



NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Cases: 44559  
13586  
(formerly J9223-99)  
17 November 2004

Mr. Frode Weierud  
Le Pre Vert, 1041 Rte de Mastegnin  
Prevessin-Moens, F-01280  
FRANCE

Dear Mr. Weierud:

This is an initial response to your Freedom of Information Act (FOIA) request of 28 October 2004, which was received by this office on 2 November 2004, for a copy of the "Catalog of Enigma Cipher Machine Wirings." Your request has been assigned case number 44559. This letter indicates that we have begun to process your request. There is certain information relating to this processing about which the FOIA and applicable Department of Defense (DoD) and NSA/CSS regulations require we inform you.

For purposes of this request and based on the information you provided in your letter, you are considered a representative of the media. Unless you qualify for a fee waiver or reduction, you must pay for duplication in excess of the first 100 pages. Your request for a waiver of fees has been granted.

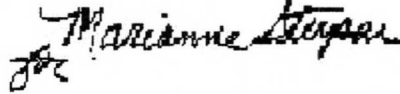
We have completed our search for records responsive to your request. The material responsive to your request is not voluminous or complex, and your request has been placed in the first-in, first-out processing queue for simple cases. Because there are several cases ahead of yours in that queue, however, we are unable to respond to your request within 20 days. We appreciate your patience with our efforts to treat all requesters fairly by responding to each on a "first-in, first-out" basis.

We have received your letter dated 21 October 2004 inquiring about the status of another FOIA case of yours (J9223-99) that is pending with this Agency. Due to an upgrade in our processing system, we have assigned a new case number to that request, FOIA Case 13586. Please be advised, FOIA case 13586 is currently being worked and near completion. Once processing has been completed, we will notify you of our final response.

FOIA Cases: 44559  
13586  
(formerly J9223-99)

Correspondence related to either of these requests should include the case number assigned to the request, both of which are included above. Your letter should be addressed to National Security Agency, FOIA Office (DC34), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248.

Sincerely,

A handwritten signature in black ink, appearing to read "Pamela N. Phillips". The signature is written in a cursive style and is positioned above the typed name.

PAMELA N. PHILLIPS  
Chief  
FOIA/PA Office



**NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE**  
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 44559A  
26 September 2007

Mr. Frode Weierud  
Le Pre Vert  
1041 Rte de Mategnin  
F-01280 Prevessin-Moens  
FRANCE

Dear Mr. Weierud:

This responds to your Freedom of Information Act (FOIA) request of 28 October 2004, which was received by this office on 2 November 2004, for a copy of the National Security Agency document entitled "Catalog of Enigma Cipher Machine Wirings," Control Number 182-4, June 1954. A copy of your request is enclosed. For purposes of this request, and based upon information you previously provided, you are considered a representative of the media. Additionally, you previously requested, and were granted, a fee waiver. There are no assessable fees associated with this request. Your request has been processed under the FOIA, and the document you requested is enclosed. Certain information, however, has been deleted from the enclosure.

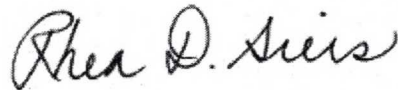
Some of the information deleted from the document was found to be currently and properly classified in accordance with Executive Order 12958, as amended. This information meets the criteria for classification as set forth in Subparagraphs (b), (c), and (g) of Section 1.4 and remains classified TOP SECRET as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. The information is exempt from automatic declassification in accordance with Section 3.3(b)(1, 3, and 6) of E.O. 12958, as amended. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in this document. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 403-1(i); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

Since these deletions may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days from the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJ4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Please be advised that the document appears to be missing some pages. This is because the blank pages in the document were removed. No information was on those pages.

Sincerely,

A handwritten signature in cursive script that reads "Rhea D. Siers".

RHEA D. SIERS  
Deputy Associate Director for Policy

Encls:  
a/s

NATIONAL SECURITY AGENCY  
Washington 25, D. C.

~~TOP SECRET FROTH~~

CATALOG OF ENIGMA CIPHER MACHINE WIRINGS

Compiled by

Astrid Hammarborg

THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18, U.S.C., SECTIONS 793, 794, AND 798, THE TRANSMISSION OR REVELATION OF WHICH IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW.

June 1954

TECHNICAL INFORMATION DIVISION  
Bibliographic Research Branch

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 1 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~INTRODUCTION

By means of the following report, it is intended to bring together under one cover the available Enigma cipher machine wirings used prior to 1946. As one of the principal targets of the combined Anglo-American cryptanalytic effort during World War II, the German Enigma machine was the basis for a considerable number of reports. These have been searched for pertinent material. The record of Enigma wirings is complex and varied due to the use of this machine by many countries in one of its basic forms, or with alterations and innovations. Included in this paper are rotor wirings given by the British, the U.S. Navy, Coast Guard, and Army. Some of these wirings are clearly and explicitly presented; others are briefly noted; many have been taken from work sheets, and bits of scattered, unassociated papers wholly intelligible only to their originators; some exist without accompaniment of explanatory data. Wirings and the machines to which they pertain will be discussed briefly under separate headings insofar as data is available.

Suggestions, critical comments, and additional sources of Enigma information are welcomed from readers for use in subsequent editions of this paper.

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 3 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

TABLE OF CONTENTS

	<u>Page</u>
I. BACKGROUND OF THE ENIGMA . . . . .	7
II. PROGRESSIVE CHANGES IN GERMAN ENIGMA . . . . .	27
III. OUTLINE OF ENIGMA MACHINES . . . . .	31
IV. ENIGMA WIRINGS . . . . .	39
<u>A. Unsteckered Enigmas . . . . .</u>	<u>39</u>
Commercial Enigma . . . . .	41
A (Old Commercial) . . . . .	42
Swiss Enigmas. . . . .	45
Commercial Enigma (A-827). . . . .	68
Enigma Cipher Machine (A-837). . . . .	70
A-1214 . . . . .	72
Standard Army "A" (Machine No. A-15465). . . . .	74
"Delta" Enigma Machine (A-16081) . . . . .	76
"Alpha" Enigma Machine (A-16749) . . . . .	78
"S" Enigma (A-17245 S) . . . . .	80
Commercial Enigma (Model D). . . . .	82
K Enigma (K-234) . . . . .	84
Italian Enigmas. . . . .	86
Spanish Enigmas. . . . .	90
Croatian Enigma. . . . .	96
Canary Islands Enigma. . . . .	98
GGG (3-G). . . . .	100
4-Jig Enigma (4-J) . . . . .	102
Rocket . . . . .	104
S. D. Commercial . . . . .	106
Rumanian Enigma. . . . .	108
<u>Tirpitz (T) Enigma . . . . .</u>	<u>110</u>
Early German 3-wheel Enigma. . . . .	116
Zaehlwerk (CA-15). . . . .	118
Group II Enigma. . . . .	120
ORANGE Enigma. . . . .	126
GREEN Enigmas. . . . .	129
RED Enigmas. . . . .	136
KK (German Armistice Commission Enigma). . . . .	146
KK Enigma (Revised Group II) . . . . .	146
G-208 Enigma . . . . .	150
G-260 Enigma . . . . .	152
KD (New ISK unsteckered Enigma). . . . .	156
Railway Enigma . . . . .	158

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 5 of 239 Pages

~~TOP SECRET FROTH~~

	<u>Page</u>
IV. ENIGMA WIRINGS (continued)	
<u>B.</u> Steckered Enigmas. . . . .	161
German Service Enigmas. . . . .	163
Yellow Enigma . . . . .	178
<u>C.</u> Miscellaneous Enigmas. . . . .	181
4-I Enigma. . . . .	183
Czechoslovakian Enigma. . . . .	184
Enigma (unidentified) . . . . .	186
V. APPENDICES. . . . .	193
<u>A.</u> Enigma Machines in Foreign Countries. Berlin, 13 Sep 1943. (TICOM/DF-190AM) . . . . .	195
<u>B.</u> Further Interrogation of R. R. Dr. Huettenhain and SDF. Dr. Fricke of OKW/CHI. TICOM, 4 Sep 1945. (TICOM/I-84). . . . .	197
<u>C.</u> Report on Berlin Targets by Major Heller of G.S.I.(S), 21.A.G. B.O.A.R. TICOM, 17 Sep 1945. (TICOM/I-104)	199
<u>D.</u> Manufacture of Enigma Machines by Heimsoeth and Rinke, Berlin. TICOM, 17 Nov 1945. (TICOM/M-13)	203
VI. LIST OF SOURCES . . . . .	209
VII. WIRING-SEQUENCE INDEX . . . . .	219
VIII. MACHINE INDEX . . . . .	233

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 6 of 239 Pages



~~TOP SECRET FROTH~~

I. BACKGROUND OF THE ENIGMA

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 7 of 239 Pages

I. BACKGROUND OF THE ENIGMA

The Enigma cipher machine was the backbone of German high-level military cryptography. Its most outstanding performance was exhibited during World War II when a series of variations and ingenious innovations made it the leading target of Allied cryptanalysis. From its first appearance in the mid-1920's to the end of the War, it went through the following forms:

1. The O-Bar Machine, used by the German Fleet.
2. The Commercial or K Enigma, used by German commercial firms, the Post Office, the railways, and other miscellaneous German governmental agencies.
3. The Counter (Zahlwerk) Enigma, also referred to as the "G" and "Abwehr", used by Military Intelligence (Abwehr), by the Reich Security Office (Reichssicherheitshauptamt), and by military attaches.
4. The plugboard (Stecker) Enigma, used by the Supreme Command of the Armed Forces (OKW); the High Command of the Army, and in Army communications down through division; by the High Command of the Air Force, and in Air Force communications, down through group and sometimes squadron.
5. The plugboard Enigma (Schlüssel M), employing an additional rotor, used by the High Command of the Navy, and in

TOP SECRET CONTROL NO. 132-4

Copy 4 of 30 CopiesPage 9 of 239 Pages

~~TOP SECRET FROTH~~

Page 10

BACKGROUND OF THE ENIGMA

Naval communications, including the submarine arm.

6. The plugboard Enigma with pluggable reflector D (Stecker mit Umkehrwalze D), used by the Air Force and proposed for the other Services.
7. The plugboard Enigma with Stecker Uhr, introduced by the German Air Force. This device was a security feature by which the stecker of individual messages on the same key could be varied.
8. The plugboard Enigma with variable notch rotors (Lueckenfuellerwalzen), proposed for the Supreme Command Armed Forces, Navy, and Air Force.
9. Cipher Device 39 (Schluesselgeraet 39), proposed for the Supreme Command Armed Forces, and the Army, Navy, and Air Force.

The last two machines do not enter into the period covered by this report. The variable notch rotors had not been distributed for general use and Cipher Device 39 was still in the development stage when the war ended.

The plugboard Enigma is contained in a wooden box about a foot square and six inches deep. When set up for use, it contains three wheels mounted between the endplate and reflector. It has a keyboard with 26 keys, labelled with the letters of the alphabet; a lampboard with 26 bulbs that shine through stencils on which the letters are marked; a stecker board; battery and switch. The lid of the box con-

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 10 of 239 Pages

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

BACKGROUND OF THE ENIGMA

Page 11

tains spare lamps, plugs, etc., and the whole is fitted with a handle for carrying. When a key is depressed, one or more of the wheels rotate one position and a current flows through the machine to one of the lamps. The letter appearing over the lamp is the enciphered result of the depressed key. The endplate is a ring of 26 terminals called entry points. In the unsteckered Enigma these are connected directly to the keys; in the steckered Enigma they are connected to the keys through the stecker board.

The stecker board has 26 pairs of sockets labelled with the letters of the alphabet, one from each pair leading to a corresponding key on the keyboard, the other to the endplate. This plate, if viewed from the side of the wheels and taken in anticlockwise order, is connected to the stecker board sockets in ABCD...Z order, this order being called the diagonal of the machine. Normally, the two sockets of a pair are connected together by a hidden spring. If a stecker is plugged into two pairs of sockets, say A and B, these springs are forced away, and the A key is connected to the endplate at a position which would otherwise be connected to the B key and vice versa. That A and B are connected by such a plug is expressed in the form A/B, or B/A. The effect of the stecker on the encipherment is as follows: if, at a position of the machine, A enciphers as R when there is no stecker, then at the same position with stecker A/B, R/X and perhaps others, B enciphers as X. A letter which is not steckered to another one is said to be self-steckered.

TOP SECRET CONTROL NO. 182-4  
 Copy 4 of 30 Copies  
 Page 11 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

A wheel has 26 terminals on its right face (as it sits in the machine) and on its left face 26 plate terminals. The plates are connected across by wires to the pins in random order. On the right side is a ratchet wheel and a large sprocket; on the left side is a metal ring, which can move freely relative to the wiring. This ring carries the letters A to Z (or the numbers 1 to 26) in order round its circumference, and is provided with one or two turnover notches on its extreme left edge. It can be held in any one of the 26 positions by a clip, the setting of which is called the ring setting.

The German Army and Air Force used five wheels, numbered I to V, each having one turnover notch in a position which varied from wheel to wheel. The Navy used three additional wheels, VI, VII, and VIII, each having two turnover notches at points diametrically opposite each other on the ring in the same positions on each of the wheels. When inserted in the machine, the wheels are mounted on an axle and the sprockets are held by pawls in the casing of the machine. Any three of the wheels in any order may be in the machine at a given time, and these are referred to as the right-hand, middle, and left-hand wheels. Parts of the sockets project through the casing of the machine, enabling each wheel to be rotated by hand and set to any one of the 26 positions. The position of the wheels is described by the letters on the rings which show through three windows in the casing of the machine; the sequence of the three letters which show are called the window position. The pins of each wheel are in contact

TOP SECRET CONTROL NO. 182-4  
 Copy 4 of 30 Copies  
 Page 12 of 239 Pages

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~BACKGROUND OF THE ENIGMA

Page 13

with the plates to the right of the wheel, or, in the case of the right-hand wheel, with the endplate. The reflector has only 26 pins which are connected in pairs and are in contact with the plates of the left-hand wheel. Unlike the wheels, the reflector is not rotatable in the steckered Enigma.

The O-Bar Enigma came into use in the early 1920's. It had three wheels and no stecker, and the curious characteristic of 29 letters on its keyboard. Of these 29 letters, X always enciphered itself without the current entering the machine, and the 28 letters were enciphered in the normal manner. The rings of the wheels had 28 letters printed on them; curiously, the o-umlaut had been omitted and from this fact the machine derived its name. It was solved by Polish cryptanalysts and all traffic was read. The German Fleet discontinued its use in 1931 when it was superseded gradually by the "Schluessel M" or Navy plugboard Enigma.

The plugboard Enigma was the standard Service machine used by the Army, Air Force, and Navy. The Germans first used this machine with three wheels and six steckers. The reflector belonging to it was the "A" or "Anton". Having obtained photographs of the keys for three months, during which period the wheel-order remained unchanged, the Poles reconstructed the wiring of wheels 1, 2, and 3. Originally, three wheels, having one notch per wheel, were chosen from a set of five. Later, under German naval procedure, three wheels were chosen from a set of eight, five of which had one notch per wheel and three,

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 13 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

Page 14

BACKGROUND OF THE ENIGMA

two notches per wheel. The reflector went through changes from the "A" to the "B" and "C". The "C" was used for a few weeks only in 1940 on one Norwegian air frequency.

The old "B" reflector, which replaced the "A" in the summer of 1937, was abandoned by the Navy and a new "B", half its size, plus an additional wheel (Zusatzwalze) - the number 9 Delta or Beta wheel - were introduced 1 February 1942, making the Navy machine a four-wheel Enigma. The Beta wheel was so wired that when set at the letter A, the combination of it and the new "B" reflector would give an effect equivalent to that of the old "B" reflector, thus enabling holders of the four-wheel machine to continue communicating with holders of the three-wheel machines. On 1 July 1943, a tenth wheel, the Gamma wheel, was introduced. When this wheel was set at the letter A and combined with the new "B" reflector, the effect of the "C" reflector was produced. These last two additional wheels had no notches and were used interchangeably in the fourth wheel position. Subsequently, about 1 January 1944, the Air Force introduced the pluggable reflector "D" which caused considerable difficulties for Allied cryptanalysts. This form of the machine as employed by the Air Force used three one-notched wheels from a set of five. The plugging of the reflector formed part of the key and changed at first three times and later four times a month. At least two Army keys used the "D" reflector with a daily changing plugging, and it seems probable that it was introduced on one of them in 1943. The pluggable reflector was not used by the Navy.

TOP SECRET CONTROL NO. 182-4

Copy 4 of 30 CopiesPage 14 of 239 Pages~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

---

BACKGROUND OF THE ENIGMA

---

Page 15

Still another version of the plugboard Enigma was proposed, using three from a set of five multiple- and variable-notched wheels called the Lueckenfuellerwalzen.<sup>1</sup> The reflector in this machine was a pluggable or non-pluggable fixed plate, as desired. These changes introduced an aspect of unpredictability in key change.

During the 1930's various patents were issued to German inventors for Enigma machines manufactured for sale in Germany and other countries. These machines were used mostly by German commercial firms for sending business instructions to their agents in other countries and could be bought freely on the open market. The Commercial or K Enigma was sold openly until about 1934. It was used in various versions by the Croatian puppet government, the Spaniards, Italians, the Swiss, and, of course, by the Germans themselves. It had three single-notched wheels, a settable reflector, and a fixed input. Many countries rewired the wheels for greater security. After the Nazis acceded to power the machine was withdrawn from the market.

The years 1936 to 1939 cover the period of the Spanish Civil War. When it started, the A Commercial Enigma, an unsteckered machine, was already in existence. A serial number accompanied the A on these machines. They were so marked by their manufacturer, Heimsoeth and Rinke of Berlin. If no letter followed this serial number the machine

---

1. The compiler tested a set of captured Lueckenfuellerwalzen (in the NSA Museum) for wiring; it was learned that these rotors had the same wiring as the standard military machine.

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 15 of 239 Pages

~~TOP SECRET FROTH~~



~~TOP SECRET FROTH~~

Page 16

BACKGROUND OF THE ENIGMA

was usually a standard Army model used by the German Army, the Schutzstaffel, and the German Air Force. If a Greek letter "Alpha" or "Delta" followed the serial number (e.g., A-246176a) the machine was a standard model returned to its manufacturer for special rewiring. The purpose or destination of these machines has not been determined.

The Italian "K" Naval Enigma was an improved version of the "A" Commercial. It differed from the "A" in that the notch on each of its three wheels was attached to the ring of the wheel instead of to the wheel itself. It was used by the Spaniards during the Spanish Civil War and by the Italians for naval communications between Rome and the Italian colonies. In this capacity it was called by the British the "Italian K" or the "K Italian Naval Enigma".

During the summer of 1937 the German Intelligence Service and its subsection, the Security Service, referred to respectively as "Abwehr"<sup>2</sup> and "Sicherheitsdienst"<sup>3</sup>, were sending secret agent traffic from Germany on various networks throughout Europe. This traffic was being intercepted by the British at GC&CS. Mr. Knox of GC&CS is credited with having been the first to solve messages from this traffic and with the setting up of a section for the purpose of continued cryptanalytic attack on the system. This unit was called the "Illicit Series Knox

- 
- 2. Amt, Auslandsnachrichten and Abwehr or "AAA", (headed by General Canaris) a part of Hitler's Oberkommando der Wehrmacht (OKW), the Military High Command responsible for coordinating and controlling the Army, Air Force, and Navy in the general conduct of the war.
  - 3. The Sicherheitsdienst (SD) headed by Himmler; the principal intelligence organization of the German Nazi Party.

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 16 of 239 Pages

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~BACKGROUND OF THE ENIGMA

Page 17

Section", thenceforth referred to as ISK. Since the Italian and Spanish traffic, discussed in the previous paragraph, presented the same kind of cryptanalytic problem as the messages coming from Germany, though entirely unrelated, ISK also took this traffic under surveillance, and during the Spanish Civil War solved the Italian K Enigma. By this time, the reflector known as "Anton" had been changed in the standard Service machine to "Bruno".

From the earliest days of World War II (1939-1945) Berlin maintained an extensive network with the main Balkan cities - Vienna, Belgrade, Bucharest, and the whole of eastern occupied Europe as far afield as Salonika and Warsaw. Previously, messages already solved by the British and identified as coming from the Abwehr had been enciphered in a non-machine system. Suddenly towards the end of 1939, Enigma traffic, related to these earlier messages, began to appear on a Berlin to Madrid net and consequently was recognized as also coming from the Abwehr. This traffic involved many keys. Abwehr agents also appeared in Turkey during the early part of the war. They sent numerous messages to the Balkans and to Berlin; throughout the war the Abwehr kept up extensive communications with Madrid and Lisbon.<sup>4</sup>

At the end of the Spanish Civil War, the Spanish used their K

- 
4. It was during 1939 that Cipher Device 39 (Schlüsselgerät 39) was proposed for the Supreme Command Armed Forces, Army, Navy, and Air Force. But there were so many alterations and time difficulties involved in getting this machine under way that it actually never left the development stage.

TOP SECRET CONTROL NO. 182-4  
 Copy 4 of 30 Copies  
 Page 17 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

Page 18

BACKGROUND OF THE ENIGMA

Enigma for communications with the Naval attache and the Italians sent theirs to stations in the colonies - Asmara, Rhodes, Tripoli, Bengazi, Leros, and Tobruk. The Enigma referred to by the British as "Italian Naval II" was used for this new Italian traffic and ISK began work on it in April 1940. During this year also, the British recovered the "C" (Caesar) reflector used in the Naval Enigma. This reflector was never used with Army or Air Force keys.

The Abwehr at this time was using ten steckers and eight wheels. In the course of World War II, it and the Sicherheitsdienst used nine different Enigma machines.<sup>5</sup> In May 1941 they introduced the Canary Islands Enigma for messages passing between Cisneros and Paris. ISK began attacking these. By December Abwehr traffic had reached a high peak, enabling such good cryptanalytic attack that from then on to the end of the war most of the important Enigma traffic sent by the Abwehr and Sicherheitsdienst was read consistently. Towards the end of the war, an important network of mobile Abwehr units appeared in France and the Low Countries. This network used a key of its own and the decrypted messages provided one of the most important sources of cribs for attack on other Abwehr Enigma systems.

On December 7 1941 (Pearl Harbor Day), the A-837, an old model three-wheel lampboard Enigma, was seized by the U.S. Treasury Department on the premises of CHEMNYCO in New York. It was thought that the

5. These were the Group II, GGG, KK, GREEN South American, Canary Islands, SD, RED South American, KD, and the Service Enigmas.

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 18 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~BACKGROUND OF THE ENIGMA

Page 19

German censor used this machine and that it probably was the only one employed by German firms throughout the world. On the 25th of this month the first ISK key (Balkan or "B") was solved. The control station for this key was at Berlin and the network included all the principal Balkan cities - Vienna, Bucharest, Zagreb, Sofia, Athens, and Salonika.

Towards the end of 1941 Abwehr and Sicherheitsdienst cipher messages began passing between certain stations in the Gibraltar area using the "GGG" or "3 G" commercial type three-wheel Enigma. This machine was solved by ISK in February 1942. About the same date the Naval Service Enigma became a four-wheel machine by splitting its old reflector into a "Bruno" reflector and a "Beta" Zusatzwalze.

By 1 June 1942 a new wheel had been introduced in the Italian Naval II Enigma. In July, American analysts in the Signal Security Service became aware of the ORANGE Enigma used by the Abwehr and Sicherheitsdienst on a special German diplomatic net operated and controlled by the "Auslands Organisation" which was concerned with German persons living abroad. This was a multi-turnover Enigma with a rotating reflector and without a stecker. It differed from the Commercial machine in the wiring of its wheels and in their motion.

In August of the same year the Swiss Enigma (U.S. cover name: INDIGO), a commercial model with special wiring of its rotors and with its turnover mechanism on the ring, underwent the first of four periodic changes in cipher wheels. Then in October, the KK Enigma was

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 19 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

Page 20

BACKGROUND OF THE ENIGMA

captured in North Africa. It was described by the U.S. Army Signal Corps as a revised version of the 11-15-17-notch Group II Enigma, with three wheels and a rotatable reflector and was used by the German Armistice Commission in French Africa. On the tenth of this month the 3-K (GREEN) Enigma, a multiple-notch machine, was first heard on a European station in Cologne. It was believed to be linked with a station in South America. There was also an alternate control from Bordeaux. This machine was solved by the British in December. At this time also, messages transmitted between the Spanish Military Attache in Berlin and Army Headquarters in Madrid were being analysed by ISK. It was assumed that since the Naval Attache used a Commercial machine, the Military Attache would do likewise, although it was certain that the two differed in wiring. About this time, the "Counter" or Zählwerk Enigma came into the picture. It was so named from the fact that it had a letter counter in its mechanism. This machine introduced multiple-notch wheels. Approximately 100 of this model were made. They were first issued to German military attaches.

In February 1943 the U.S. Coast Guard solved the 3-K (GREEN) Enigma independently of the British. On 7 April the Swiss (SZD) INDIGO Enigma underwent its second change in wheel wirings. In May the Canary Islands Enigma was solved by the British and was established as a single-turnover, unstackered type machine used by the Abwehr and Sicherheitsdienst for maintaining a weather- and ship-reporting service between Berlin and the Canary Islands. In the summer of the same year,

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 20 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~BACKGROUND OF THE ENIGMA

Page 21

interest was revived in the German diplomatic ORANGE Enigma; July brought forth in the Service Enigma alternate wheels for the reflector and Zusatzwalze. The Caesar and Gamma wheels were solved by the British in mid-July. Later they learned these had already been captured some time previously in North Africa, but had not been sent on to GC&CS. In July, too, British solution of the Italian Naval II Enigma, and the wiring for the INDIGO were obtained.

Until the end of July 1943 the only Enigma messages sent by the Sicherheitsdienst were passed from Pskov and Smolensk to Berlin. On the 27th however, a cipher link was discovered between Rome and Berlin. The machine used by the Sicherheitsdienst was called the "SD Commercial". It was solved by the British in August.

It was during 1943 that the Counter Enigma was withdrawn from the Military Attache service and issued to Military Intelligence (Abwehr). Some were also sold to the Dutch government. In October, American analysts received the April-September keys for the ORANGE Enigma from the British. It was suggested that GGG holders were possibly using the standard Group II machine. November 4th brought mention of a RED (Rot) machine on the 3-N circuit. This was a multiple-notch Enigma using the old Commercial reflector. It was similar to the GREEN machine and was used by the Abwehr and Sicherheitsdienst for communications to South America. By 12 November the first solution of the German diplomatic ORANGE system was effected, and on the same day the British solved the Spanish Military Attache Enigma. It had been used for communications

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 21 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

Page 22

BACKGROUND OF THE ENIGMA

between Madrid, Berlin, Rome, Vichy, and Berne.

On December 1943 a machine using RED Enigma wheels and GREEN Enigma reflector was discovered through superenciphered instructions sent from Berlin to Argentina. It appeared that a Kryha machine previously used for communications between these two cities was wearing out, and was to be replaced by the RED Enigma. Confusion reigned. Messages were sent back and forth on BLUE, GREEN, and RED keys. The BLUE key was never solved. The Argentine station revealed in a complaint to Berlin that its machine, the G-208 Enigma<sup>6</sup>, could not decipher the Berlin messages. Finally, Berlin admitted having made an error by using wheels from two different machines, and the combined RED and GREEN Enigma was originated. It was apparently used later by the 4-O component of the Sicherheitsdienst and as such was solved by the U.S. Coast Guard. The British solved the South American RED Enigma in January 1944.

From 1 January to October 1944 the third periodic change occurred in the wiring of the Swiss (SZD) cipher wheels, and in February the cipher link between Rome and Berlin using the SD Commercial changed its cipher system. Thenceforth the Enigma was steckered. Both the Italian service and the Eastern Sicherheitsdienst machine service died early in 1944 at which time the Sicherheitsdienst organization in Turkey began using the Commercial machine. In March, the U.S. Coast

6. A wheel marked G-208 was sold with a machine sent to the Dutch State with the consent of OKW.

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 22 of 239 Pages

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

BACKGROUND OF THE ENIGMA

Guard solved the RED (3-N or 3-Nan) Enigma independently of the British. In July the Germans introduced the Enigma Uhr, which was confined to only a few Air Force keys. This device took Allied cryptanalysts completely by surprise, and it was not until after the war that a model was captured. Solution and reconstruction of the machine were obtained from theoretical study within a few days after its introduction. [During the summer a number of "T" or Tirpitz Enigmas, produced by the Germans for the Japanese, were captured in a warehouse in Normandy. In August the Americans raided the port at Lorient in Brittany, France and carried away 60 of these machines. These were similar to the old three-wheel, movable reflector Commercial model, but had a different input sequence, and eight wheels from which three were chosen at a time. In December the principal Enigma used by the Abwehr for European communications - the Group II - was solved by the British. On December third, the KD Enigma was introduced on the Berlin-Madrid-Lisbon network as a Group II replacement for the last part of the German phase of the war. This Enigma used a pluggable "D" (Dora) reflector, had nine notches per wheel and identical turnover pattern for all wheels. Six wheels were recovered, and the machine was solved by the British on 28 January 1945. Near the end of the war the German Air Force made use of a pluggable reflector.

On 1 February 1945 the Swiss made a fourth routine change in the wiring of the SZD cipher wheels. On 20 February and 25 March the

Rumanian Air Force (PINE) and antiaircraft (ASH) traffic, respectively,  
 TOP SECRET CONTROL NO. 182-4  
 Copy 4 of 30 Copies  
 Page 23 of 239 Pages



~~TOP SECRET FROTH~~~~TOP SECRET FROTH~~

Page 24

BACKGROUND OF THE ENIGMA

began coming in. The Rumanian Enigma differed from the German Enigma only in the use of a new reflector. During April the equivalent wiring for three wheels of the Swiss (SZD) Enigma was recovered. On the 29th, the A-1214 was captured by U.S. Naval Officers at Brescia in Northern Italy, and sent to Washington for study. It was the old commercial type, its three wheels having Enigma motion and its reflector settable by hand. The wheels, however, had a new set of wirings and were notched the same as the 4-J Coast Guard wheels though for differently numbered wheels.

On 6 May 1945 Germany surrendered to the Allies. In July the TICOM Unit at the Signal Security Agency furnished the wirings for the A-16081 or "Delta" Enigma, used by the German Attache at Zagreb. This was a standard Army Enigma wired for special use. On 3 July the U.S. Military Attache in Buenos Aires reported on the G-260 Enigma, captured by the Argentine Police in a raid on German headquarters.

In September 1945 Japan surrendered to the Allies.

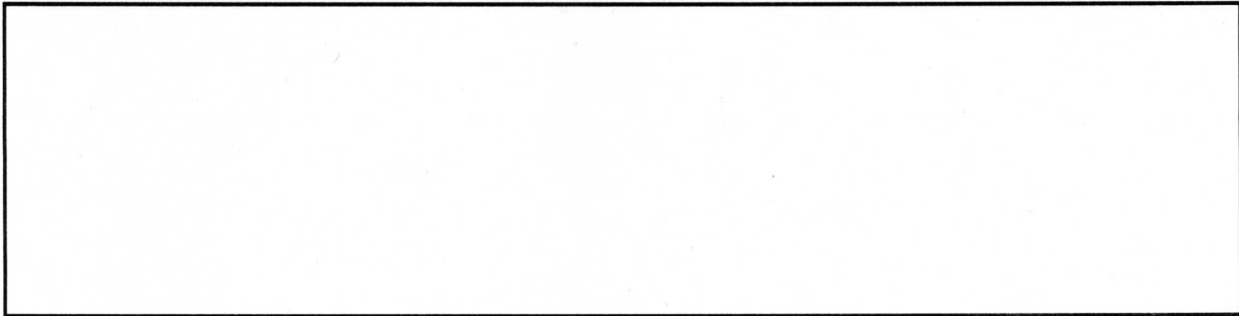


TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 24 of 239 Pages

(b) (1)  
(b) (3)-P.L. 86-36  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~



A chart on the following page gives in brief outline a description of the progressive changes in the German Enigmas. All the foregoing machines, except the O-Bar, Cipher Device 39, and the ~~NEWA~~ are discussed in the succeeding pages under individual headings, with additional details and variations.

(b) (1)  
(b) (3)-P.L. 86-36  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798

TOP SECRET CONTROL NO. 182-4  
Copy 4 of 30 Copies  
Page 25 of 239 Pages