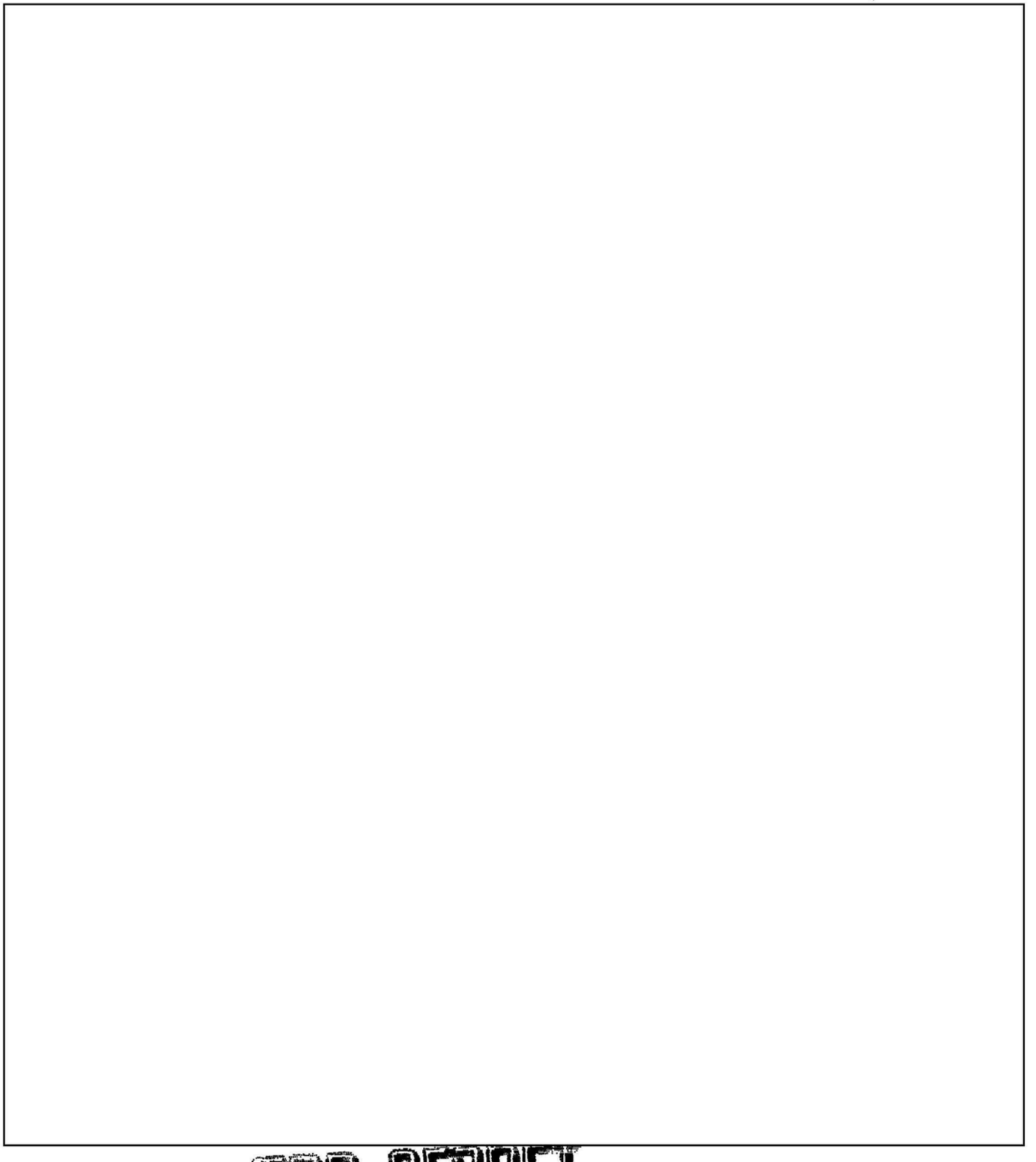
TRANSLATION



Doc ID: 6554247

EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

THE JSC PROCESS FROM INTERCEPT TO TRANSLATION



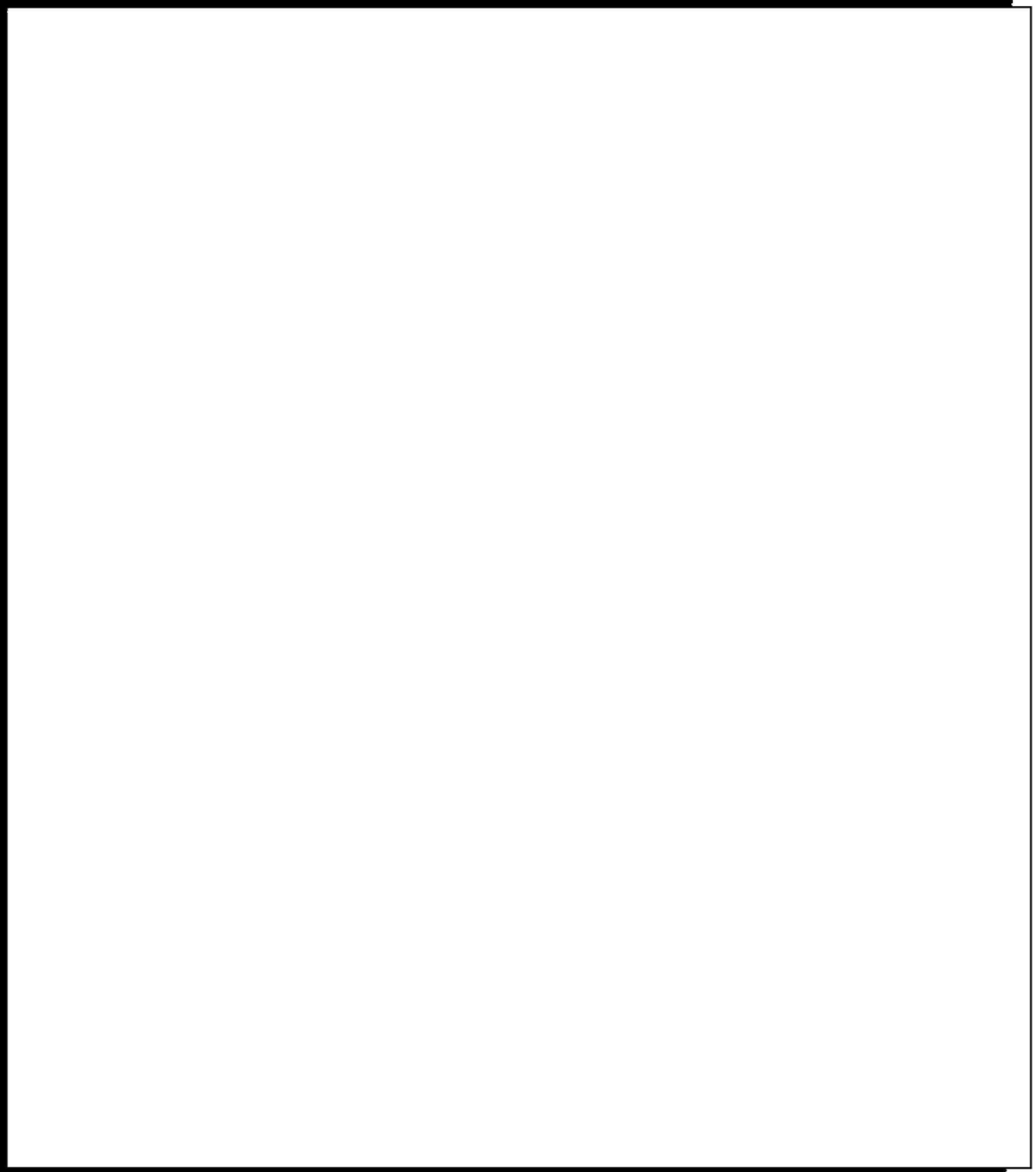
EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

[redacted]

[redacted]

EO 3.3b(3)
EO 3.3(h)(2)
PL 86-36/50 USC 3605



EO 3.3b(6)
PL 86-36/50 USC 3605
EO 3.3(h)(2)

Doc ID: 6554247

~~SECRET~~

PERSIAN ENCIPHERED CODE PROCESSING

~~SECRET~~

~~SECRET~~

PERSIAN

FROM: NEW YORK (DOCTOR NASSR)

TO: TEHERAN (FINANCE MINISTRY)

MSG.NO.: 1173

1. Message as received:

ENPPE LNIIK EZEJX KTSRF XUOHI NXVGC BXOYX FXFYK ZYYZU UBEGL XQIDP

ELMUO TUOUJ TQPRD BSUYO QIDHL PNKAM XKVHB PLTFMZ

2. The same message as above divided into tri-literal code groups and showing decipherment (purple color) and decodement (orange color). Plain text (orange) is Persian plain-text in English script.

ENP	PEL	NIL	KEZ	EJX	KTS	RFX	UOH
RBX	XRP	BLP	YRA	RED	YQZ	VND	IMN
KMP'NY	NFT	'ST'ND'R-Y	V'	KV	V	MYHV'HND	ÇN'NÇH
INX	VGC	BKO	YXE	XFY	KZY	YZU	UBE
LBZ	SGU	FDM	TDH	DHT	YAT	TAI	IFR
DVLT 'YR'N	M'YL'ST	BH	MΔ'KRH	D'ŞD	NM'YNDH	MNṢVṢ-Y	JHT
GIX	QID	PEL	MUO	TUO	UJT	QPR	DBS
GPD	CLJ	XRP	KIM	QIM	CEQ	CxV	JFZ
THṢYL	'MTY'Z-Y	NFT	DR	QSMTN'Y	'Q'MH D=VY	'YR'N-Y	H'RJ'Z
UYO	QID	HIP	NKA	MXK	VHB	PLT	FMZ
ITM	CLJ	NPX ŞRKT NFT	BYO 'GZ'MY	KDY	SNF	XPQ	HKA TLGR'F
HDVD	'MTY'Z-Y	'YR'N V 'NCLYS		D'RD	MTMNY'ST	NZRYH	NM''YD

[redacted]

~~SECRET~~

~~SECRET~~

3. Transliteration into Persian script:

کمپانی نفت استاندار واکووم میخواهند چنانچه دولت ایران مایل است به مذاکره با نماینده منصوص جهت تحصیل امتیاز نفت در قسمتهای خارج از حدود امتیاز شرکت نفت ایران و انگلیس اعزام دارد مقتضی است نظریه تلگراف نمائید

4. Translation:

The SOCONY-VACUUM OIL COMPANY wishes, if the Iranian Government is so inclined, to confer with its special representative with the view to obtaining an oil concession outside the limits of the ANGLO-PERSIAN OIL COMPANY's concession. Please wire your opinion.

~~SECRET~~

Doc ID: 6554247

TURKISH ENCIPHERED-CODE PROCESSING

Doc ID: 6554247

SECRET

TURKISH

FROM: WASHINGTON (TURKISH AMBASSADOR, MUNIR ERTEGUN)

TO: ANKARA (HARICIYE)

MSG. NO.: 47

1.

01115 15493 27024 61965 07881 68189 32544 34452 31842 11237 54431 76137 90585

49683 85086 94171 85638 48092 87039 14106 22847 76557 52212 39360 50495 34472

35500 08352 80381 68189 32164 06245 09587 82042 55113 95732 72897 33229 70437

97171 06941 61705 76481 62554 44780 35780 09090 34428 58845

2.

4653	8297	6534	5971	8765	2456	9345	8745	3638	7564
0111	5154	9327	0246	1965	0789	1681	8932	5443	4452
4764	3341	5851	5117	9620	2134	0926	6677	8071	1916
14	ŞUBAT	TARIH	VE	#24	N.T.	DA	ile	TÜRKİYE	BUGÜN
3184	2112	3754	4317	6137	9058	5496	8365	0869	4171
7737	0309	9288	9288	4892	1404	4731	6000	3497	1635
BU	BARIN-DAN	HEMEN	HEMEN	HARB	E	HAZIR	//	NUSHA	SINDAN
8563	8480	9287	0391	4106	2284	7765	5752	2123	9360
2116	6677	5711	5262	2861	4630	6000	3497	5751	6824
GEÇILEN	ile	HAFTA	LARCA	SÜRME	SI	//	NÜSHA	SINA	KADAR
5049	5344	7235	6000	8352	8033	1681	8932	1640	6245
9692	3531	3769	1971	6017	0489	0926	6677	4278	3709
OLAN	GRUP	LAR	OLUP	DAHA	AŞAĞI	DA	ile	MÜNA KAŞA	LAR
0958	7920	4255	1139	5732	7289	7332	2970	4379	7171
4601	5117	0789	6000	3497	9635	6677	0615	7907	4635
EVVELCE	VE	AHIREM	//	NUSHA	SINDAN	//	SAFHA	YA	INTIKAL
0694	1617	0576	4816	2554	4478	0357	8009	0903	4428
4247	9804	6000	9787	0219	6824	9692	6744	3531	1982
ETTIRIL	MIŞ	//	NÜSHALARINA	KADAR	OLAN	#6	GRUP	RICA	EDERIM

5864
9437
#47

TURKISH-ENCIPHERED-CODE PROCESSING

SECRET

SECRET

1. Section one represents the message as received.

2. Section two is the same message in enciphered four-digit code groups (black); and the basic four-digit code groups (red), derived by the application of the forty-digit additive (green). The plain component is Turkish plain-text (blue).

3. Turkish plain-text:

Ondört Şubat tarih ve yirmidört numerali telgrafta "Türkiye bugün bakim hemen-hemen harbe hazir" nushasindan geçilen "haftalarca sürmesi" nushasina kadar olan gruplar olup daha aşagida "münakaşalar evvelce ve ahirem" nushasindan "safhaya intikal ettirilmiş" nushalarina kadar olan alti grup ricaederim kirkyedi

4. Translation:

I request the (code) groups in your message number twenty-four, dated fourteen February, beginning with the text, "Türkiye bugün bakim hemen-hemen harbe hazir" as far as the text, "haftalarca sürmesi"; and further on, the six groups beginning with "münakaşalar evvelce ve ahirem" up to the text "safhaya intikal ettirilmiş", forty-seven.

SECRET

Doc ID: 6554247

~~SECRET~~

24

ARABIC CODE AND CIPHER PROCESSING

~~SECRET~~

Doc ID: 6554247

~~SECRET~~

ARABIC

FROM : WASHINGTON (IRAQIYAH)

TO : BAGHDAD (KHARIJIYAH)

MSG. NO. : 11

1.

DDCUN CSSGP ZUNCP SSIPN LEXXL HZCJS HWDLU HCVEE XHBMZ NHKEE AHHVP ZEHXL KFBRU

CUZUN NULUW GMMCK CDKAH WXZLE PZWYH ZBFVK HWULH WVLCW VUEHP ZALKX LFIML NLXFX

LNSEM KOHAH LAFHH VSDLF NGHFH HKPZE HXLLX BRFPW ULHAP UZJOK SPZWC ASUPF KPNLX

JSUNB KNGHF HHKWH CLEVM WBUEP EHXCZ LONSF VKHFM FWBRF ZLAOF KSFDC WCASU PAHKU

PVKHW ETMJV UEHFP ZNLKL XFNLE KWCAS UPFKP EXOAW HZCZN LXLCS ONHXV KHSUN BKWNG

HFNHC LEVLW BUEPC VFMLX UHCZL AKFWD FZMDX DLXEN GNCLL NSUBX LEEUN HSEXL WCUNC

SEXJS GZASI PZLUA LKEUN HLSWH YBAPW ULHAP UZJOK SPZWH PGGDH HVCXN EKYBA HLSEL

UJFOH WETMW VUEHF ZCXNE KWCDL KAWSY UHVHF LBSDL DLVKH LVCLK WAFHZ XHHXP

2.

CIPHER: DDC UNC SSG P Z UNC P SSI P NLEXXL HZC SSH WDLUH CV KKX HHM ZNHK EEA HHV P

PLAIN : BRQX/TYNA | RQM | ∧ | W RQM | / | Q>BLN> | YMM | 9 | LT>RY | MS | N>>B | M>SR | WKYL | HAR-JYN | AMY-RKA |

ZEHXL KF BRU CUZU WNULU WCNMC KCDKAH WXZLE P ZWYHZB P VKH WULH WVLC WVUEH

WBYN> | LH | HTR | MRWR | LQR>R | LMQ3M | LMJLSY | LNW>B | W>LSYWM | SLY | LR>Y | LS>M | LSRBY |

ZALKXLF LML NLX FXLN SEXK OH AHLAF HHV SDLF NGHF HHK P ZEHXL LX BRF P WULHA

WS>LN>H | >3> | K>N | HH>K | TBDL | FY | SY>SH | AMY-RKA | TS>H | QBYM | FLS-TYN | WBYN> | >M | HTH | LR>YS |

P UZJOKS P Z WCASU P FK P NLXS JUNB KNGHF HHK WH CL EVM WBUE P EHX CZLONSF

RWZFLT | W >LMSTR | HL | K>NT | TRKH | LQBYM | FLS-TYN | >LY | M> | BSJ | >LHRB | BYN | MW>FQTH |

VKH FMF WBRF ZLAOF KSFDC WCASU P AHKU P VKH WEDM WVUEHF P Z NLK LXF NLEK WCASU

SLY | HBH | >LHTH | M>SFH | LTHJM | >LMSTR | SYLR | SLY | >LBDX | >LSRBYH | W Q>L | >NN | Q>BL | >LMSTR |

FK P EXOA WEZC Z NLXL CSONHX VKH SUN BK WNGHF WH CL EVM WBUE P CV FML XUH

HL | BNFS | >LYNM | W K>N> | MTFQYN | SLY | TRK | HL | LQBYH | >LY | M> | BSJ | >LHRB | MS | HB> | NRY |

CZLAKF WDFZM CX DLXENC NCL LNSUBXL EEUNHSHXL WCUNCSHX SSG Z SSI P Z LUALK

MW>SLH | >LTHWJ | MH | J>NBKM | KM> | >QTRHN> | BBRQYYYN> | >LMRQMTYN | ∧ | W | 1· | W >RS>L |

EUNHLS WH YBA P WULHA P UZJOKS P Z WH P GGD HHV CX NEK YBAHLS KLUJF OH WETM

BRQY>T | >LY | SNS | >LR>YS | RWZFLT | W >LY | HKW-MN | AMRI-KA | MH | QBL | SNSY>T | B>RZH | FY | >LBL>B |

WVUEHF Z CX NEK WCDLKA WSYUHVHF LBSDLDL VKH LVCLK WAFHZXHHX P

>LSRBYH W HM QBL >LMB>LS >LTSRYSYH >HTJ>J> SLY >SM>L >LSHYWHYYN

~~SECRET~~

~~SECRET~~

1. Section one represents message as received.

2. Section two is the same message showing the segregation of code groups (red underscore) from the cipher text. Plain component (orange color) is Arabic plain-text in English script.

3. Transliteration into Arabic script:

برقيتينا رقم ٨ ورقم ١٠ / قابلنا يوم ٩ الجاري مع نائب
مصر وكيل الخارجية الاميركية وبينا له خطر مرور القرار
المقدم لمجلسي النواب والشيوخ على الراي العام العربي
وسألناه اذا كان هناك تبدل في سياسة اميركا تجاه قضية
فلسطين / وبينا ان خطة الرئيس روزفلت والمستر هل
كانت ترك حل قضية فلسطين الى ما بعد الحرب /
بين موافقته على هذه الخطة واصفة لتهجم المستر سيلر
على البلاد العربية / وقال انه قابل المستر هل بنفس
اليوم وكانا متفقين على ترك حل القضية الى ما بعد الحرب
مع هذا نري مواصلة الجهود من جانبكم كما اقترحنا
ببرقيتينا المرقمتين ٨ و ١٠ / وارسال برقيات الى شخ
الرئيس روزفلت والى حكومة الاميركية من قبل

~~SECRET~~

شخصيات بارزة في البلاد العربية ومن قبل المجالس
التشريعية احتجاجاً على اعمال الصهيونيين

4. Translation:

Reference our telegrams No. 8 and No. 10:
On the 9th. instant the Egyptian minister and I called on the United States Undersecretary of State. We explained to him the dangers attached to the passing of the resolution presented to the House of Representatives and the Senate as regards Arab public opinion, and we asked him whether this meant a change in American policy on the Palestine question. We explained that the plan of President Roosevelt and Mr. Hull had been to leave the solution of the Palestine question until after the war. He expressed his agreement with this plan and his regrets at the attack of Mr. Celler on the Arab countries. He said that he had called on Mr. Hull on that very day, and that they had agreed on leaving the solution of the problem until after the war. In spite of this, we think it advisable to pursue the efforts to be made on your part, as we suggested in our telegrams No.. 8 and No. 10, in person; and to despatch telegrams to President Roosevelt and the American Government from prominent personalities in the Arab countries and from legislative assemblies, protesting against the activities of the Zionists.

ARABIC CODE AND CIPHER PROCESSING

Doc ID: 6554247

RESTRICTED

A TYPICAL PROBLEM ROUTED TO THE

SPECIAL EXAMINATION UNIT

A COMBINATION CIPHER AND PLAIN TEXT COMMUNICATION ADDRESSED TO "DEPARTMENT OF MILITARY INTELLIGENCE, WASHINGTON, D. C. " FROM SOMERVILLE, MASSACHUSETTS. SOLUTION READS:

"THERE COMES A TIME IN THE LIFE OF EVERY INTELLIGENT MAN WHEN HE REALIZES HOW DUMB HE IS."

RESTRICTED

SOMERVILLE, MASS.
NOV 22
11—PM
1943

BUY
WAR SAV
BONDS AND S

25

Dept of Military Intelligence
Washington D.C.

new code

4875

The funny qualities of this code
make it extremly difficult
To decipher without the key
with the accompanying translation
Can you reconstruct the key?
or read the following message?

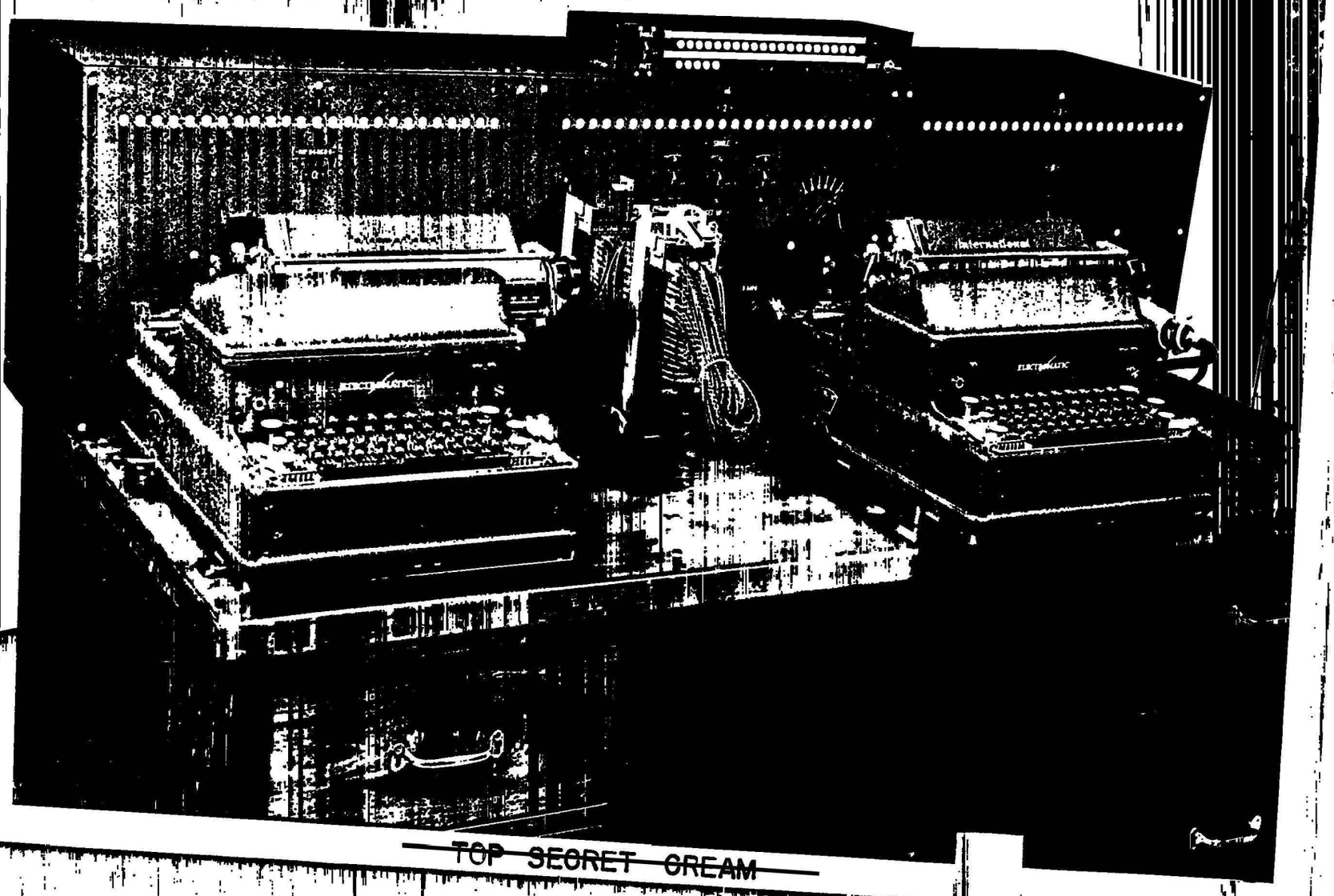
Doc ID: 6554247

TOP SECRET CREAM

ANALOGUE OF THE PURPLE MACHINE

Although the cryptanalysts had never seen the Japanese cipher machine used for secret diplomatic messages, they were able to duplicate the operation of the Japanese machine in the analogue pictured here. The design and construction of the analogue was based on the cryptographic principles established by the cryptanalysts in their solution of the system and carried out by the engineering staff.

TOP SECRET CREAM


International
ELECTROMATIC

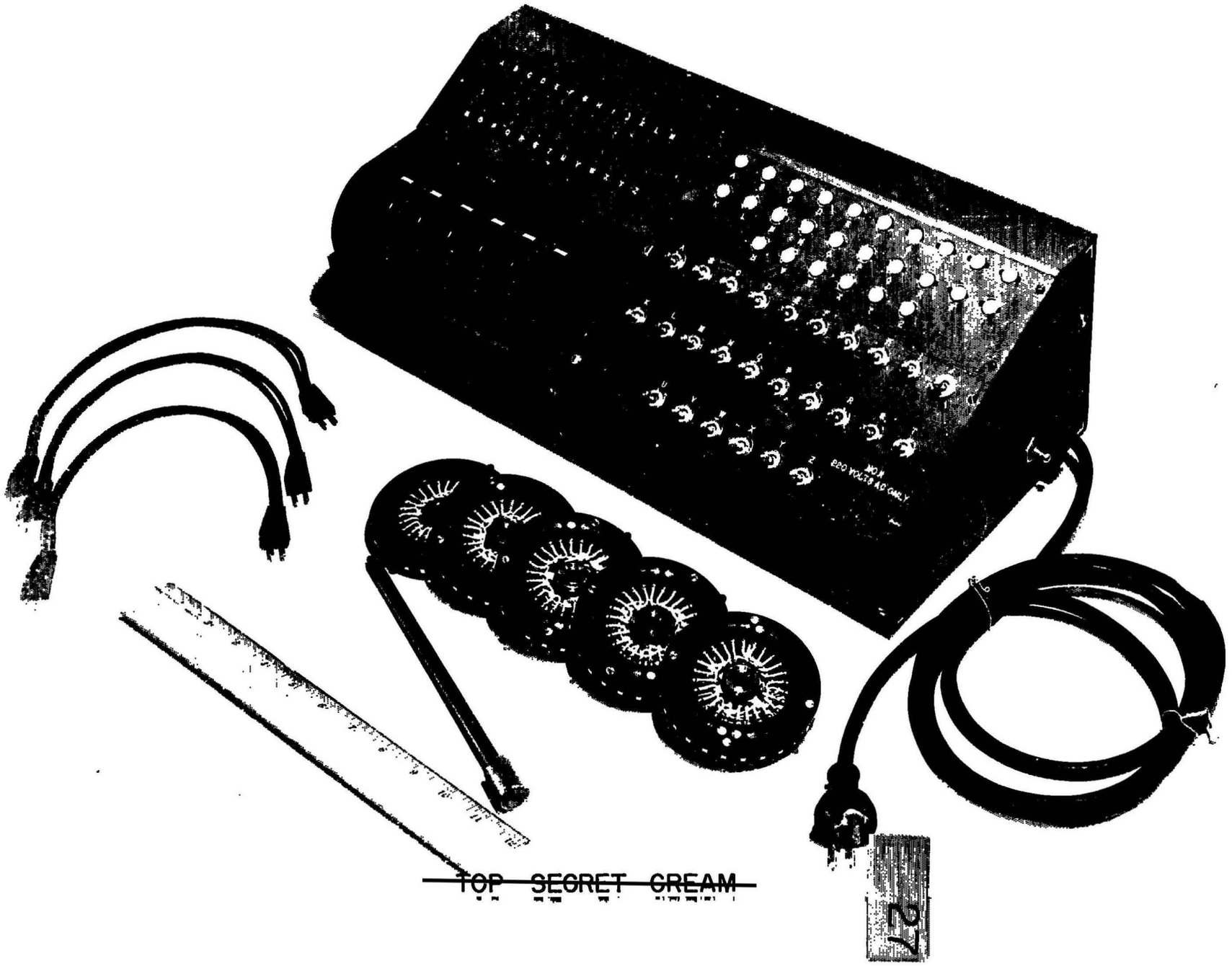
Doc ID: 6554247

TOP SECRET CREAM

ENIGMA REPLICA

This useful gadget for testing further by hand the several likely settings after other methods had eliminated most settings was often called the "Handtester."

TOP SECRET CREAM



Doc ID: 6554247

TOP SECRET CREAM

THE "003"

The Cryptanalytic machine, called for convenience and security the "003" (from the project number X68003), was designed to test rapidly the many assumptions required in the solution activities of messages enciphered by a cipher machine of the Enigma type. The innovation of a relay switching system, a departure from the rotary type of construction usually found in this kind of equipment, provided greater flexibility in the use of the equipment.

TOP SECRET CREAM

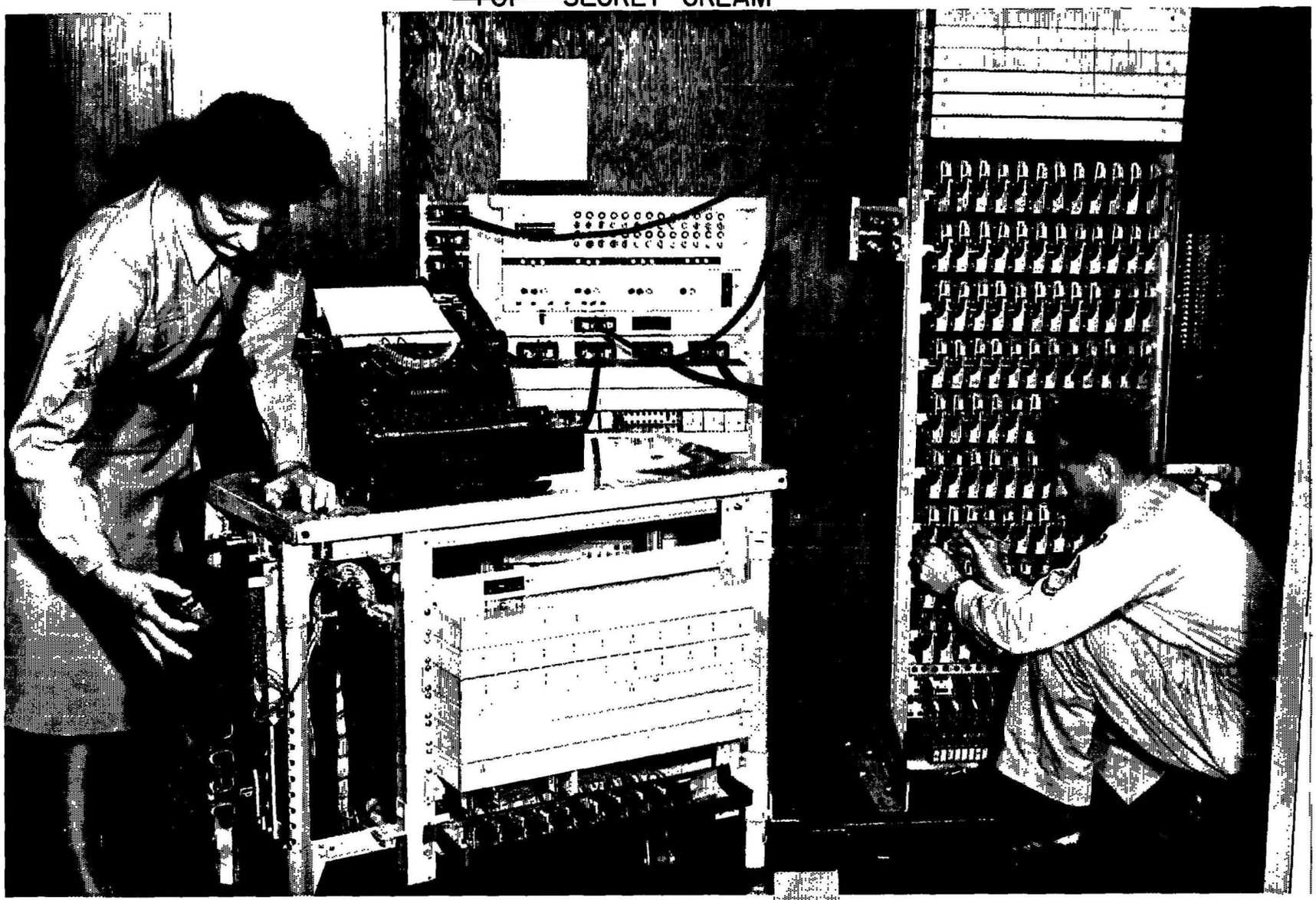
Doc ID: 6554247

TOP SECRET CREAM

THE "ARLINGTON DUDBUSTER"

Designed to speed the solution of a special class of messages with faulty indicators, termed "dud messages" and in conjunction with the 003, the "Dudbuster" piled up a notable record of solutions.

TOP SECRET CREAM



Doc ID: 6554247

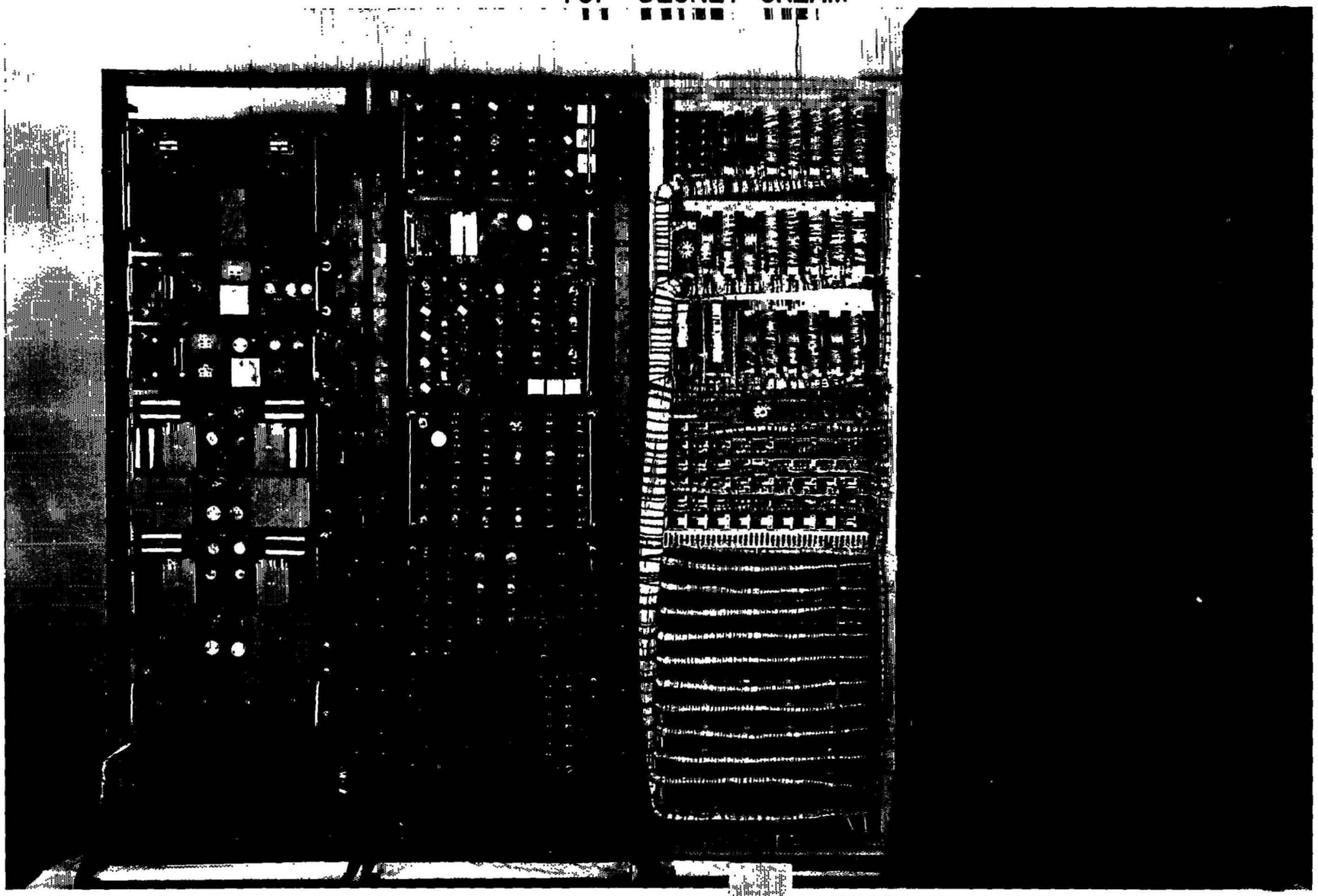
TOP SECRET CREAM

THE "AUTO[illegible]"

VIEWED FROM THE REAR

In order to perform the millions of tests necessary for solution, diverse elements (relays, electronic tubes, selectors, rotors, plugs, and jacks) were combined in an intricate wiring system.

TOP SECRET CREAM



Doc ID: 6554247

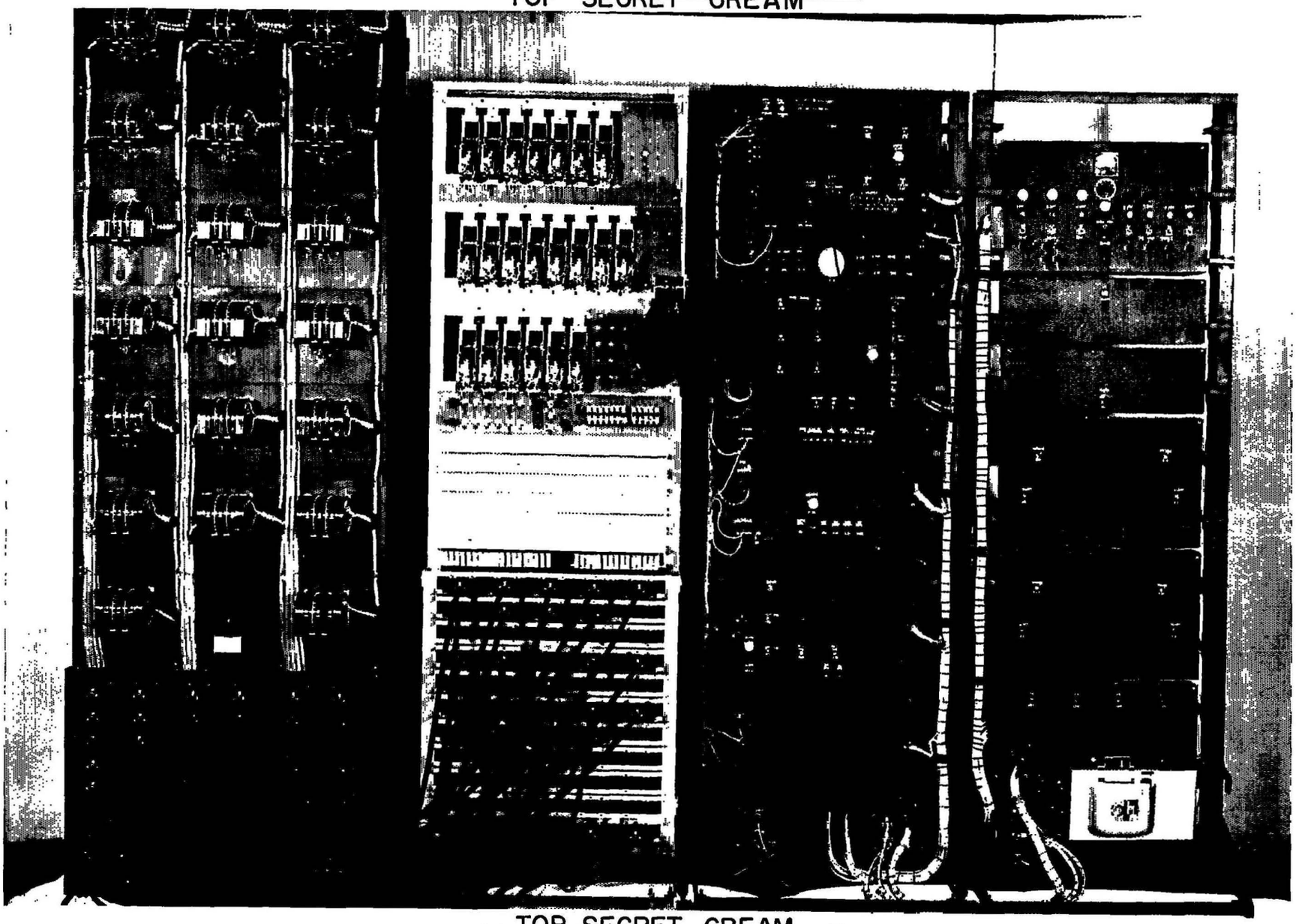
TOP SECRET CREAM

THE "AUTOSCRITCHER"

VIEWED FROM THE FRONT

When changes in systems required new techniques for solution, new machinery was needed to perform tirelessly the new and lengthy processes. The "autoscritcher" was designed to take care of the superhuman task of solution involving pluggable reflectors.

TOP SECRET CREAM



Doc ID: 6554247

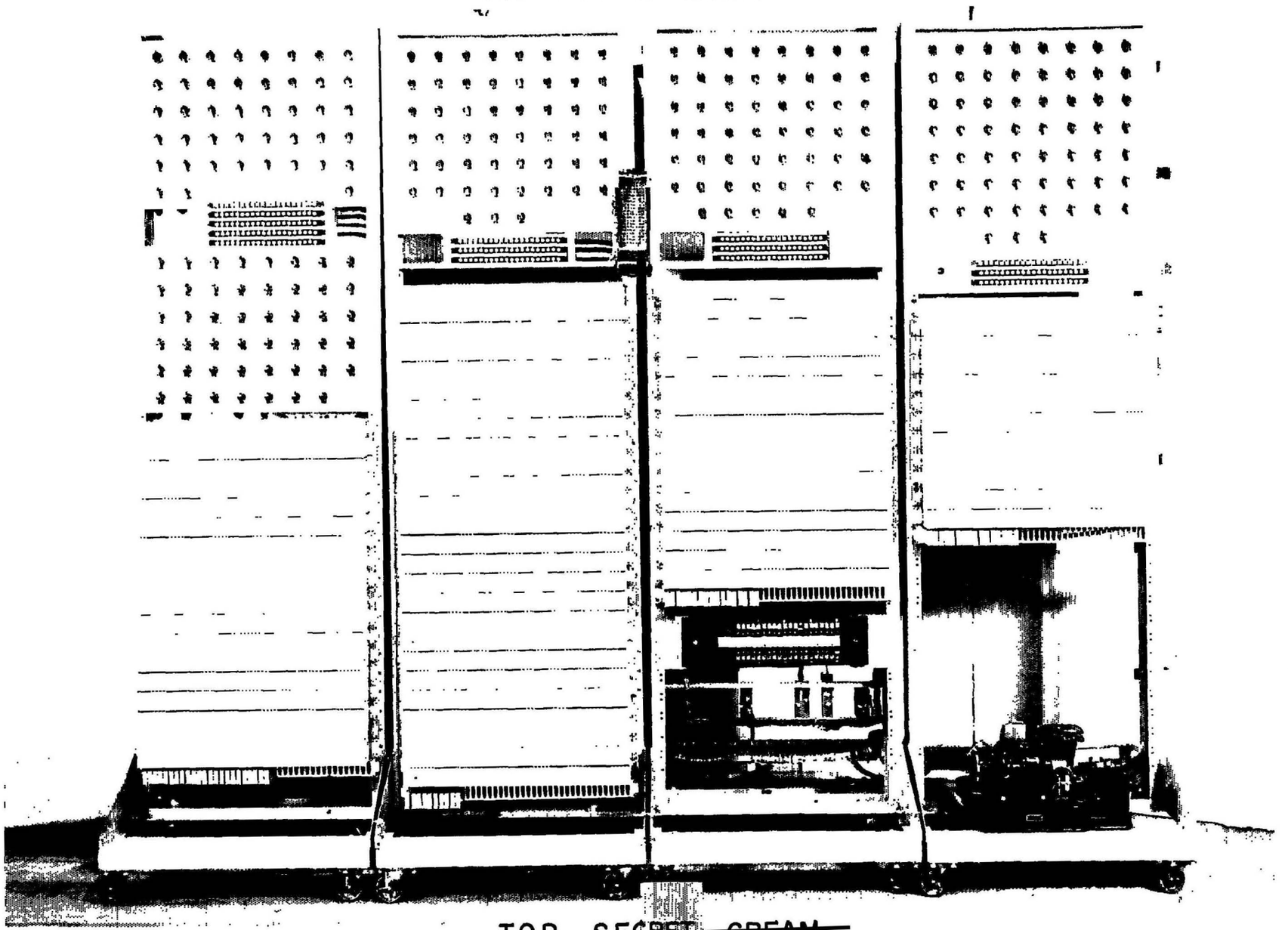
TOP SECRET CREAM

THE DRAGON

Solution of teletypewriter cipher systems was aided by the specially designed RAM equipment, the Dragon, which "dragged" cribs through messages.

TOP SECRET CREAM

TOP SECRET CREAM



TOP SECRET CREAM

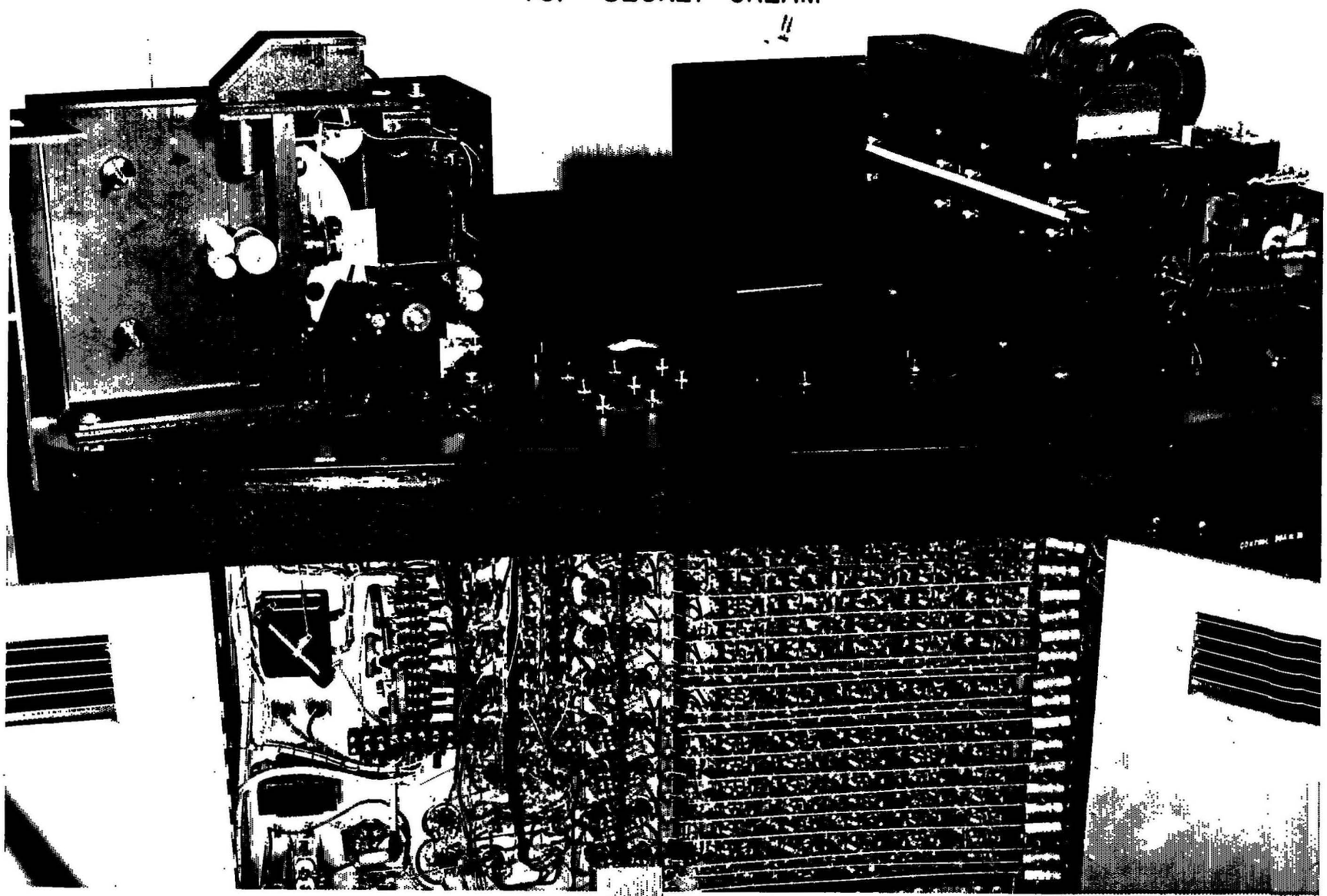
Doc ID: 6554247

TOP SECRET CREAM

THE 5202 CAMERA, TARGET, AND GENERATOR

The high-speed camera of the RAM equipment, the 5202, photographed the sequences of impulses produced by the generator. The speed, the accuracy, the number of characters it records, and the smallness of the space which this record occupies on the film are noteworthy characteristics of the 5202.

TOP SECRET CREAM



Doc ID: 6554247

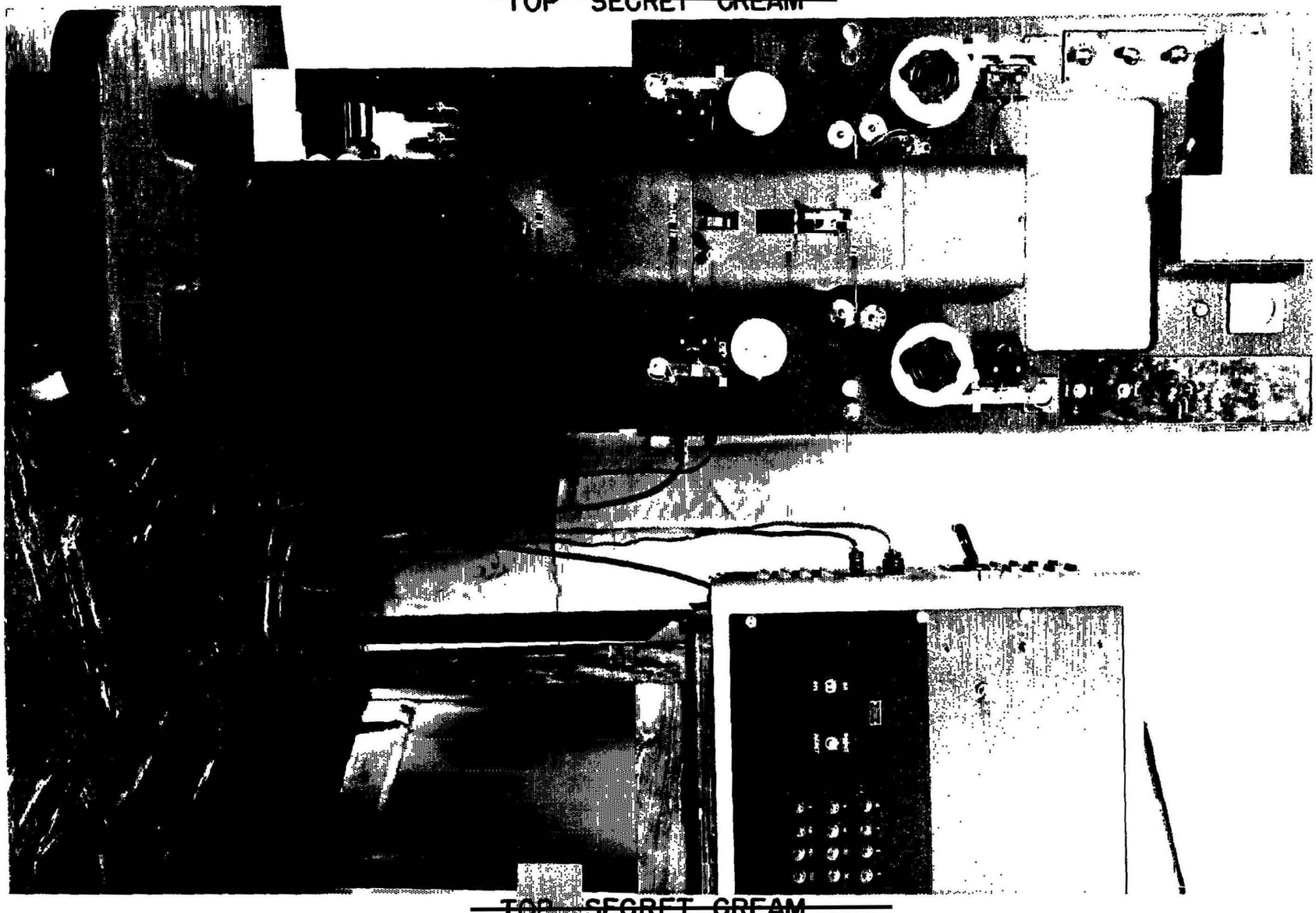
TOP SECRET CREAM

THE 5202 COMPARATOR AND COUNTER

The Comparator measures the coincidence between the texts recorded on film, identifies the juxtaposition where given degrees of coincidence occur, and displays the nature of the coincidence. The Counter, an electronic device, counts the number of coincidences.

TOP SECRET CREAM

Doc ID: 6554247



Doc ID: 6554247

AHA
119