DOCID: 3525898

~~TOP SECRET~~





# The Cryptology of the German Intelligence Services (U)

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~Classified By NSA/CSSM 123-2~~
~~Declassify On: Originating Agency's Determination Required~~

national security agency
central security service

~~TOP SECRET~~

Declassified and approved for release by NSA on 04-13-2009 pursuant to E.O. 12958, as amended MDR53595

DOCID: 3525898



Contents of this publication should not be reproduced, or further disseminated outside the U.S. Intelligence Community without the permission of the Director, NSA/CSS. Inquiries about reproduction and dissemination should be directed to the Office of Cryptologic Archives and History, T54.

■ DOCID: 3525898



*UNITED STATES CRYPTOLOGIC HISTORY*

*SERIES IV*

*World War II*

*Volume 4*

# The Cryptology of the German Intelligence Services (U)

David P. Mowry

**This document is classified TOP SECRET UMBRA in its entirety and can not be used as a source for derivative classification decisions.**

**OFFICE OF ARCHIVES AND HISTORY**

**NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE**

**1989**

DOCID: 3525898



# Table of Contents

DOCID: 3525898



# Foreword

The second part of David Mowry's history of German clandestine activity in South America is devoted exclusively to descriptions of the cryptographic systems used by the German intelligence organizations and their agents in South America. In fact, this detailed report covers German cryptographic systems used on a number of agent circuits in Europe as well. Mr. Mowry's interesting work invites a number of questions about German cryptography. For example, what does this collection of facts about these systems tell us about the state of German cryptography during World War II? Were these systems on a par with those of the United States, England, Japan, or more or less advanced? Were they new, obsolete, innovative, standard? Was there a correlation between the system and the level of information? And what of German security procedures and practices? Mr. Mowry has provided a valuable service in identifying and describing these systems. Perhaps future historians will attempt the challenge of answering these more general questions. It is, however, an excellent companion piece for his part one.

Henry F. Schorreck
NSA Historian

DOCID: 3525898



# The Cryptology of the German Intelligence Services

## Introduction

Historical records concerning the exploitation of Axis clandestine traffic in World War II are few. The following account depends primarily on *GC&CS Secret Service Sigint*, Volumes I–III, which covers the period 1928–45; "History of OP-20-GU (Coast Guard Unit of the Naval Communications Annex )," which covers only the period 1941 to 30 June 1943 and is concerned primarily with administrative matters rather than the cryptanalytic effort itself; and *History of Coast Guard Unit #387; 1940–1945*. Both the Coast Guard and the British Government Code &Cipher School (GC& CS) cryptanalytic histories cover the entire war, but consist of series of technical reports on the cryptanalytic methods used, with little regard for historical continuity, and little or no traffic analytic information. In addition, there is a file of over 10,000 Coast Guard translations of clandestine messages. Because the following is a synthesis of all of the above sources, footnotes have been omitted except for information derived from Colonel Albert MacCormack's London trip report and for the descriptions of the cryptographic machines developed by Fritz Menzer of the Abwehr, which are taken from TICOM (Target Intelligence Committee) documents. This account is not to serve as a course in cryptanalysis, but rather as a description of German cryptology. The reader is referred to the appropriate histories for details of analysis.

Each of the cryptanalytic agencies at this time used its own cryptosystem titling and case notation conventions. Coast Guard system titles consisted of a letter or digraph followed by a digit. The letters were "S" for substitution systems, "T" for transposition systems, "ST" for substitution followed by transposition, and "TS" for transposition followed by substitution. The systems were numbered one-up by type. Case notations consisted of a digit, signifying geographic area, followed by a one-up literal serialization within area. GC&CS broke the clandestine network down into 15 groups, notated I to XV. Individual links or "services" received a digital notation so that, for example, Stuttgart-St. Jean de Luz was notated X/290 and Paris-Wiesbaden was notated III/20. Unfortunately, no equation list for the British notation system has been found. Cryptosystems were referred to by the link notation. In the following discussion, terminals will be given when known.

## Code Systems

On 1 January 1940, messages encrypted with a dictionary code were intercepted on the Mexico-Nauen commercial circuit. Only 11 letters were used in the transmission: A, C, E, D, H, K, L, N, R, U, and W, with N having the highest frequency. It was apparent that a letter-for-number substitution was being used, with N as a separator. Anagramming the letters gave the result:

| D | U | R | C | H | W | A | L | K | E | N |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | – |

Thus, the text

UHHNR LNDAL NURND WCNCK ...

became

255-38 178-23 164-79 ...

Three other key words were used during the effective period of the system. All were easily recovered. All of the 1940–41 messages in this system were sent with the addresses SUDAMERIAT, WEDEKIND, SUDAMERO, or EGMARSUND.

Similar traffic was sent from Chile to BACOCHASE in March 1942, signed by the German ambassador to Chile. In these messages ten-letter key words were used with the other sixteen letters of the alphabet serving as separators. Eventually it was determined that the dictionary used was *Langenscheidt's Spanish-German Pocket Dictionary*. With this discovery all messages were completely decrypted.

With the beginning of the war in Europe, the Coast Guard was tasked with the collection of commercial circuits between the Western Hemisphere and Germany. This collection revealed that many Axis-dominated commercial firms in Mexico and Central and South America were using enciphered commercial codes in their communications with Germany.

The largest group of messages in enciphered commercial code used the *Rudolph Mosse* code with the letters of each code group transposed and a monoalphabetic substitution applied to the last two letters of the transposed group. These messages used the indicator OPALU as the first group of text (A1 group). Traffic was passed to and from SUDAMERO and SUDAMERIAT, Mexico; SUDAMERIAT, Hamburg; and SUDAMVORST, SUDAMERO, and SUDAMERIAT, Berlin.

In August 1941, traffic from SOLINGEN in Nauen, Germany, to BOKER in Mexico used the same code book with a subtracter of seven applied to each letter (i.e., EMUAS became XANTL). Other variations were noted: in 1941, MUENCHIMPO, Hamburg used a mixed arrangement of *Rudolph Mosse* and *Peterson* codes and other links used *Acme, Peterson, Mosse* or *Alpha* codes either enciphered or in combination with one another.

Three other codes were intercepted, two of them designed for encoding stereotyped weather messages. The *Dago* code (GC&CS terminology), used by German ships in the Baltic Sea, encrypted figures with a daily-changing key and encoded words with a two-letter code. A sliding code was used by all of the German trawlers in the Ijmuiden. Two sliding strips were used with clear values on a fixed table, with single-letter code values on one strip and mononome or dinome code values on the other. The A1 group of each message gave the position of each strip against an index mark and the number of characters in the message. Circuit II/405's five-letter code used the *International Signalbuch* with a simple substitution applied to the first character of each group.

**Monoalphabetic Substitution**

Only four monoalphabetic substitution systems were used by the German agent organization. The first of these was initially intercepted on the England-Germany circuit in October 1940. The preamble consisted of two four-letter and two three-letter groups which contained the date and time of encryption, character count, and serial number, encrypted with a monoalphabetic letter-for-figure substitution. The alphabets used in encrypting both the preambles and the messages were derived from a disk. There were two parts to the disk, each of which carried an alphabet and a series of numbers and could be rotated relative to the other. Each agent was assigned a fixed key letter. This letter, on the inner disk, would be set against the date (mod 26) on the outer disk. Plain values on the inner disk were then encrypted with cipher values from the outer disk. The numbers in both the preamble and in the text were similarly encrypted. OP-20-GU

interpreted the observed phenomena as a Vigenère square with progress through the square governed by the date, with a separate key used to encipher numbers in the text. The underlying plain text was English. The British were notified and it was later learned that they had arrested the agent and taken over his station. (Author's note: This was possibly the agent SNOW mentioned in part one.)

Circuit X/203, a ship, used a letter-for-figure substitution for encrypting its weather reports which consisted entirely of figures. Twelve different keys were used. The preamble consisted of the Q-signal QTT followed by a three-letter group. The first and third letters of this group were the equivalents of one and two, respectively, in the key being used.

A third system, referred to by the British as the *Wigo* cipher, was a dinomic substitution without variants sent in five-figure groups. The Z1 group of the message gave a character count and the Z0 identified the substitution set. The users of this system were never identified.

The only other monoalphabetic substitution system noted, first intercepted on the Hamburg-Cape Spartel circuit in January 1945, was used to report convoys spotted off Cape Spartel. The plain text was Spanish and eight substitution systems were used in daily rotation.

### Polyalphabetic Substitution

A number of links used variations on Gronsfeld polyalphabetic substitution, where all cipher alphabets were direct standard with the offset from the plain component determined by a running key. The maximum offset, therefore, was nine.

The "French Gronsfelds" used on II/320 and II/321 used a fixed 20-long key; while II/335 used daily-changing, variable-length keys. No indicators were used.

One variation on Gronsfeld cipher was used by an agent in England to communicate with his headquarters in occupied France. The system, referred to by the British as the *Constantinople* cipher, used the word "Constantinople" to derive the daily key. A numerical key was derived in the normal way and then multiplied by the date. Thus, for the eighth of the month

```
CONS T ANT INO P LE
29612131714481011 53
                  x8
-------------------
23689705371584809224
```

In October 1941, Rio de Janeiro was intercepted using a seven-alphabet Gronsfeld with a key of 3141592. Since 3.141592 is the decimal equivalent of the mathematical constant *pi*, this circuit was dubbed "the *pi* circuit."

The so-called "Dutch Gronsfelds" were not, strictly speaking, true Gronsfelds, since the slide of one alphabet against the other could exceed nine letters. The term is somewhat justified, however, by the fact that the different shifts of the slide used in encrypting a message never differed by more than nine. The key was periodic, based on the date, with two digits always used for the day and one or two digits for the month. Thus, 2 March was represented by 023 and 25 December by 2512. These figures were converted to letters by a daily-changing key to give a three- or four-letter key. In encipherment, the first letter of the key in the cipher component was aligned with A on the plain component and the first letter of text was enciphered; the second letter of the key was aligned with A and the

second letter was enciphered, and so on, repeating the key as often as necessary.

All of the above used direct standard alphabets. Some other circuits used random mixed alphabets. The "Spanish Substitutions" used tables of five random cipher alphabets in various ways, while the "Bordeaux Substitutions" used tables of five or ten alphabets. The *BF* cipher used a 21-long key to encrypt traffic passed on the Nantes-Paris-St.-Jean-de-Luz circuit. Keys were changed infrequently and the traffic could be identified by the letters "BF" in the preamble. The X/203 circuit, mentioned above, used a ten-alphabet substitution for traffic other than weather. The starting alphabet was indicated by a number in the preamble. That alphabet was then used to encipher the first five letters, the next alphabet enciphered the next five letters, etc., cycling after the tenth alphabet.

Much later, in 1944–45, the Shanghai-Canton circuit used a periodic polyalphabetic system to pass information concerning air traffic between China and India, United States aid to China, United States planes and equipment, and information and rumors concerning Russia. Each message used five alphabets taken from a 24-alphabet Latin square. The alphabets to be used in each case were indicated by a five-letter A1/Z0 indicator. Each alphabet served as both plain and cipher component, offset according to a key derived from the date of the message.

### Digraphic Substitution

Two digraphic substitution systems were used. The first, a double-square Playfair system was used according to normal rules. The second used a Playfair-like square in which any character from the same column as the plain letter could be used as a column coordinate and any character from the same row as the plain letter could be used as a row coordinate. Thus, in the square

N A T I O
L S E C U
R Y G B D
F H K M P
Q V W X Z

the letter P could be represented by 16 different digraphs:

OF UF DF ZF OH UH DH ZH
OK UK DK ZK OM UM DM ZM

As used on the Cologne-Maastricht circuit, the letter J was omitted from the square. The key was changed monthly, but only one key was broken as the traffic had no particular value. On another circuit, the underlying plain was in French and the letter K was omitted. In this case, ten nontextual letters at the beginning of text probably constituted a concealed preamble enciphered with a key.

### Single Transposition: Columnar

The story of the VVV TEST-AOR circuit has already been told in part one. In January 1941, when the FBI asked the Coast Guard for assistance in the solution of a group of

DOCID: 3525898



messages, examination revealed that they were copies of the traffic being relayed from GLENN to AOR through VVV TEST. The system was diagnosed as a simple columnar transposition and solved. Traffic on the VVV TEST-AOR circuit used a 20-wide key. The relay traffic turned out to be in two systems: a simple columnar transposition using a 16-wide key that was later reversed and then replaced by a 23-wide key; and a grille transposition which will be described later.

In April 1941, Coast Guard intercept operators found another circuit with the same characteristics as the VVV TEST-AOR circuit, using the callsigns REW and PYL. The control sounded very much like AOR. The A1–A4 groups of the messages, enciphered by a number key, contained date, time, and character count. Traffic on this circuit read as columnar transposition on a 20-wide key. This key was later reversed and still later replaced by another 20-wide key. In June 1941, Hamburg instructed the outstation Valparaiso to use the Albatross edition of the novel *South Latitude* as a key book. In the use of this key book the agent was assigned a secret number which, when added to the date and the number of the month, designated the page from which the number key and transposition key were to be extracted. Dummy letters were inserted in the plain text according to the transposition key for the first 100 letters of text. For example, if the key began 18, 20, 15, 11, . . . . , the first dummy character was inserted in the 18th position, the second 20 letters after that, the third 15 letters after that, etc. In the second 100 letters, the dummies were placed so as to reflect those in the first 100, making a symmetrical pattern.

The Belgium-France-England circuits were similar to the above, except that the keys varied in length from circuit to circuit, keys were taken from a line of a key page, there were no dummies, and the key page was given by an indicator inserted in a fixed position in the message.

Two Hamburg-Rio de Janeiro circuits were sister circuits that came up at approximately the same time. The key books for these circuits were the Albatross editions of *In the Midst of Life* and *The Story of San Michele*. On one of these circuits the agent's secret number was added to the date plus eight times the number of the month to determine the page from which the key was to be extracted. Traffic on the Bremen-Rio de Janeiro circuit had "buried" indicator groups at A4 and A6. Breaking these out with a key number gave the date, time, two-figure serial number, and two-figure key number.

On the Lisbon-Portuguese Guinea circuit the A10 group contained the key indicator enciphered with the key number. Text was inscribed boustrophedonically in columns with dummies at the top of columns 1 and 11, in the second position in groups 2 and 12, in the third position in 3 and 13, etc. Long messages were broken into 10-deep matrices, each separately transposed. On Lisbon-Lourenco Marques the A8bcd (the middle three letters of the A8 group) constituted the page indicator to an unknown book. All columns read downward, with dummies at the top of columns 1 and 9, in second place in 2 and 10, etc. Messages were transposed in toto, not broken up into multiple matrices. On the Lisbon-North America circuit the indicator was in the A5bcd. Key length was 17 and dummies were placed at the top of columns 1 and 10, in second position in 2 and 11, etc. The dummy pattern was reflected after nine lines. Messages from America began with an internal serial number. The messages on the Lisbon-Azores circuit carried a character count in the preamble with the key page given in A7abc and the dummy pattern identified in the A7de.

In the system used by Stettin-controlled stations, one basic key word provided all the keys. Key 01 was derived in the normal manner. For subsequent keys the key word was permuted cyclically (see fig. 1). Key lengths varied considerably from circuit to circuit. Dummies were placed according to the transposition key as on Hamburg-controlled circuits. The preamble gave the key number and the character count.

| Key Word: | A | N | T | E | N | N | E | N | A | N | L | A | G | E | A | N | T | E | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key 01 | 1 | 9 | 14 | 4 | 10 | 11 | 5 | 12 | 2 | 13 | 8 | 3 | 7 | 6 | | | | | |
| Key 02 | | 9 | 14 | 4 | 10 | 11 | 5 | 12 | 1 | 13 | 8 | 2 | 7 | 6 | 3 | | | | |
| Key 03 | | | 14 | 4 | 9 | 10 | 5 | 11 | 1 | 12 | 8 | 2 | 7 | 6 | 3 | 13 | | | |
| Key 04 | | | | 4 | 9 | 10 | 5 | 11 | 1 | 12 | 8 | 2 | 7 | 6 | 3 | 13 | 14 | | |
| Key 05 | | | | | 9 | 10 | 4 | 11 | 1 | 12 | 8 | 2 | 7 | 5 | 3 | 13 | 14 | 6 | |
| Key 06 | | | | | | 9 | 4 | 10 | 1 | 11 | 8 | 2 | 7 | 5 | 3 | 12 | 14 | 6 | 13 |

**Fig. 1. Derivation of Stettin Transposition Keys**

On the Stuttgart-Libya circuit, the key word appeared in the cipher text, inserted one letter at a time in prearranged positions, namely:

01 07 13 19 25
26 32 38 44 50
51 57 63 .. ..

The preamble gave a character count, the middle or first digit of which gave the position of an indicator group. For the purpose of writing in the key word this indicator group counted as a textual group and one of its letters was a letter of the key word. The other four letters gave the length of the key word enciphered twice, each on a different key number.

### Single Transposition: Combs and Grilles

The comb transposition system used on Cologne-Rio de Janeiro used the "Bluejacket" edition of the King James version of the Bible as a key source. This circuit used daily-changing callsigns and the specific indicator for the date of encryption was given by including the callsign for that date in the preamble. This date determined the page of the key book from which the key was extracted.

$$\text{Page} = 30 \times \text{number of month} \times \text{date} \times 10$$

The number "10" above was a secret agent number assigned to this agent for the year 1941. It was changed to "20" in 1942. This gave a page range of 41–401 for 1941 and 51–411 for 1942.

Figure 2 illustrates the encryption process using Genesis 1:1 as key. Inscribed across the top of the matrix, the key phrase determined the order of transposition of columns. Odd numbered columns were extracted from top to bottom, even numbered columns from bottom to top. Written down the left side of the matrix, the position of each letter of the key phrase in the standard alphabet determined the length of that line in the matrix.

In the case of Hamburg-Sao Paulo, only the Hamburg terminal was ever heard and only five messages were read. After the agent involved was arrested in 1943, it was

```
      I N T H E B E G I N N I N G G O D C R E
      1 1 2 1       1 1 1 1 1    1     1
      1 4 0 0 4 1 5 7 2 5 6 3 7 8 9 8 3 2 9 6

I  9 D E I N E N R V I
N 14 E R X X W A S C H B E R I C
T 20 H T E T O L D S M O B I L E X O L D S M
H  8 O B I L E H E R
E  5 S T E L L
B  2 T M
E  5 O N A T L
G  7 I C H H U N D
I  9 E R T T A U S E N
N 14 D S T U E C K E I N S F U E
N 14 N F F U E N F M M X M M U N
I  9 D H U N D E R T T
N 14 A U S E N D S T U E C K E I
G  7 N S N U L L F
G  7 U E N F M M X
O 15 M M C A N N O N M U N I T I O
D  4 N X X P
C  3 O N T
R 18 I A C X P O N T I A C H E R S T E L
E  5 L T M O N
A  1 A
T 20 T L I C H H U N D E R T T A U S E N D S
E  5 T U E C K
D  4 E I N S
```

**Fig. 2a. Comb Transposition Matrix**

```
NALHN  UCNED  LMNOH  NLDLE  EKHNP  NMLND
EEAUL  LEOWE  RSDED  SKFRS  FXONU  SMVCS
REEMT  TNTNA  EIINE  ECXOS  USCCO  XPAFU
ENUUT  HTLLT  XNDEH  OSTOI  EDNDA  NUMNO
ILATT  EDIMU  TMINM  HIEIF  MEIHT  ..... etc.
```

**Fig. 2b. Text after Comb Transposition**

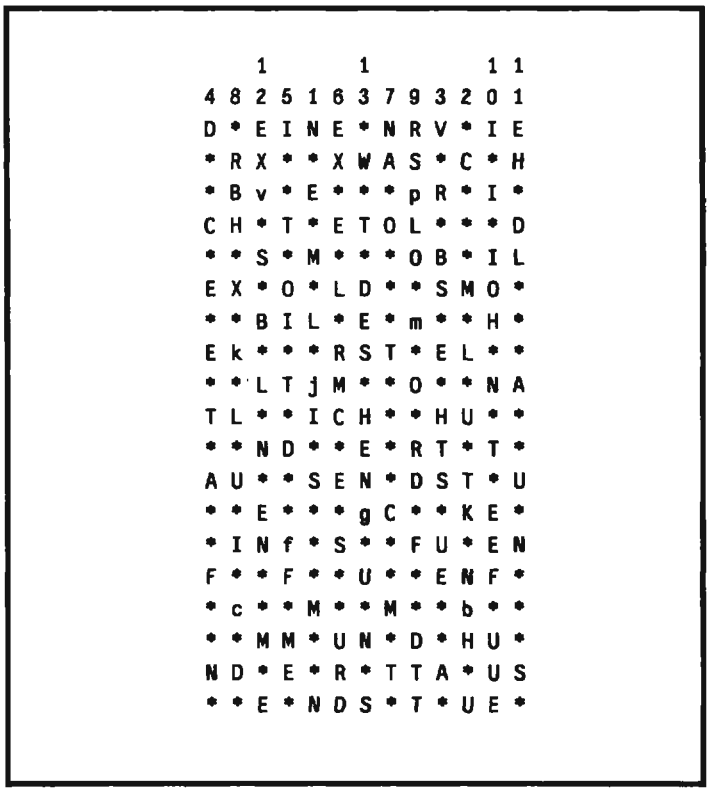
discovered that the initial key had been INCONSTITUTIONALISIMAMENTE. After contact was established, keys were taken from the book, *Pagel in Glueck.* When the agent was apprehended he turned over a copy of *The Martyrdom of Man* which was to have replaced

*Pagel in Glueck.* The key page was determined by adding the agent number to the day of the year.

Only six keys were recovered on Hamburg-Lisbon, and the key book, which was in either Spanish or Portuguese, was never determined.

Grilles were sheets of cardboard divided into squares with some of the squares cut out. Plain text was written into the cutout squares horizontally and extracted vertically by key. Dummy characters were inserted in prearranged squares (see fig. 3a). The grille could be used directly or in reverse (i.e., turned over) and in any one of four orientations, giving eight possible positions for any one grille.

Late in the autumn of 1940, intercept operators collecting the Chapultepec-Nauen ILC circuit intercepted some suspicious traffic from cable address VOLCO in Mexico City to BRAJOB in Berlin. These cable addresses were later changed to GESIK and INTERCIALE. In contrast to the commercial code traffic usually intercepted on ILC, this traffic was evidently transposed German text using low frequency letters as nulls. Further analysis determined that an overlay of some sort, with two sides, was being used. This overlay had 135 open cells (27 five-letter groups) with certain cells marked for the insertion of nulls. In figure 3, lowercase letters are nulls; the plain text is the same as in figure 2. Any one of



| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | | | 1 | | | | | 1 | 1 | | |
| 4 | 8 | 2 | 5 | 1 | 6 | 3 | 7 | 9 | 3 | 2 | 0 | 1 |
| D | * | E | I | N | E | * | N | R | V | * | I | E |
| * | R | X | * | * | X | W | A | S | * | C | * | H |
| * | B | v | * | E | * | * | * | p | R | * | I | * |
| C | H | * | T | * | E | T | O | L | * | * | * | D |
| * | * | S | * | M | * | * | * | O | B | * | I | L |
| E | X | * | O | * | L | D | * | * | S | M | O | * |
| * | * | B | I | L | * | E | * | m | * | * | H | * |
| E | k | * | * | * | R | S | T | * | E | L | * | * |
| * | * | L | T | j | M | * | * | O | * | * | N | A |
| T | L | * | * | I | C | H | * | * | H | U | * | * |
| * | * | N | D | * | * | E | * | R | T | * | T | * |
| A | U | * | * | S | E | N | * | D | S | T | * | U |
| * | * | E | * | * | * | g | C | * | * | K | E | * |
| * | I | N | f | * | S | * | * | F | U | * | E | N |
| F | * | * | F | * | * | U | * | * | E | N | F | * |
| * | c | * | * | M | * | * | M | * | * | b | * | * |
| * | * | M | M | * | U | N | * | D | * | H | U | * |
| N | D | * | E | * | R | * | T | T | A | * | U | S |
| * | * | E | * | N | D | S | * | T | * | U | E | * |

**Fig. 3a. Grille Transposition Matrix**
**(Lower case letters are dummies)**

the eight corners of the grille (obverse or reverse) could be placed in the upper left-hand corner.

Although the system is technically only a single transposition, the method effectively prevented solution by the normal method of matching columns and anagramming the resulting rows. Since there were no stereotyped beginnings or endings in this traffic, the

```
NEMLJ ISMNU HBNKT ULMCV RBSEH
TSUEA NFATE ECDIT OITDF FMEDR
USECM RLEXE NAOTC MTDCI ULKXH
BRRSP LOMOR DFDTT EUUFE ETNHO
IIIEH DLAUN XSEMN ENLBS VXEWT
DESHE NGUNS
```

**Fig. 3b. Sample of Grille-Transposed Text.**

solution of single messages of less than 54 groups presented a problem so difficult that not all of the messages in this system were ever read.

Some traffic in this system was also sent from GLENN to AOR via VVV TEST. The system was also discovered being used in secret ink messages carried out of Mexico by couriers. These were labeled the *Max Code* by the Germans.

In September 1941, Berlin-Rio de Janeiro stopped using simple transposition. The system introduced used the same type of indicator as that used on the BRAJOB-VOLCO circuit: the A3abc identified a key page and the A3d identified the upper left corner of the grille. The grille used proved to be the same as the BRAJOB-VOLCO grille with 125 open cells vice 135.

Traffic intercepted on the Madrid-West Africa circuit also used the 13×19 grille, but with 136 open cells; the same size grille as used by Paris had 140 open cells. The Las Palmas-Cisneros grille was only 9×13 with 88 open cells, while the grille used on the Bulogne-Ostend-Brussels-Lille circuit was 15×21 with 224 open cells.

It is interesting to note the degree of security which the German authorities believed this system possessed. After the rupture in German-Brazilian relations and during the period of the German spy roundup in Brazil, German Foreign Office dispatches were sent over the Madrid-West Africa circuit in this system, when commercial circuits could no longer be used.

### Aperiodic Polyalphabetic Substitution

These systems were encountered after the roundup of German spies in Brazil. Immediately after the Brazilian arrests, two new circuits were found which had the transmission characteristics of Hamburg-controlled agent communications: daily-changing callsigns, slow transmission speed, and voluminous "ham" chatter. The cipher system used was "running key," i.e., one in which the juxtaposition of two sliding alphabets is determined by a continuous aperiodic key, usually taken from a book or magazine. It was known that the Germans preferred to equip their agents with systems in which the elements could be memorized and used in combination with a popular novel or other innocent book; and it was hoped that either direct or reverse standard alphabets had been employed for the plain and cipher components. Such proved to be the case and decryption of messages revealed that the new circuit was a Hamburg-Chile one, which while it did not replace the previous Hamburg-Chile circuit, reported the same type of information. Intercepted traffic contained information on U.S. equipment and ship movements. It was later learned that the Spanish book *Sonar la Vida* was used for the

key source. The A1–A4 groups contained an enciphered preamble, and the A5 group usually contained the same letter repeated three times. After the system had been analyzed and some messages read, it was determined that the repeated letter was the reference letter used for sliding the plain and cipher components.

The other circuit which appeared in March 1942 linked Hamburg and Lisbon and passed information concerning the movement of Allied vessels to and from Lisbon. The key book in this case was eventually identified as the Portuguese novel *O Servo de Deus*. This circuit departed from normal agent communications procedures in that it used multiple frequencies on multiple schedules. The Lisbon terminal was assigned as many as eight different frequencies. Later these were changed weekly for greater security.

Another user never became fully operative. For several months Hamburg repeatedly sent what appeared to be seven different encipherments of the same two messages. No contact was ever made and transmissions finally ceased. In this case the plain text was in German with a Portuguese running key.

A new circuit out of Rio de Janeiro began operation in June 1942 using a running-key system. Traffic was very irregular and was concerned primarily with administrative matters. Both key and plain text were in German, but the book was never identified.

On the Stuttgart-St.-Jean-de-Luz circuit the preamble gave the character count and the penultimate digit of this number gave the position of the indicator. The indicator was five-letter, with the "ab" positions giving the page and the "cd" positions the line, both enciphered with a letter-for-figure number key. The "e" position identified the index letter to be used. Messages with *ER* in the preamble used a German key book to encipher German text. Other messages used a Spanish key book to encipher Spanish and occasionally German text.

A running-key system used in France was sent with the indicator in the A1 group in January and July, in the A2 group in February and August, etc., and in the Z0 group. On some links the key was in French. The fixed index letter was "Z."

**Single Transposition/Substitution Systems**

Around the end of 1942, the Hamburg-Bordeaux circuit used a 16-wide simple columnar transposition in conjunction with a trivial monoalphabetic substitution. Long after the fact it was learned that this circuit had used the "Janowski" (see below) system with a 16-wide key from July to November 1942. It had then changed over to the transposition/substitution system, which remained in effect until April 1943 when the Janowski encipherment was reintroduced, this time with a 22-wide key.

In the latter part of February 1943, the FCC provided the Coast Guard with intercept of an unknown circuit controlled by Hamburg. The traffic, intercepted in November and December 1942, included three messages of eleven groups each which matched two eleven-group messages intercepted by the Coast Guard on the same circuit in January and February 1943. The Coast Guard had already determined that a simple substitution using standard alphabets was involved with the resulting intermediate plain text transposed. Analysis of the five equal-length messages revealed the existence of a comb transposition matrix with a 21-long key which was finally determined to be *Ueb immer Treu und Redlichkeit* (always practice loyalty and integrity). The A1 group was the indicator for the substitution. Two standard alphabets were juxtaposed so that the A1b was the cipher equivalent of the A1a. The outstation on this circuit never responded by radio, but was apparently in South America.

The system referred to by the British as the "Bloodhound Cipher" was used on the Bremen-Bayonne circuit. It was a single transposition system substituted in columns.

The 25-long transposition key was made up of 25 consecutive letters from a lengthy key phrase. The starting point was determined by adding the date and the month.

Substitution was performed after the plain text had been written into the transposition matrix, and was based on a fixed substitution key

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 |
| G | M | V | W | L | B | C | U | T | S | D | I | Q | Y | X | E | O | J | F | K | A | P | R | N | H |

that is, "G" was the key for column 1, "M" for column 2, etc.

The message key letter to be used was determined by subtracting 2 from the date; thus, on the sixth of the month the key letter would be "D," the fourth letter of the alphabet. Two direct standard alphabets were used for encipherment with the message key letter set against the appropriate letter of the substitution key. In this case, "D" plain would be set against "G" cipher for column 1. Substitution for the 1st, 4th, 7th, 10th, etc. letters of the column was normal. For enciphering the 2nd, 5th, 8th, etc. letters, the plain component was moved one space to the right of the initial setting; and for the 3rd, 6th, 9th, etc., the plain component was moved one space to the left of the initial setting. For instance, if the first column read

E
N
X
B
W
N

setting "D" plain to "G" cipher would give

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plain: | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Cipher: | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

and the column would be enciphered

E = H
N = R
X = Z
B = E
W = A
N = P

After the substitution was performed columns were extracted from the bottom upward. The indicator was in the A3 group with the A3ad being the first two letters of the transposition key.

In December 1942, the Royal Canadian Mounted Police provided the Coast Guard with the record of a German agent named Janowski who had been arrested in Canada in November. Among the materials turned over were two novels which were to be used to generate his encryption keys. The agent's number, 28 in this case, added to the number of the month and date, gave the page of the book to be used. Messages had a five-group preamble enciphered with two keys: one for the first four groups which contained transmission date, time, character count, and serial number, and the second for the fifth

group which contained the date of encryption. In this system, the Janowski method (see fig. 4), the text was first written horizontally into a transposition rectangle and extracted according to a 20-long key derived from the first 20 letters reading downward from the top left-hand corner of the page for the day (see fig. 4a). Substitution was performed on

| W | R | V | C | S | L | P | T | H | F | A | S | F | P | A | A | G | M | A | Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 1 | | 1 | 1 | 1 | 1 | | | | 1 | | 1 | | | | 1 | | 1 |
| 0 | 5 | 9 | 5 | 6 | 0 | 2 | 8 | 9 | 6 | 1 | 7 | 7 | 3 | 2 | 3 | 8 | 1 | 4 | 4 |

**Fig. 4a. Janowski Transposition Key**

| 2 | 1 | 1 | | 1 | 1 | 1 | 1 | | | | 1 | | 1 | | | | 1 | | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 5 | 9 | 5 | 6 | 0 | 2 | 8 | 9 | 6 | 1 | 7 | 7 | 3 | 2 | 3 | 8 | 1 | 4 | 4 |
| D | E | I | N | E | N | R | V | I | E | R | X | X | W | A | S | C | H | B | E |
| R | I | C | H | T | E | T | O | L | D | S | M | O | B | I | L | E | X | O | L |
| D | S | M | O | B | I | L | E | H | E | R | S | T | E | L | L | T | M | O | N |
| A | T | L | I | C | H | H | U | N | D | E | R | T | T | A | U | S | E | N | D |

**Fig. 4b. Transposition Rectangle**

| T | W | B | T | M | K | G | K | M | A | T | H | T | M | Q | T | B | Q | T | B |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | | 1 | | | | | 1 | | 1 | | 1 | 1 | 1 | 1 | | 1 | 1 | |
| 4 | 0 | 2 | 5 | 9 | 7 | 5 | 8 | 0 | 1 | 6 | 6 | 7 | 1 | 2 | 8 | 3 | 3 | 9 | 4 |

**Fig. 4c. Substitution Key**

```
Fixed Alphabet:  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

                 ( N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
Slide:           ( 1 1 1   1 1               1 2   1         1   1   1
                 ( 1 2 8 3 3 9               4 0 2 5 9 5 7 8 0 1 6 6 7

                      Column:     1          Substitution:   1

                                  R                          E
                                  S                          F
                                  R                          E
                                  E                          R
```

**Fig. 4d. Substitution**

each column separately by means of a substitution key derived from the first 20 letters reading downward from the top left-hand corner of the page for the first of the month. The substitution key was slid against a stationary standard alphabet using as an index the letter in the top left-hand corner of the day page. Substitution was column by column with the key number corresponding to the column number set against the index. In figure 4c, the strips are set up for enciphering column 1. Figure 4d shows a sample substitution.

Subsequently, seven circuits were noted using Janowski method with, at most, minor variations in indicator placement and encipherment procedure: Hamburg-Spain, Hamburg-Gijon (Spain), Hamburg-Madrid, Hamburg-Lisbon, Hamburg-Vigo (Spain), Hamburg-Bordeaux, and Hamburg-Tangier.

On the Hamburg-Spain circuit, Hamburg started off by sending two messages. Two days later another two messages were sent. When compared it was obvious that the second transmission was a repeat of the first with a different encipherment. Further examination revealed that both messages of the first transmission tested for substitution, as did the second message of the second transmission. The first message of the second transmission tested for transposition. When the two first messages were superimposed it was found that each segment of the transposed version equated to a segment of the substituted version. This stripped off the substitution, determined the number of columns, and fixed the column lengths, all in one operation. All that remained was the anagramming of one message and two keys were recovered simultaneously. This constituted one of the worst breaches of communications security encountered by the Coast Guard. Unfortunately, no further traffic was passed on this circuit.

Only two variations were noted in the use of Janowski. Hamburg-Gijon used a constant key for a short time before shifting to book key, and Hamburg-Bordeaux used a 16-long key from July to November 1942, at which time the circuit changed over to the transposition substitution system previously described. In April and May 1943, Hamburg-Bordeaux again used Janowski, this time with a 22-wide key.

Two versions of substitution with grille transposition were used. The simpler method used three simple substitution tables for the 1st to the 10th of the month, the 11th to the 20th, and the 21st to the 31st. Normal grilles were used, but the spaces for dummy letters were filled with plain text. On the Madrid-San Sebastian circuit a five-alphabet periodic substitution was applied to the plain text which was then written into the grille and extracted by key. Later, the plain text was written into the grille and extracted by key, after which the substitution was performed. Some of the links that used this system used dummies, others did not. Indicators were the same as for normal grille usage; each circuit had only one substitution table.

### Double Transposition

The four circuits using double transposition, all in late 1942, were Berlin-Madrid, Berlin-Tetuan (Morocco), Berlin-Teheran, and Berlin-Argentina.

The first system of this type successfully solved by the Coast Guard was intercepted on Berlin-Madrid in late 1942. Inspection revealed that the A1/A2 and Z1/Z0 groups contained a repeated enciphered indicator which deciphered as follows:

1. The first three digits ranged under 400, probably indicating the pages of a book.
2. The next two digits ranged low enough to be a line indicator.
3. The next four digits consisted of two pairs, each ranging from 10 to 30.
4. The last digit was not significant.

It seemed obvious that the two dinomes ranging from 10 to 30 were indicators designating the length of keys to be selected for a double transposition. A search was made for a message in which the length of the text equaled the product of the two keys. This constitutes a classic case for solution since such a situation nullifies the transposition. After initial success in this case, various other cases were also solved in which the message lengths bore specific relationships to the products of key widths. In November 1943, the indicator was reduced to one numerical group which the British believed designated the page number in the first three digits and the line number in the last two. A constant five-figure group was added to this indicator using noncarrying arithmetic. From the line so determined, the first four words were selected as first key and the first four words of the next line were selected as second key. Since no solution for the additive was ever obtained, no traffic in the newer system was ever read.

In traffic on the Berlin-Tetuan circuit the indicator initially consisted of a single group, giving only the date of encipherment. This was sufficient because there were only seven keys used for the first transposition, one for each day of the week, and the key for the second transposition was weekly-changing. On 1 April 1943, the indicator was changed to one similar to the first system used on Berlin-Madrid. On 4 November 1943, the indicator was again changed, in the same fashion as Berlin-Madrid, and solutions ceased. Keys on this circuit were derived from a German translation of a British detective story.

In the Berlin-Teheran traffic the dates were sent unenciphered in the preamble. The only other possible indicator was a number in the preamble which looked like a serial number, but which did not run in sequence. Although a few messages were solved individually, it was not until the German agent in Teheran was caught in the autumn of 1943 and the record of his interrogation forwarded to the Coast Guard that the remainder of the traffic on this circuit could be read. The complete literal key was a six-line verse:

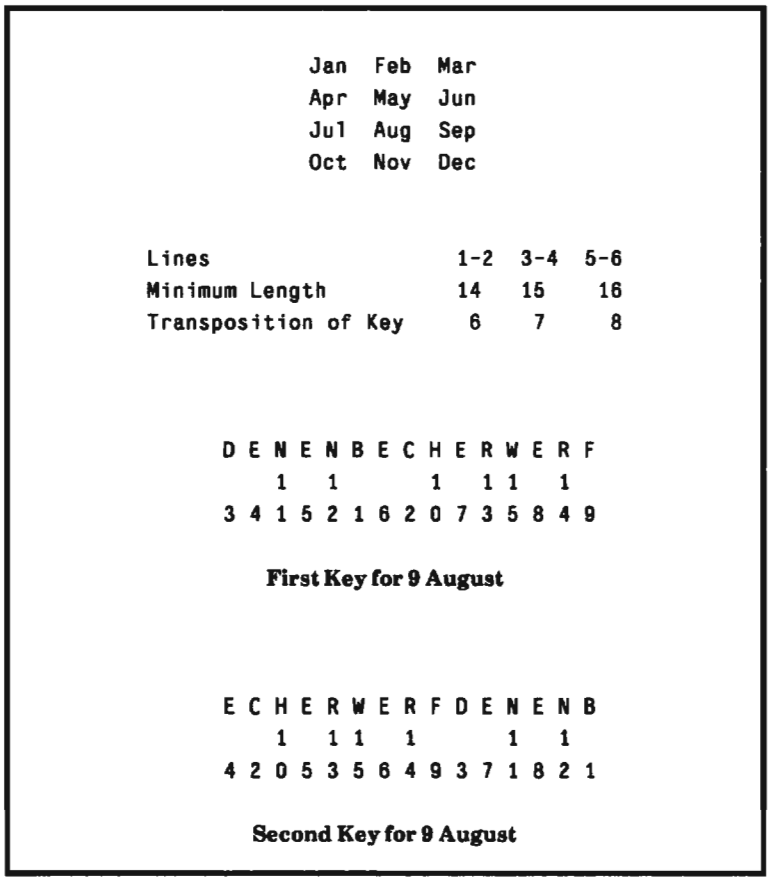
| | |
|---|---|
| Wer wagt es Rittersman oder Knapp | [Who will risk it, knight or squire |
| Zu taugen in diesen Schlund? | To faithfully serve in this abyss? |
| Einen goldenen Becher werf ich hinab | I hurl a golden chalice down, |
| Verschlungen schon hat ihn der schwarze Mund | A black mouth engulfs it all around. |
| Wer mir den Becher kann wieder zeigen– | But whoever makes it again be shown, |
| Er mag ihn behalten, er ist sein eigen. | He shall retain it, for it's his own.] |

The month determined the pair of lines from which the numerical key was derived; the date determined the number of the letter in this pair of lines with which the literal key started; the month then determined the minimum number of letters taken from this point for the first key; and the month finally determined the number of letters transposed from the beginning to the end of the first key to give the second key. Figure 5 shows the way in which the month controlled the key. It should be noted that if after counting the minimum number of letters, the end of a word had not been reached, the word was completed.

The Berlin-Argentina circuit was actually a number of circuits operating in and around Buenos Aires, several of them simultaneously. A variety of systems were employed on these circuits during the time they were intercepted, but double transposition was the only hand system used. The first such traffic was transmitted in November 1942, but it did not start appearing regularly until January 1943. The Coast Guard had no success with the system until GC&CS solved a 16 March 1943 message and passed the keys on to OP-20-GU. The only apparent indicator was a preamble number similar to that found on Berlin-Teheran. The first key was a constant, of which four were used: SONDESCHLUESSEL (probe key), GASGESELLSCHAFT (gas company), SCHAEFFNER

DOCID: 3525898





Jan Feb Mar
Apr May Jun
Jul Aug Sep
Oct Nov Dec

| Lines | 1-2 | 3-4 | 5-6 |
|---|---|---|---|
| Minimum Length | 14 | 15 | 16 |
| Transposition of Key | 6 | 7 | 8 |

D E N E N B E C H E R W E R F
1 1 1 1 1
3 4 1 5 2 1 6 2 0 7 3 5 8 4 9

**First Key for 9 August**

E C H E R W E R F D E N E N B
1 1 1 1 1 1
4 2 0 5 3 5 6 4 9 3 7 1 8 2 1

**Second Key for 9 August**

**Fig.5. Double Transposition: Berlin-Teheran**

(conductor), and a fourth that apparently was the true name of the agent, NOORD. This last key was recovered, but the name could not be reconstructed. The second transposition key was a spell of the three-figure preamble group.

### Double Transposition/Substitution

Three systems involving both double transposition and substitution were introduced in the summer of 1943 after Chief Inspector Fritz Menzer of the Cipher Department of the German Army High Command was given the job of revamping all clandestine cryptosystems.

The first to appear was the "ABC Key" (see fig. 6) which appeared on all Hamburg-controlled circuits in Europe and Africa. The system used double columnar transposition and monoalphabetic substitution with variants. The substitution cipher alphabet was a keyword transposition mixed sequence and was applied after the message was written into the first transposition rectangle. The variants were introduced by placing the letter E between W and X in the plain component for German-language messages and the letter A between V and W in Spanish-language messages. These alphabets were used without change in the first, fifth, and ninth lines of the first transposition rectangle. Figure 6

```
P       : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

C      I: A N W B K V E G S H C P Y I D Q Z L J T M F R U O X
      II:                       I Y D Q           U R O X
     III:                       D I Y Q           O U R X
      IV:                       Q I D Y           X U O R
```

**Substitution Alphabets**
**Keyword Transposition Mixed Sequence Using Keyword HIMMELBLAU (sky blue)**

```
K R A F T W A G E N F U E H R E R S C H E I N P R U E F U N G
1 2   2 3   1   1 1 2   1 2   2 2   1   1 1 2 2 2   1 3 2 1
7 2 1 9 7 1 2 2 4 8 0 8 5 4 3 6 4 6 3 5 7 6 9 1 5 9 8 1 0 0 3

* * * * * * * * * D E I N E N R V I E R X X W A S C H B E R I
C H T E T O L D S M O B I L E X O L D S M O B I L E H E R S T
E L L T M O N A T L I C H H U N D E R T T A U S E N D S T U E
C K E I N S F U E N F F U E N F M M X M M U N D H U N D E R T
T A U S E N D S T U E C K E I N S N U L L F U E N F M M X M M
```

**First Transposition Rectangle**

```
* * * * * * * * * B R G Y R Y Z M G R Z U U F A L W E B R Z G
W E J U J Y C B L P Y N G C U R Y C B L P Y N G C U E U Z L J
O C C J P I D A J C G W E E T D B O Z J J A T L O D B L J T O
W S X G Q L K T X Q K K T X Q K P P U P P T Q B E T Q B X Z J
J A T L R Y B L J T R W H R G Y L Y T C C K T R Y K P P U P P
```

**Substitution**

```
* * * * * * * J C * X T C D K B R B Z U T L J X J Y G E T H Z
R D K Y U P J P C * E E B Q P U J G L R Y G K R B U L B P B A
T L G J O J P R C * E X R Z L J P C U Y A T K W O W J B P C Q
T F N T Q T Z L T * Z P A G L B R E C S A Y U T Q G M Y B P L
L C O E Y G C O P * Y J P Q R G N W K W W U D T K R Z J X U O
O S N
```

**Second Transposition Rectangle**

Transposition rectangles for December 18 (12/18). Text is inscribed horizontally into the first rectangle, substitution is made, the resulting text is inscribed horizontally into the second rectangle, and extracted according to the ABC key.

**Fig. 6**

DOCID: 3525898



shows how the cipher component was changed for the second, sixth, and tenth lines; the third, seventh, and eleventh lines; and the fourth, eighth, and twelfth lines.

The transposition key was 31-long, usually an easily remembered phrase or compound word. In the first rectangle all first row squares to the left of the column whose key number was the same as the date of encipherment were blocked out and the plain text started in that column. In the second rectangle the column corresponding to the date and all first row squares to the left of the column corresponding to the month were blocked out and the text was started in the latter column. If the two numbers were the same, then the column was not blocked out in the second rectangle and both rectangles were the same. Figure 6 shows two rectangles prepared for the substitution and transposition.

The major weakness of the system was that once a message was completely solved all traffic enciphered on the same basic phrase was readable and keys remained in effect for three to six months.

At about the same time that the ABC Key was introduced on the Hamburg circuits, other forms of combined double transposition and substitution were introduced on the Berlin-controlled circuits. Descriptions of only two of these, Procedure 62 and Procedure 40, are available.

Procedure 62 used a 31-long key in which the key phrase was written out in two lines. The first line of 16 characters had a space after each letter, with the spaces numbered from 1 to 15. The second line was started in the space corresponding to the number of the month of encryption and wrapped around. The following illustrates the procedure, using the phrase LA MUJER MAS HERMOSA EN ESPANA DEL SUR for the month of April.

```
                  1 1 1 1 1 1
1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
L A M U J E R M A S H E R M O S
  S U R A E N E S P A N A D E L
```

The two lines were then merged

L S A U M R U A J E E N R E M S A P S A H N E A R D M E O L S

and the numerical key derived in the usual manner.

In the first transposition rectangle the column immediately to the left of the number corresponding to the date was blocked out, as were all squares to the left of this column on the first line. In the second rectangle the column was not blocked out, but the same first row squares were. A trivial substitution was applied to the text in the first rectangle to camouflage the letters A and E.

Line 1 – Plain
Line 2 – A became W, E became F and vice versa
Line 3 – A became X, E became G and vice versa
Line 4 – A became Y, E became H and vice versa

This four-line cycle was repeated throughout the message.

Procedure 40 was used on the Madrid-Ceuta circuit as a back-up system to the cipher machine normally used. In this procedure substitution took place before the first transposition. Both transposition and substitution used the same key phrase.

For substitution, a keyword mixed sequence derived from the key phrase, in this example DONDE MENOS SEPIENSA SALTA LA LIEBRA, was written into a 5×5 square, omitting the letter J.

| | 1 | | | | | |
|---|---|---|---|---|---|---|
| | D | O | N | E | M | |
| | S | P | I | A | L | |
| 4 | T | B | R | C | F | 2 |
| | G | H | K | Q | U | |
| | V | W | X | Y | Z | |
| | | | 3 | | | |

The plain text was divided into five-letter groups and the following substitution was made, group by group:

> The first letter was replaced by the letter above it in the square.
> The second letter was replaced by the letter to its right in the square.
> The third letter was replaced by the letter below it in the square.
> The fourth letter was replaced by the letter to its left in the square.
> The fifth letter was left plain.

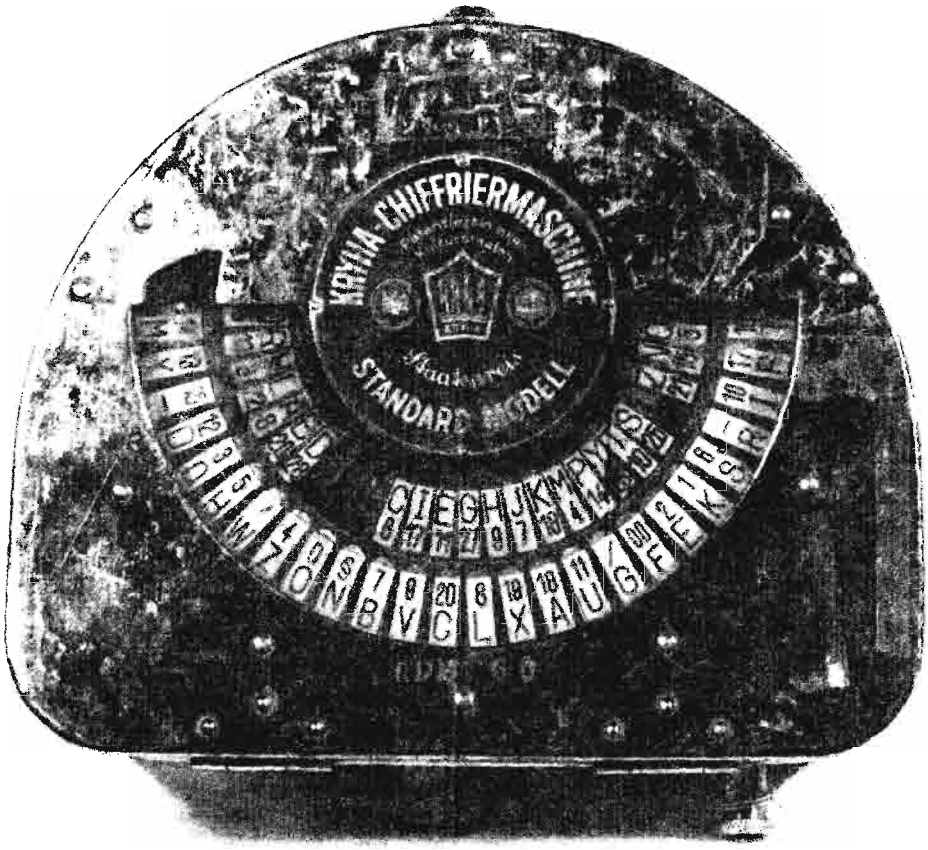
The letter J was left plain in all positions. Thus, MESSAGE would become ZMTLA TM....

In the first transposition rectangle all squares in the first line to the left of the number corresponding to the date of encipherment were blocked out. In the second rectangle the same was done to the first line squares to the left of the number corresponding to the month of encipherment.

### The Kryha Machine

The Kryha machine was a clockwork-powered mechanical running key encipherment device. Two alphabets were on movable tabs so that the sequences of the plain component and the cipher component could be changed at will. The movement of the cipher alphabet disk was controlled by a cogwheel with 52 holes around the edge. A plunger on the end of a lever served as a detent by dropping into each of the holes in succession. These holes could be individually covered, thus changing the wheel pattern, and varying the "kick" with each step of the wheel. The total kick in one full revolution was prime to 26 so that the period of the machine was equal to 26 times the total kick. The cryptovariables of the system were therefore the plain sequence, the cipher sequence, the wheel pattern, the initial setting of the cogwheel, and the initial setting of the cipher sequence against the plain sequence. The last two variables were changed with each message, the others less frequently.

A pair of indicators, enciphered with a multivalued number key, gave the alphabet setting (the number of the cipher letter set against O plain) in the "ab" positions, and the cogwheel setting in the "de" positions. The "c" position was a filler.

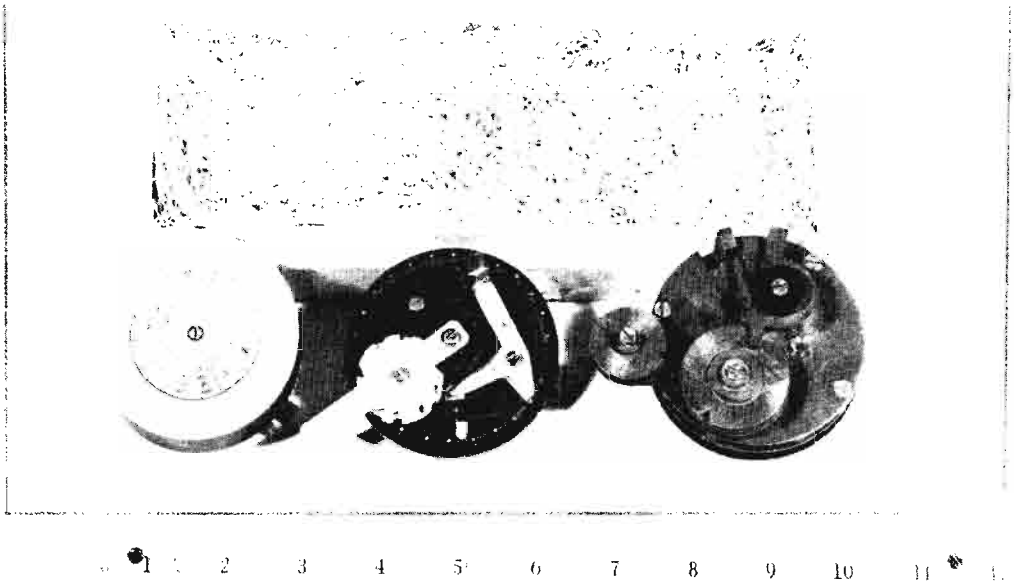



**The clockwork-driven Kryha, a popular German made cipher machine that was widely used commercially in the 1930s.**

### The Menzer Devices

When Chief inspector Menzer had been tasked by Admiral Canaris with testing the security of the Abwehr cryptosystems in 1942, he found them depressingly inadequate In addition to the ABC Key, Procedure 40, and Procedure 62, he introduced the cipher plate and the cipher wheel as field agent cipher devices; and Cipher Device 41 for use by Abwehr nets within Germany.[1]

The cipher plate was designed by Menzer specifically for agent use. It consisted of a circular box about the size of a shoe polish can containing three resettable notched wheels and a spring. On the top a mixed alphabet could be written with pencil or grease pencil, 13 characters on the fixed ring and 13 on the movable disk. The disk was rotated to wind the spring for encipherment. Pressing a button on the side would release the disk and allow it to rotate until stopped by the notch rings. If the disk stopped in a position where its letters were in phase with those on the outer ring, the cipher value was read directly. If the stop was in an intermediate position, the number of the line opposite the plain value would be read, and the cipher value taken from the cell with that number.[2]



**Menzer Device**

The cipher wheel was another hand-operated cipher device designed for agent use. It was made up of two disks mounted concentrically. The lower disk had 52 notches or holes around its edge into which a pencil or stylus could be inserted to turn the disk. On the face of the disk were 52 cells into which a keyword-mixed alphabet could be inscribed twice, clockwise. The upper disk had a direct standard alphabet inscribed on half of its periphery, next to a semicircular window that revealed 26 characters of the mixed sequence on the lower disk. The upper disk also had a notch cut into its edge which exposed ten of the holes on the lower disk. This notch had the numbers 0 to 9 inscribed next to it, in a counterclockwise direction, so that when the exposed holes were lined up with the numbers, the letters on the lower disk were lined up with the letters on the upper disk.

Various methods of key generation were used. On Chilean circuits an 11-letter key word was numbered as for a transposition key, with the first digit of two-digit numbers dropped. The key was extended by appending a two-digit group count and a four-digit time group

| A | N | T | O | F | O | G | A | S | T | A | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 6 | 0 | 7 | 4 | 8 | 5 | 2 | 9 | 1 | 3 | 1 | 2 | 1 | 4 | 4 | 0 |

On other circuits a Fibonacci sequence of 100–125 digits would be generated through various manipulations of the date, time, and agent number. If the message was longer than the key, the latter would be reversed as many times as necessary. Key generation tables were also used.

The key constituted the input to an autoclave. After aligning the alphabets according to an indicator in the message, a stylus was inserted in the hole corresponding to the first key digit, and the lower disk was rotated clockwise until the stylus was stopped by the end of the notch. The plaintext letter was then found on the upper disk and its cipher value read off of the lower disk. The stylus was then placed in the hole corresponding to the

second digit of key and the same procedure was repeated for the second letter of text. Thus the true key at any point in the cipher was equal to the sum of all the previous key inputs.[3]

The Cipher Device 41 was a cipher machine invented by Menzer in 1941 which was based on Hagelin encipherment but included a mechanism for variably stepping the Hagelin wheels. The Cipher Device 41 had six pin wheels that were mutually prime. The first five wheels had kicks of 1, 2, 4, 8, and 10, respectively; the sixth wheel made these kicks positive or negative. The enciphering cycle (encipherment of one letter) consisted of three elements:

1. This took place if and only if the sixth key wheel had an active pin in the "motion index position." If this were the case, then all of the following occurred: Wheel 1 moved one step and each of the remaining four wheels moved one step unless the wheel to its left had an active pin in the "motion index position," in which case it would move two steps.
2. A key kick was generated which was the sum of the kicks of wheels which had active pins in the "kick index position." If, however, the sixth wheel had an active pin in the "kick index position," the key kick would be 25 minus the sum of all of the other kicks. In other words, under such a circumstance, the key would complement itself.
3. This was identical to Step 1, except that it occurred whether or not Wheel 6 had an active pin in the "motion index position." In this step, Wheel 6 also stepped one or two positions, depending on the state of Wheel 5.

**Menzer Device SG-41. A successful encipherment system, but of limited use due to its heavy weight.**

The original specifications called for a light weight, durable machine to be used by military units forward of division. Menzer designed it to provide a cipher tape and to be keyboard-operated to improve the speed of encipherment. As a result of the keyboard operation, he was able to redesign the arrangement of letters on the print wheels to flatten the cipher frequency count.[4]

Because of the wartime shortages of aluminum and magnesium the machine ended up weighing between 12 and 15 kilograms, too heavy for field use. Removal of the keyboard would have lightened the machine, but the redesign of the print wheels prevented their being used directly for encipherment. Production stopped because no one knew what to do. About 1,000 machines had been constructed and were distributed to the Abwehr which began using them on circuits within Europe in 1944.[5]

GC&CS read a number of Cipher Device 41 messages through depth reading techniques, but even after some of the machines had been captured and examined, no one could postulate a theory of cryptanalytic attack. A 1947 WDGAS-71 report stated that if a mechanically reliable machine could be built embodying the same principles as the Cipher Device 41, it would undoubtedly be a valuable asset. The report noted that because of the key complementing characteristic of the machine, statistical tests did not seem to offer any particular promise for solution.[6]

**The Coast Guard Solution of Enigma: The Commercial Machine**

In January 1940, Coast Guard intercept operators collected a suspicious circuit using the calls MAN V NDR, RDA V MAN, and the like, transmitting one to five encrypted messages a day. It soon became apparent that all messages intercepted were in flush depth, although the method of encipherment was as yet unknown.

Attempts to solve the first twenty or thirty messages in depth met with no success because of badly garbled copy and lack of any definite evidence as to the underlying language. By the time sixty or seventy messages had accumulated, however, it seemed certain that the language was German and that a word separator had been used.

In the progressive development of the plain cipher equivalences for each position of the depth, it was observed that no plain letter was represented by itself in the cipher text and that the plain cipher equivalences within each alphabet were reciprocal. This, together with the language, seemed ample justification for assuming that the traffic had been encrypted on an Enigma cipher machine. The Coast Guard Intelligence Unit had a model of the commercial version of the machine, together with the original manufacturer's instructions and suggestions for its use. These instructions included the practice of using "X" as a word separator, and of representing numbers by their equivalent letters as shown on the keyboard of the machine

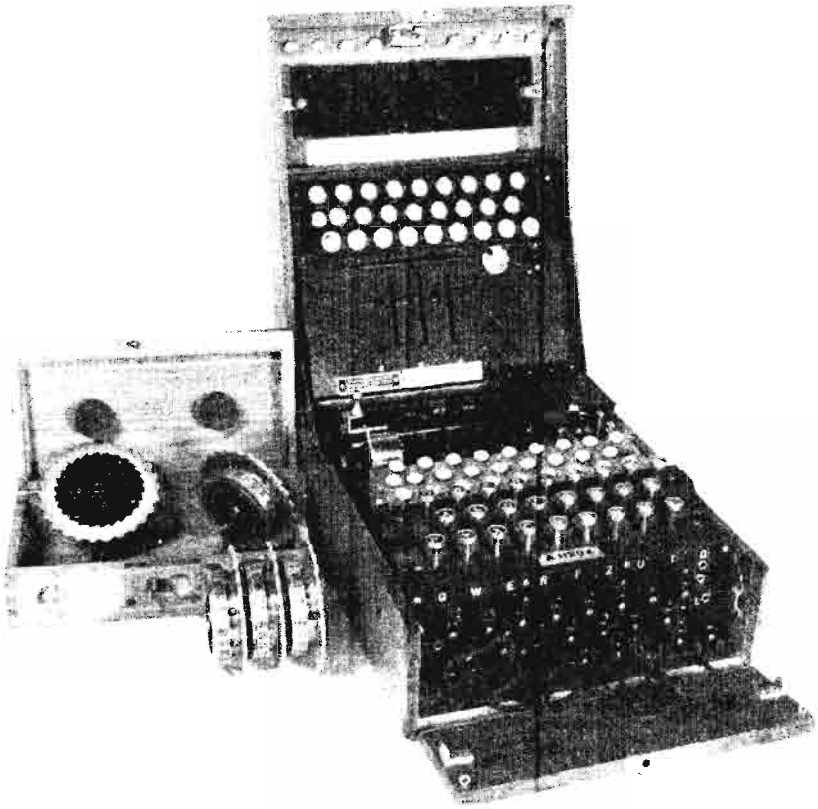
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
|---|---|---|---|---|---|---|---|---|---|
| Q | W | E | R | T | Z | U | I | O | P |

After almost fully recovering the first 32 alphabets, the Coast Guard cryptanalysts developed a technique for stripping off the effect of the reflector and then of successive wheels, resulting in a complete solution of the machine with all wirings. The wiring recovered in this solution later proved to be known wiring, but the Coast Guard recovery of wiring assumed to be unknown was achieved without prior knowledge of any solution or technique. This is believed to be the first instance of Enigma wiring recovery in the United States. It should be noted that the initial approach to the problem was an adaptation of the procedure used in the solution of the Hebern machine.

From the equivalent wirings of the two outside wheels, the Signal Intelligence Service (SIS) identified them as the actual ones furnished in the old commercial Enigma machine, and the Navy later identified the traffic as Swiss army. With respect to the numbers on the actual wheels, the wheel order used was 1–3–2 (left to right, as one faces the machine).

### The Coast Guard Solution of Enigma: The Green Machine[7]

A station using the call TQI2 was first heard on 10 October 1942 on 10,415 kHz. The station sent calls only up to 30 October, when a message was intercepted. The message preamble was 2910/301/66. TQI2 was believed to be linked with a station using the call TIM2 on 11,310 kHz. On 12 November 1942, it was learned from bearings taken by the FCC that TQI2 was in Europe and TIM2 was in South America. This was confirmed by the Radio Security Service (RSS) at a radio intelligence meeting on 17 November on the basis of Hamburg-Bordeaux traffic which was being read by GC&CS. The Bordeaux terminal had been instructed to monitor the circuit and to assist in case of difficulty. Station TQI2 also used the call RSE, which was believed to be the alternate control in Bordeaux.



**Enigma with extra rotors**

During October and December 1942, 28 messages were intercepted from TQI2. This series of messages had several duplicate message numbers (two 315s, three 316s, etc.) The messages were tested for depth and although the coincidence rate was definitely above random, it was rather poor. It was assumed, therefore, that most of the messages were encrypted on the same key, but that the duplicate message numbers were possible evidence of different keys. Actually, all messages turned out to have been encrypted on the same key. The poor coincidence rate was a result of the inclusion of several practice messages in the series. These practice messages contained a short text at the beginning and were filled out to average length with dummy text.

The lessons learned from solving the commercial Enigma were applied, together with the improved techniques learned from the British, and the machine was solved. Wheel motion patterns were similar to the Enigmas used by German agents in Europe which had been solved by the British prior to the appearance of TQI2. Decrypted texts showed that the circuit was between Berlin and Argentina.

On 11 January 1943, messages were transmitted with external serial numbers 322–328. It was possible to align these in depth by stepping each successive message one position to the right, producing a ten-letter repeat in messages 322 and 327. The complete plain text was quickly reconstructed. Two later sets of messages sent in June and July confirmed the method used on this circuit for determining monthly ring settings and normal positions.

**The Coast Guard Solution of Enigma: The Red Machine**

The first mention of this machine appeared in message number 145 from Argentina to Berlin on 4 November 1943. This message was sent on the "Green" circuit and encrypted on the "Green" Enigma. The message read

> THE TRUNK TRANSMITTER WITH ACCESSORIES AND ENIGMA ARRIVED VIA RED. THANK YOU VERY MUCH. FROM OUR MESSAGE 150 WE SHALL ENCIPHER WITH THE NEW ENIGMA. WE SHALL GIVE THE OLD DEVICE TO GREEN. PLEASE ACKNOWLEDGE BY RETURN MESSAGE WITH NEW ENIGMA. [s]LUNA

On the same day, the "Red" section sent message number 989 stating that an additional Enigma machine had arrived. This message had been encrypted with the Kryha machine which the Coast Guard had solved.

On 5 November 1943, Berlin sent message number 585 to the "Green" section in Argentina:

> RE YOUR 145: NEW ENIGMA IS INTENDED FOR RED ONLY.

The following day, Berlin sent message number 917 to the "Red" section:

> INTERN 86. THE NEW ENIGMA WHICH ARRIVED TOGETHER WITH TRUNK TRANSMITTER IS FOR RED. IT IS A BIRTHDAY SURPRISE FOR LUNA.

On the same day, 6 November, the "Red" section in Argentina sent message number 991 requesting a key for the new Enigma, asking that it be sent via the "Blue" key (unsolved) and not via the "Red" Kryha key. The message went on to say that they were constantly making a fundamental blunder in transmitting a new key by means of the old one.

DOCID: 3525898



Berlin replied to this message on 9 November, asking the "Red" section to be patient for a few more days until a key for the new Enigma could be forwarded.

At this point there ensued a considerable amount of confusion regarding methods of transmission of key, settings for the "Red" Enigma, and settings for the "Red" Kryha, all of which was finally resolved by 14 December. Once the Germans got their encryption procedures squared away, the Coast Guard solved the "Red" Enigma by normal methods.

### The Coast Guard Solution of Enigma: The Berlin-Madrid Machine

About 5 May 1944, the Berlin-Madrid circuit stopped using double transposition and began using Enigma. An examination of the traffic on a single day revealed that messages from the same transmitting agent could be superimposed in depth by use of the time group. For example, a message having a preamble encipherment time of 1410 would be in phase with a message encrypted at 1400 hours from the eleventh letter of the latter message. This was similar to one method previously encountered on the Berlin-Argentina circuit, where a secret daily-changing number was added to the encryption time and the machine was then stepped that number of positions forward from the basic key for the day.

After determining the indicator system being used, the various Enigmas used by the Security Service group, of which the Berlin-Madrid circuit was a part, were considered. Only four machines had been employed by this group: the "Green," the "Red," a combination of "Red" wheels and a "Green" reflector, and the so-called "M" machine. Assuming that the traffic was encrypted on one of the known machines, a considerable time was expended on guesses in depth (the depth of any series of messages was never enough to yield a solution by that method alone), followed by running menus on the sliding GRENADE and checking the resulting hits in the uncribbed depth.

This method eventually read the system on a depth of twelve. The successful cribs were easily expanded and the full text recovered. The machine involved employed the "Red" wheels and the "Green" reflector. The only other time this type of usage was encountered was when the instructions for the "Red" machine were first sent to Argentina.

### The Coast Guard Solution of Enigma: The Hamburg-Bordeaux Stecker

In the period immediately preceding the change from hand to machine system, several Hamburg-Bordeaux messages were solved which proved to be reencipherments of unidentified cipher texts. These had a short plaintext internal preamble giving a serial number, letter count, and a cover name to identify the encrypted traffic.

An analysis of the plain texts of messages encrypted in the old system showed that some type of radio intercept activity was involved. From this information it was deduced that the Bordeaux end of the circuit acted as a sort of monitoring and relay station which listened in to certain outstations for the Hamburg control and furnished Hamburg with the texts of outstation messages which Hamburg had failed to receive.

Further information was secured through a reencryption sent by Bordeaux. Ten groups of a message were sent; the transmission was interrupted and later a message was sent which repeated the ten groups with some of the letters changed. The changed letters had been substituted in a manner which suggested that a stecker had been employed and that one or perhaps two wires had been improperly plugged. The combination of the

stecker and the three-letter indicator found on the traffic strongly suggested the use of the German Service wheels.

The next step in the analysis was the identification of the traffic reencrypted in the last days of the old hand system. This proved to be traffic from the FBI-controlled Hamburg-New York circuit. By examining message lengths and transmission times, it was then possible to find days on which Bordeaux had reencrypted New York traffic by machine and relayed it to Hamburg. Correct message placement supplied cribs which were tried on the Bombe and the machine was solved. It proved to be using Service wheels 1, 2, and 3 with a fixed "Bruno" reflector and adapter.

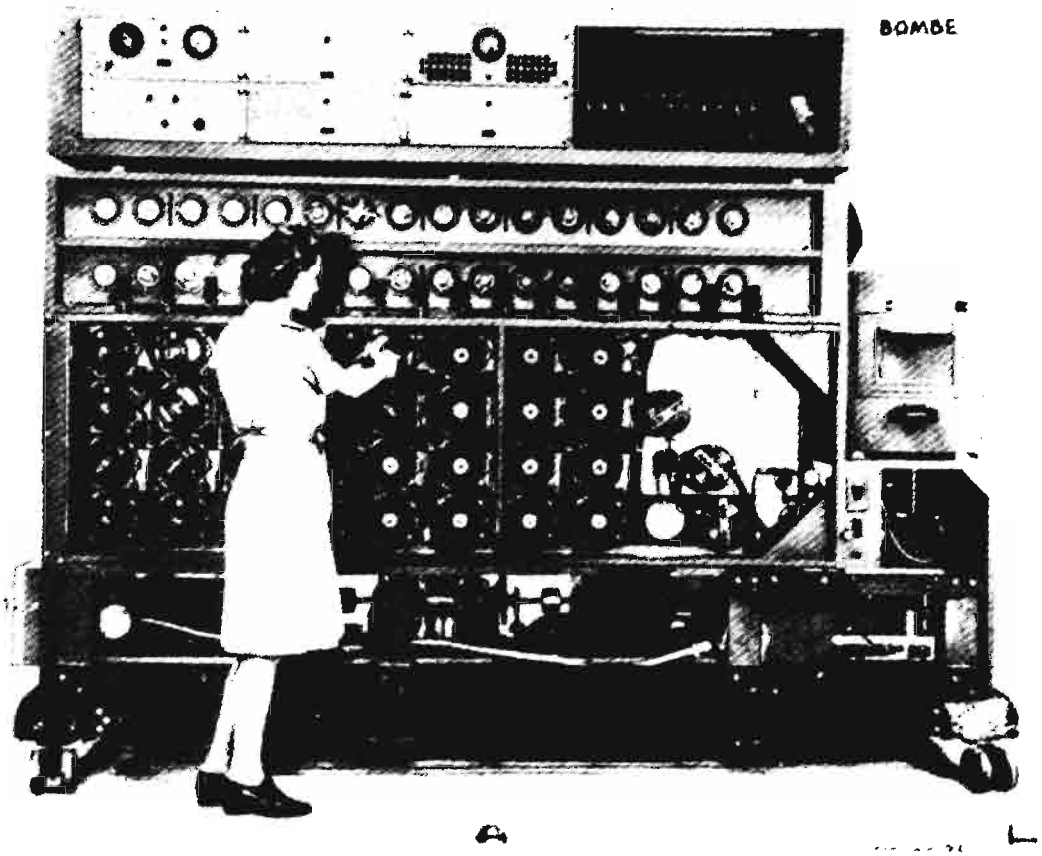
From a security standpoint, the conditions under which this circuit operated exhibited an almost complete abandonment of good cryptographic practices. Not only did the Germans use their most secure cryptomachine to retransmit low-grade traffic, but the settings used were those employed on Spanish Abwehr nets. Furthermore, there were indications that the Germans were aware that the New York circuit was controlled – yet the reencryption of this low-grade traffic was permitted. This was also the only example known to the Coast Guard of the Service machine being employed for clandestine traffic.

**The British Effort**

Clandestine traffic worked by the British fell into three cryptographic segments called ISK (Illicit Series Knox), ISOS (Illicit Services Oliver Strachey), and ISTUN (Illicit Series TUNNEY). Two sections at Bletchley Park were solely engaged on clandestine: Section ISK was wholly cryptanalytic, and Section ISOS did crypt work on all traffic other than ISK and ISTUN. ISOS also was the intelligence and distributing center for the entire clandestine output. ISTUN was broken by the TUNNEY Section under Pritchard which handled all TUNNEY traffic, including clandestine.[8]

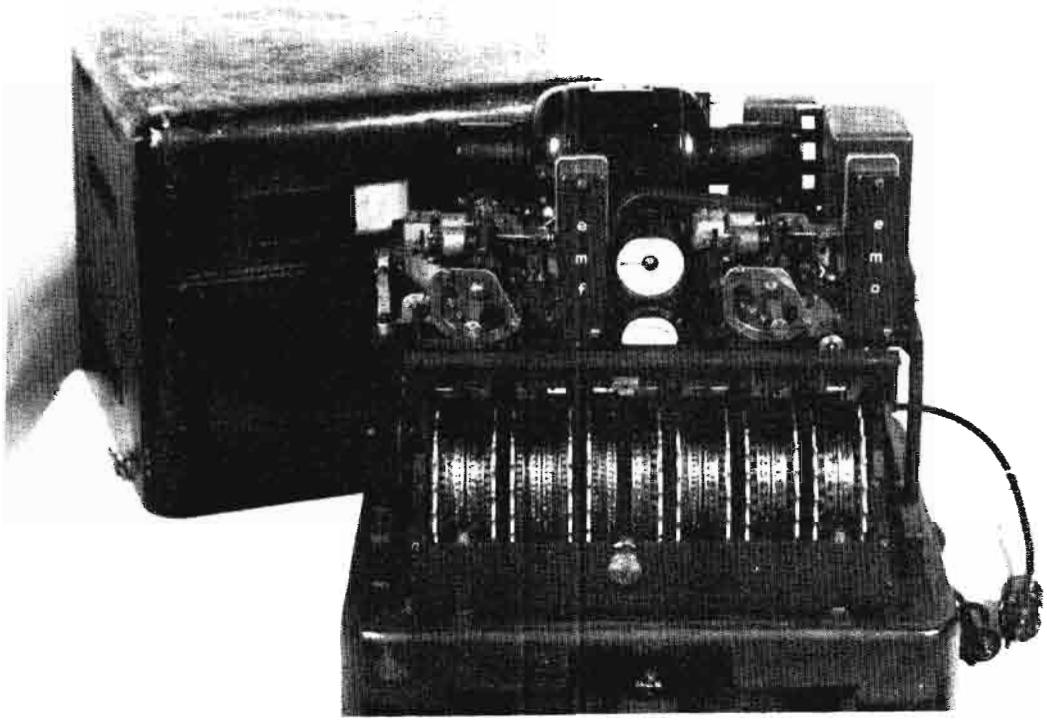
Bletchley Park

As of mid-1943, the ISK Section had the use of one to two Bombes, but most of the work was done by hand and the Bombes were used only for research and particularly difficult keys. The solutions were entirely based on probable word and cribs were frequently derived from ISOS traffic. The solution of a key usually took one to three days, but was often much faster if demanded, as in the case of Spanish traffic during the Mediterranean operations.[9]




**The Bombe, named for the loud ticking sound it made during operation.**

The traffic intake was about 350 messages per day, of which about 300 were read. Much of the unreadable traffic was too garbled; the Norwegian keys were especially difficult. Spanish Morocco used the commercial type Enigma but all the other ISK machines were uniform except the Paris-Canaries circuit which had its own wiring. ISK was mostly used by important Abwehr stations in RSS groups II, XIII, XIV, and VII/23. It was estimated that the coverage of Spanish ISK was 95 percent complete, Balkans 75 percent, Berlin to Turkey 80 percent, and 90 percent for group VII/23. After the messages were broken they were sent to the ISOS Section for translating and distribution.



TUNNEY

The ISK machine was introduced at the end of 1940 and was first broken by the British on Christmas Day, 1941.[10]

The ISOS Section was established at the end of 1939 and by mid-1943 was reading about 150 illicit radio circuits. The traffic consisted of a wide variety of transposition and substitution ciphers, with the traffic usually in German but including considerable Spanish and French and occasionally many other languages. All RSS groups, except VIII, XII, XIV, and XVI carried only Abwehr traffic. Groups VIII and XVI were Italian Secret Intelligence and were not handled by ISOS but by Bletchley Park's Research Section. Group XIII was ISK and ISOS traffic of the Security Service; Group XIV carried Abwehr traffic, both ISK and ISOS, and diplomatic traffic. Group XIII ISOS traffic was double transposition. Groups I and XV used simple transposition; Group XIV ISOS included a variety of substitution and double transposition.[11]

In 1943 the average daily ISOS traffic intake was 150–200 messages per day. All incoming traffic was sorted in the ISOS Section Registry Room into RSS groups and sent to the appropriate sections, all three of which sent their decodes back to the ISOS Registry Room, which handed decodes to the Watch Room. The Watch Room ran 24 hours, with eight people usually on duty except on the graveyard shift when there was only one. The Watch Room translated and amended the texts which were often severely garbled. Messages then went to typists who made sixteen English copies and also German copies for certain users. The Watch Room kept a file of recent back traffic in German, and the Registry Room kept a complete back file in English. As of June 1943, GC&CS had produced 115,000 clandestine serial numbers, of which a little over half were ISOS type.

One serial number frequently contained one or several messages, averaging about two per serial number. During 1942 GC&CS produced 61,267 serial numbers, and the daily average rose from 101 to 209. ISOS, ISK, and ISTUN were circulated twice daily (each in a separate series) to MI6, to the three service ministries, to MI5 and RSS. Group XIII was circulated separately twice daily, under the title "ISOSICLE," to the same recipients, plus the London Office of the Chief of the Secret Service. In addition, the following special series were circulated:

1. ISMEW traffic from the Bilbao-Biarritz circuit, covering the movements of ore boats, went to MEW in addition to usual customers;
2. ISBA, containing all messages referring to British agents abroad, went only to MI-6;
3. TUNNEY traffic, referring to DF of British transmitters, went only to MI-8;
4. Paris to Stuttgart traffic, referring to White Russians who listened in on Paris to Russian radio telephone conversations, was circulated only to the office of CSS;
5. Norwegian traffic went to the usual customers; and
6. The Intelligence Branch of ISOS kept indexes of persons and places; studied organization of the Abwehr and Security Service, abbreviations, vocabulary, and cover names. It studied ISOS for cribs into ISK and both for cribs into Enigma or other traffic. It maintained liaison with the recipients of the output and studied the entire output for the benefit of the section as a whole.[12]

In 1943 most of the ISOS traffic was in Groups II and VII, with a considerable amount in Group I, and a little in Group III. The principal topics of the messages were[13]

1. Chetnik and Partisan operations in Yugoslavia;
2. Naval observations from Spain and Portugal of Iberian harbors, Gibraltar, and the Eastern Mediterranean;
3. Agents reports from Spanish Morocco on the situation in North Africa;
4. Military developments in Turkey and the Near East, including disposition of Turkish forces and arrivals of British missions;
5. Red Cross activities in Greece;
6. Ship movements in the North Sea and off the Scandinavian coast;
7. Military intelligence about Russian troop movements;
8. General arrangements for carrying on espionage;
9. Slipping agents through to their destination;
10. Administrative;
11. Service messages on radio communications and use of ciphers.

Almost all ISK traffic was in Groups II and XIV and occasionally Group VII. The principal subjects were[14]

1. Naval observations from Spain and Spanish Morocco;
2. Administrative;
3. Naval observations in the Near East;
4. British troop movements in the Near East;
5. Military activity in Turkey;
6. Naval activity in the Black Sea;
7. Partisan and Chetnik warfare in Yugoslavia;
8. Organization of communists in Yugoslavia;
9. Slipping agents into Turkey;
10. Russian military movements;
11. Conditions in Iran;
12. Military supplies from the Allies to Turkey;
13. Inquiries about the loyalty and reliability of individuals.

ISTUN traffic was not intercepted by RSS but by the non-Morse intercept station at Knockholt and, therefore, did not carry RSS group numbers but was entirely Abwehr traffic. The great bulk of the messages was between Berlin and Greece and included much information on suspected individuals, some messages on German propaganda to Arab countries, and a little on enterprises of Branch II.[15]

ISOSICLE messages were transmitted between Berlin and Lisbon, Istanbul, Sofia, Madrid, Bucharest, Helsinki, Switzerland, Budapest, Tetuan, Paris, Marseilles, and unknown locations. This was traffic of the Security Service, and was very different from Abwehr traffic, much more diplomatic and political. The principal topics were[16]

1. The Finnish political situation;
2. Finnish broadcasts to Estonia embarrassing to the Germans because of "underlying democratic ideology" and because the Germans had forbidden the Estonians to listen to foreign radio;
3. Italian activities in Corsica, which seemed to foreshadow Italian attempt at colonization and annexation;
4. Jewish problem in Bulgaria;
5. The troubles of the American army in Algiers;
6. Economic warfare plans;
7. Administrative;
8. Communications service.

The reliability of information contained in Abwehr and Security Service traffic varied widely, from completely inaccurate to substantially accurate. Intelligence reports were often prepared by paid agents and had to be assessed in that light.[17]

DOCID: 3525898



## Glossary

| | |
|---|---|
| Abteilung | Branch |
| Abwehr | Counterintelligence |
| Abwehrleitstelle (Alst) | Counterintelligence Control Post |
| Abwehrstelle (Ast) | Counterintelligence Post |
| Allgemeine SS | General SS |
| Amt | Department |
| Grundstellung | Setting |
| Gruppe | Group |
| Hauptabteilung | Bureau |
| Kriegsorganization (KO) | Combat Organization |
| Meldekopf (MK) | Message Center |
| Nebenstelle (Nest or Anst) | Branch Post |
| Oberinspektor | Chief Inspector |
| Oberkommando Wehrmacht (OKW) | High Command of the Armed Forces |
| Oberkommando des Heeres | Army High Command |
| Reich | The nation |
| Reichsfuehrer | Leader of the Reich |
| Reichssicherheitshauptamt (RSHA) | Reich Security Administration |
| Schluesselgeraet | Crypto Device |
| Schluesselrad | Cipher Wheel |
| Schluesselscheibe | Cipher Plate |
| Schutzstaffel (SS) | The SS, Blackshirts (lit., "Protection Squad") |
| Sicherheitsdienst (SD) | Security Service |
| Sicherheitspolizei (SiPo) | Security Police |
| Sondeschluessel | Probe Key |
| Unternehmen | (Special) Operation |
| Verfahren | Procedure |
| Wehrkreis | Military District |
| Zahlschluessel | Key Number |

DOCID: 3525898



**NOTES**

1. 79/49/TOPSEC/AS-14, TICOM DF-174, "Description of Contacts of Fritz Menzer with American and Soviet Authorities and Summary of Career," p. 21. ~~(TSC)~~
2. 79/49/TOPSEC/AS-14, p.33; and 33/51/TOPSEC/AFSA-14, R-2,"Schluesselscheibe 50" (May 1951). (TSC)
3. LCDR L.A. Griffiths, RNVR, *GC&CS Secret Service Sigint*, Vol. III, pp. 111–15. ~~(TSC)~~
4. WDGAS-14's *European Axis Signal Intelligence in World War II as Revealed by TICOM Investigations and Other Prisoner of War Interrogations and Captured Material, Principally German*, Vol. II, p. 29. ~~(TSC)~~
5. Ibid., p. 29. ~~(TSC)~~
6. TICOM DF-19, "Cipher Device-41" (10 January 1944); Memorandum from Frank W. Lewis, WDGAS-71, to COL Solomon Kullback, WDGAS-70, "Study of the C-41 Cipher Device" (4 March 1947); and *GC&CS Secret Service Sigint*, Vol. II, pp. 165–71. ~~(TSC)~~
7. The descriptives "Red" and "Green" were applied by traffic analysts to Enigma to designate different circuits serving two different groups of agents. In addition, the set-ups on the two machines differed.
8. COL Alfred MacCormack's report on his trip to London, May-June 1943, p. 42. ~~(TSC)~~
9. Ibid., pp. 42–43. ~~(TSC)~~
10. Ibid., p. 43. ~~(TSC)~~
11. Ibid., pp. 44–45. ~~(TSC)~~
12. Ibid., pp. 44–47. ~~(TSC)~~
13. Ibid., pp. 47–48. ~~(TSC)~~
14. Ibid., pp. 48–49. ~~(TSC)~~
15. Ibid., p. 49. ~~(TSC)~~
16. Ibid., pp. 49–50. ~~(TSC)~~
17. Ibid., p. 50. ~~(TSC)~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~