R.I.P. 401 — German Naval Ciphers
October 1944

Source: NARA, College Park, Md., Record Group 457, National Security Agency, Historic Cryptographic Collection, Box 1393, NR 4457, ARC Identifier: 2811218, HMS/MLR Entry Number: A1 9032
https://catalog.archives.gov/id/2811218

Explanatory note: The document is only a partial copy of the NARA archive document. The cover sheet is missing so the exact title is not known, however in the NARA index for this holding the document is entitles "German Naval Ciphers." It is marked R.I.P. 401, but R.I.P. — Radio Intelligence Publications is crossed out. What this means is not clear. A copy of R.I.P. 401, with the title "German Ciphers Methods and Procedures for Decrypting," is at NARA in Record Group 38, The Crane Collection, in Box 168. If that document is identical or is a later version of the present document is unknown. The RG38 document is much longer at a total of some 260 pages.

Editor: Frode Weierud, Crypto Cellar Research
Web Site: www.cryptocellar.org

Version: 28 May 2022

TOP SECRET-ULTRA

~~R.I.P~~. No. 401

TABLE OF CONTENTS AND LIST OF EFFECTIVE PAGES

TOP SECRET-ULTRA

LIST OF FIGURES

LIST OF FIGURES CONT'D.

TOP SECRET-ULTRA

LIST OF FIGURES CONT'D.

they effectively spiked the guns of their own attack.

The cause of this fiasco lay in the German national trait of boundless blind and arrogant conceit. Their attitude was expressed repeatedly by German cryptanalysts captured in the closing days of the War, who stated "At an early stage we had progressed so far that further study was useless. The Enigma, used as we have issued instructions to use it, is unbreakable."

The blunders the Germans made were mainly four:

a) Virtually unparaphrased reencodements from System to System and Key to Key.

b) Standard phraseology endlessly repeated.

c) Gradual, rather than sweeping changes in cipher aids.

d) Systematic rather than random Keys.

In the pages which follow we will trace the usages of the unbreakable machine, and the abuses which broke it, confining ourselves to Naval usage during the period of American participation in the War.

II - <u>THE MACHINE</u>

a) Its General Characteristics

The only cipher machine used by the German Navy was a special model of a general type of device called the "Enigma" by its manufacturer, HEIMSOTH and RINKE, of Berlin. In its first form, Series A, it had been sold commercially before the War. Later models were made increasingly complex and assigned Series-letters which progressed through the alphabet. The Naval type had been assigned Series M as designator, called by the Germans "Schluessel M".

It was a well-built device--rugged, portable, compact (14" x12 " x 6 ") and fairly easy to operate./ It is recommended that the reader the machine, each of which we will briefly discuss.

a) the Stecker (See Figure 4)

b) the Fast Wheel "

c) the Medium Wheel "

d) the Slow Wheel "

e) the Reflector combination "
(Reflector Wheel and Reflector)

f) Back through Slow, Medium and Fast Wheels, and the Stecker.

Although Figure 4 shows each of these elements diverting the current from a straight path, in fact each except the Reflector might, in certain instances (as in the case of Self Steckers) let the current go straight through it. The combination of all the elements can, therefore, be considered as an electrical maze.

This Maze can be changed in either of two ways. The first is by changing the identity of the elements composing it (using different Wheels or Reflector, or Steckering differently). The possible ways of doing this gives the number of Cycles. The second way of changing the Maze is by causing to change their relative positions those portions of the Maze capable of motion. The number of different positions which the movable elements can take is the length of the Cycle. We can, therefore, estimate the security of the device by considering (a) the number of choices of different elements in the Maze, and (b) the degree of freedom of their motion. We will consider them in the order given above. Again the writer is advised to use an actual captured device in conjunction with Figure 4.

The Stecker (English "sticking" or "plugging") was not a self-contained unit of the device, as were the Wheels and Reflectors. It was a method of connecting the Typewriter Keys, on the one hand, and the Lights, on the other, with the contacts on the right-hand side of the Fast Wheel. Users of the Schluessel M were each issued a series of ten double-ended wires, of which one is shown in Figure 5. These were plugged into the front of the machine in the fashion shown in Figures 1a and b (only 5 of the 10 wires being put in). In Figure 1a, the reader will see that one of the wires connects the two holes labelled 6 with those two labelled 11. As might be inferred from the fact that four holes were used, the result of using a given wire was to make a four-way displacement of current: current starting at the F (6) key entered the Fast Wheel at point 11, while current starting at the K (11) key entered at the 6 point. Similarly, current leaving the Fast Wheel at the 6 point went to the 11 (K) light, and leaving at the 11 point went to the F (6) light. Each wire interchanged a pair of letters both going into and coming out of the machine. With 10 wires, 20 letters would be Steckered, and 6 would be left Self-Steckered. There are 230,230 ways of selecting 6 holes out of 26, and 624,729,075 ways of interconnecting the remaining 20 holes in pairs. The product of these two figures is the contribution of the Stecker to the number of different Cycles for which the machine can be set up. Once the wires are plugged into the holes, they stay there until a new plugging is set up. Hence the Stecker makes no contribution to the length of any given cycle.

Wheels - Place was provided in the machine for use of three Wheels at a time (called by the Allies the Fast, Medium and Slow). In Figures 2a, b, and c, one can see their external appearance and size. Figure 6 shows a partially destroyed captured Wheel, with

ORIGINAL

some of its internal wiring still in place. Actually, on each Wheel each spring contact on the right was wired to one, and only one, flat contact on the left. These wires were permanently installed according to the eight different patterns set out in [redacted] 450 pp 26c and 32. The Wheels were numbered I to VIII, depending on their pattern. That shown in Figures 2 was No. III. Since there are 336 ways of selecting three out of eight objects, this is the factor which the Wheels contribute to the number of possible different cycles set up on the machine. Similarly, since each Wheel could occupy any one of 26 positions on its axle, 26^3 or 17,576 is the factor which the Wheels would be expected to contribute to the length of the individual cycle. Actually, for reasons not necessary to discuss here, the motion of the device was such that for each cycle certain settings were skipped, and in some cases the cycle was half the length. See [redacted]. 475 pp 16ff.

Reflector Combination. Until the end of 1941, immediately after American entry into the War, the Naval Enigma had been Three-Wheel. That is to say, in the space labelled Reflector Combination, in Figure 4, there had been merely a single Reflector. In an attempt at greater security the Germans modified the device in such fashion that, instead, use was made of a Reflector and a Reflector Wheel. The former is shown in Figure 7. It will be observed to be much smaller than a regular Wheel, to have no letters around its rim, and to have flat contacts on one side only. The Reflector Wheel was identical in design with a Regular Wheel, except for one feature. It had spring contacts on both faces--to brush against the flat contacts of the Wheel on its right and of the Reflector on its left. The wirings of Reflectors and Reflector Wheels are given in ~~R.I.P~~. 450 pps. 26c and 32.

Immediately after American entry into hostilities, the Germans had one Reflector (Bruno) and one Reflector Wheel (Beta). Later, in July of 1943, another pair, Reflector Caesar and Reflector Wheel Gamma were introduced. There were four ways of choosing one of two Reflectors and one of two Reflector Wheels, so that this is one contribution of the Reflector combination to the number of possible Cycles on the machine. The Reflector had always to be put in the Enigma in the same position, while the Reflector Wheel could be set at any one of 26 positions; hence, between them, they added another factor of 26 to the number of different cycles. Neither Reflector nor Reflector Wheel moved, once set up. Consequently, the Reflector Combination added nothing to the length of cycle.

There is one feature of the machine which has not, so far, been mentioned. That is the fashion in which the Wheels moved. This is irrelevant to our present discussion, since, at present, we are concerned only with the number of possible positions in each Cycle, and not with the order in which they are used. Actually, it will be seen below that the motion of the device is one of its weaknesses, rather than one of its strong points.

From the above we can now give a numerical measure of the security of the Enigma--in terms of the number of different ways in which any given message might have been enciphered. That is the product of the number of different cycles available, and the number of possible places (starting points) in any given cycle. We then have:

Number of Possible Cycles	
Self Steckers	230,230
Stecker Pairs	624,729,075
Wheel Orders	336
Reflector Combinations	4
Reflector Wheel Setting	26
Length of each Cycle (not always this large)	17,576
Total possible encipherments	92,579,782,159,868,838,064,000

Surely, one would say, to take a given message and try each of these 92 plus septillion ways would be impossible. The machine should be unbreakable. It would have been but for the combination of American and British skill on the one hand, and the natural weakness of any machine plus German blunders on the other. The former are discussed in ~~R.I.P.~~s 425 and 450. We now proceed with the latter.

b) The Weaknesses of the Device

The flaws in the Enigma cipher system were twofold:- those inherent in the design of the machine, itself, and those arising from its abuse. For the former the remedy lay in improved design; while for the latter improved rules for use and strict discipline in their application were needed. The German Navy almost completely overlooked both--being, in this respect, less sagacious than their colleagues in the Army and Air Force.

For the present we will confine ourselves to a discussion of inherent flaws only. Those in the usage of the machine, of auxiliary aids (such as underlying codes), and of substitute hand systems will be discussed in later sections of this book.

The first general weakness of the Enigma lay in the combination of the regularity of its motion and the relative brevity of its cycle. Each cycle, if not too long, and if regular, can be examined by taking a copy of the device, or "a reasonable facsimile thereof", and running it at high speed through all its positions, while looking for the "right answer" (a term we will discuss below). We have seen that for Schluessel M each cycle was at most about 17,000 positions long. Furthermore these positions were run through in a most regular fashion, which we must now discuss.

Every time a key on the Enigma was pressed down, it caused a fork shown in Figure 4 to move downward and press its prongs against the bakelite ring on the right of the Fast, Medium and Slow Wheels, and the metal Rings on the left sides of these Wheels. There was no prong for the Reflector Wheel or Reflector; so that these elements never moved. The Fast Wheel moved after every letter enciphered or deciphered. The Medium Wheel moved only when a notch on the left side of the Fast Wheel was in position to accomodate the prong of the Fork. This occurred every 26 letters if the Fast Wheel was any of Numbers I to V, and every 13 letters if the Fast Wheel was VI, VII or VIII. The Slow Wheel moved only if a notch on the left side of the Medium Wheel was in proper position. This never occurred more often than every 150 letters. Consequently, if a cryptanalyst could work with a small enough portion of cipher text, he could with a fair degree of certainty, specify the number of turnovers of the various Wheels throughout that text. We will see below with how little text the Germans enabled the Allied cryptanalysts to work.

Returning to the specific elements of the machine, the first to be considered is the Steckering. Here we find two glaring weaknesses. The first lay in the fact that each Stecker pair was reciprocal. If, going into the machine, key E (5) was plugged to point J (10), then similarly key J (10), was plugged to point E (5). This, as we will note below, was unnecessary, and greatly simplified the problem of designing Allied countermachinery. The second flaw lay in the fact that there were always just six Self Steckers. This made it possible for Allied cryptanalysts to attack otherwise impossible problems.

The Wheels, so far as they formed parts of the electrical maze, had no outstanding flaw, yet having fixed wirings, once captured their inner secrets could be uncovered and were permanently possessed. As part of the means of motion, they were very faulty. The notches on their lefthand sides determined the regularity of motion, and with only one notch each for five out of eight Wheels, and two notches each for the remaining three, very little irregularity was accomplished.

The Reflector Wheel had no basic flaw in its design. Without a sweeping change in the whole principle of Enigma motion, it could not, in any event, be made to move (except manually, as the Japs discovered when they used the device) in less than 650 letters; and the usual message seldom exceeded this length. The fact that it could be set at the beginning of each message was sufficient. It did, of course, share the flaw of all Wheels in having fixed wiring.

The Reflector was largely above criticism, except for fixed wiring.

d) Possible Remedies

In considering what the Germans could have done, and did do, to improve the design of the German Naval Enigma, criticism is based only on failure to make changes which were obviously practical, or which they had been willing to make in other branches of the service.

In regard to modifying the length of the cycle of Enigma, the Germans did nothing and cannot be blamed for so doing. The usual length of the cycle (around 17,000 letters) was more than long enough to insure that the usual message would not run through the whole machine and start in again at the original setting. As to the regularity of the cycle, the German Navy never did realize the real worth of a feature that had been incorporated in the later commercial Enigmas and that was provided on the models supplied to the Japanese:- that of many notches on the left side of each Wheel. To have used this improvement would have meant, at most, issuing new Rings only. Even this would not have been necessary, since the notches could have been cut aboard ship. Failure to take this step immeasurably reduced the number of trials Allied cryptanalysts had to make in testing possible encipherment. See ~~RIP~~. 450 pp 35 et seq.

The most glaring neglect of change occurred in Steckering. As the reader will note from Figure 5, the wires used were of very simple design. There was no real need for them having two plugs at each end. Two wires, each with a large plug at one end and a small one at the other, would have been as easy to manufacture, and would have eliminated the reciprocal characteristic which, again, was of tremendous aid to Allied cryptanalysis. See ~~RIP~~. 450, pp 29 et seq. Similarly, it would have been a simple task to issue 26 such wires and use varying numbers. Nevertheless, in every German Naval Key throughout the War, each device had 10 wires of the type shown Statement is an error. in Figure 5, always producing just 6 Selfs and 10 Pairs. Once, more Allied cryptos were aided by German designers since they were able to reject any tentative solution to a Problem which had the wrong number of Selfs and Pairs.

As previously remarked, no great criticism could be directed against the basic design of the Wheels. It would have been a nasty job to have their wiring variable, in view of their small size and tight construction. However, it was gross neglect not to provide them with more notches.

The original (Beta) Reflector Wheel was badly wired--but with some justification. It was so constructed that when it and the new Reflector were set in the correct position, the result was to reproduce the wiring of the old three-Wheel Reflector. It was this fact which enabled Allied cryptanalysts to recover the wiring of the new combination, even before a copy was captured. However, since the Germans were not then prepared to abandon all three wheel usage, their designers can be excused.

The Reflector shared with the Wheels the flaw of fixed wiring. The German Army and Air Force were sufficiently progressive to prepare and use a pluggable Reflector (Dora). This required the design of an entirely new American cryptanalytic device (Duenna, see ~~R.I.P~~. 450). Fortunately, the German Navy once more erred in self-satisfaction.

e) Summary: It is not be supposed that, by failing to make the improvements suggested above, the Germans were left with an insecure

ORIGINAL

TRANSLATION OF FIGURE NO. 8d

Table of Contents

Part I

Contents	Page	Paragraph
Introduction	5	1-2
Cipher Security	5	3-5
Equipping with Ciphers	6	6-10
Cipher Aids	7	11-15
Keys	8	18-23
Change of Key when Cipher Security is Endangered	9	24-27
Cipher Procedure	10	28-31
Cipher Area	11	35
Key Change	11	36
Use of Cipher and Cipher Procedure	12	40-43

Part II

Secrecy Regulations	13	50-70
Issuing of Cipher Data	17	75-86
Combination of Keys	20	90-95
Change of Key by Catchword	22	100-128
Setting Up and Securing the Cipher Machine	29	130-136
Message Settings	31	140-145
Cipher Areas and Key Changes	33	150-165
Appendix 1.	35	

(Translator's note: The German word "Schluessel" means either "key" or "cipher". Translation depends on the context.)

Figure 8c

device. In the shape in which it was employed by the German Navy, it still provided more than 92 septillion ways of enciphering any given message. It is merely that by correcting the form of Steckers, as suggested, the difficulty of Allied solution would have been immeasurably more difficult; and a similar result could have been attained by use of the Pluggable Reflector. The real crimes of the German cryptographers came in the abuse of the device, and it is this we now discuss.

III - USAGE OF THE MACHINE--GENERAL

a. The "General Regulations for the Enigma" issued to and held by the German Navy during World War II was a 38-page, pocket size pamphlet (No. 31-1), whose cover, table of contents, and introductory page are shown, together with translations, in Figures 8a-f. It is interesting to note that, while it was published in 1941, it remained unchanged throughout the War.

From the viewpoint of this [redacted]. the most interesting portion of Figure 8 is paragraph 3 (Figures 8e and f). In their analysis of the conditions upon which the security of Schluessel M depends, the Germans make no allowance for enemy cryptanalysis. We have already considered at length what the Germans designated as their first hope for security, the construction of the device. The two remaining factors, proper "use" of the machine and of collateral aids, would at first glance indicate that the Germans were on the right track. Had "use" meant what and how keys were prepared and messages drafted, and had this section been well drafted, the Germans would have come much closer to achieving their aim of an unbreakable system.

Such, however, was not the case. Not cryptanalysis, but betrayal and capture, were the thoughts uppermost in the minds of the German High Command. This clearly appears from the fact that the instructions they gave in regard to the machine concerned being orderly, limiting the personnel cognizant of details of enciphering, not photographing the device, and disposing of it and its wheels when capture is imminent. Similarly, the instructions as to Keys and cipher aids are concerned with stowage in safes, destruction when used or no longer needed, and precautions in event of imminent capture. Again, the sections of General Regulations (paragraphs 6-10) relative to "Equipping Ships and Stations", (not shown in Figure 8) with its provisions for careful accounting and close custody, are directed only against betrayal or capture. We will have occasion to note below how little comfort the Allies derived from either betrayal or capture, in contrast with the immense assistance they received from poor cryptography.

b. The next sections of General Regulations (paragraphs 11-15) are those in which are listed the cipher aids for use with the Enigma Machine. They are listed in the order used by the Germans in Figure 9. They were issued to the German Navy in a folder of the type illustrated in Figure 10. A brief consideration of the items in Figure 9, in somewhat other than the German order, will serve as a very satisfactory framework into which to fit the discussion which follows. We can then discuss the items, one by one.

A German U-Boat Skipper to whom had been issued an Enigma, and who wished to communicate with ComSubs or with other vessels, had to be told how to do so. In chronological, rather than in the order given in Figure 9, he would use the various cipher aids as follows. (Numbers refer to Figure 9 items.)

With the machine before him, our Skipper would reach for his General Regulations (Item II,a). In paragraph 90 he would find that his set-up consisted of two parts: Inner (Wheel Order and Rings) and Outer (Stecker and Grundstellung). The Rings and Grund are two terms we have not mentioned heretofore. More of them below. To one who has examined the Enigma, itself, the significance of Inner and Outer should be clear. The Wheels, and the Rings on them, once placed on the machine, are under lock and key. On the other hand, the Stecker wires are not so locked, and the Grund (Basic Setting) is obtained by moving the Wheels by means of the fluted rims which project beyond the locked compartment, through slots provided for this purpose. See Figures 1a and b.

In terms of our previous discussion, the selection of Wheel Order and Stecker amounts to our Skipper choosing the Cycle which he is to set up on his machine. After this has been done, he will want to select a starting point in that Cycle for his particular message.

The actual choice of Wheel Order and Stecker is not free. They are specified for the date in question on a Key Sheet (Item Id), where the Skipper would also find his Rings and Grund. Following the instructions on that Sheet the correct Reflector combination and Wheels would be placed inside the locked compartment, and the ten Stecker wires would be put in the right holes on the outside.

The next step would be to rotate the Wheels to some setting and start punching the keys to encipher his message--using forms to be discussed below. However, as in the case of Machine Settings, the choice of Message settings was not always wholely free. Rules on them were to be found in General Regulations (Item IIa) paragraphs 140-145, in which the main caution is against repetitions. However, in the case of doubly enciphered messages, (Offizier and Stab), used as a precaution against betrayal, there were only 26 Settings available. Furthermore, in Short Signals (used for speed) the Setting had to be selected from a limited list.

The Setting having been selected, the next consideration is how to make it known to the addressee, so that he could decipher the message. As one might imagine, this is where our Skipper made use of the letters on the Rings on his Wheels. One and only one letter on each Ring could be seen through the windows on the locked compartment at any given time. Had the Rings been rigidly attached to the Wheels, there would have been no trouble. The Skipper could just copy off these letters showing through the window at the Setting he selected and use these letters (enciphered in some way) as an Indicator. Since, however, these Rings were free to turn around the rims of the Wheels, the letters in the windows would have no significance unless both originator and addressee had first set their Rings in the same way. It is here that the Key Sheet (Item Id) saved the day. On it, in addition to the Wheel Order and Steckers, was to be found a "Ringstellung" (Ring Setting) for each Wheel used. This setting was accomplished by moving the Ring around the Wheel until the letter given as Ring Setting was opposite the white

ORIGINAL

dot on the left face of the Wheel. Needless to say, this step had actually been taken before the Wheels were placed in the locked compartment. Actually, therefore, the Rings served a twofold purpose. The notches which they carried affected the motion of the Enigma, in the fashion previously discussed; and the letters on them were used as a first step in enciphering the Setting.

We have suggested that the Skipper might merely use the letters in the Windows as an Indicator. He actually did just this in the case of certain Short Signals, mentioned below; but, even to cryptanalytic-oblivious Germans this did not seem sufficiently secure. A further encipherment was necessary. The four letters which told the Setting of the Wheels, reading from left to right, were enciphered on the Machine as already set up. To do this meant, again, having a Setting at which to start. This, too, was found on the Key Sheet (Item Id) as the Grundstellung or Basic Setting. This, of course, was known by all originators holding copies of the same Key Sheet.

This last remark suggests that there might be outstanding more than one Key Sheet for a given day. This was, in fact, true. The type of Key Sheet held depended upon the area in which the originator was operating, or, in the case of shore bases, the area with which communications were to be established. The principle of cipher areas is set out in paragraph 35 of the General Regulations (Item IIa) and the list of actual areas in paragraphs 150-165. Needless to say, our Skipper had not only to indicate the Setting he used, but to discriminate the area in which he was operating. For the present suppose he was in the Atlantic.

[redacted] No. 401

TOP SECRET-ULTRA

SAMPLE OF INTERCEPTED ENIGMA MESSAGE

```
MMA"     0151 / 4/ 370     22

HNMX UOLP FZNM HSNS CENH VHKQ TDEB XMTR GSRK DJPY

XUKW SWED NTET MWVI AUXP XXDK TYQF QBZO DDND ULDA

HNMX UOLP

        0812  F  OM   (Time of Intercept, Fair Text)
                 6790 (Frequency)
```

▨ Transmitting Station

■ Time of Origin

■ Date

■ Serial Number

▨ Group Count

▨ Indicator

Figure No.11

ORIGINAL

We have seen how he got four letters as the encipherment (Indicator) of his Wheel Setting. We next consider how he could get another set of four letters to discriminate his area. To do this he referred to the current Allotment List (Item Ib). This gave each area a series of numbers assigned to it. Let us say the Atlantic at the time in question had 201-300. He then picked any one of these numbers, say 257, and looked it up in the numerical portion of the Indicator Book (Item Ia) and copied out the three letters found there. To them he added a fourth letter of his own choice. He now had two sets of four letters, one indicating his Setting, and the other discriminating his area. This eight letters were once more enciphered, two at a time, by use of the current Bigram Tables (Item Ic) to give eight new letters, which he tacked on to his cipher text both at beginning and end. The next result was a message which, when intercepted, had the appearance of the sample shown in Figure 11.

As we have said, this was the general procedure which held in the Atlantic throughout the War. We will, throughout this book, be mainly concerned with this area, since in it was the principal American assignment. Practices in other areas did not vary from it greatly, and will be the subject of incidental comment.

Actually, all areas had Key Sheets of the same type. The difference was only in number of letters per group of cipher text (either four or five) and in the system of indicators and discriminants. In some non-Atlantic areas the originators enciphered the letters in the windows as the Setting which they selected twice in succession without resetting to ground after the first encipherment (called by the Allies, for cryptanalytic reasons, Throw-On). Those areas in which this was done did not, in some instances, make use of Bigram Tables. However, in nearly all areas the system of discriminants involved selecting one of a series of numbers assigned to the area in question and, in turn, converting that number into letters which were added to the cipher text. The Far Eastern and Blockage Running ships had a system of discriminants which eliminated use of numbers and, instead, simply divided a list of five-letter groups among the various users.

Returning to Figure 9 we see there are still four items which we have not considered. We will consider them briefly before proceeding to a detailed study of the various usages.

We have so far been concerned with the general encipherment of either plain text or code groups, where no special precautions were taken to keep knowledge of the text from the regular cipher personnel. In the Officer and Staff Procedure, (covered in the pamphlet listed as Item IIb), steps were provided to limit such knowledge to the originators and addressees only. This was done by use of special Steckers and Settings, issued on special Key Sheets. A final form of special Key Sheet, designed for the same general purpose were tnose for Sonderschluesseln, referred to in Item IV.

c. Last of all were two pamphlets (Items IIc and III) designed to cover cases where the machine was out of order or where fears of compromise had arisen. The former covered the Reserve Hand Procedure, which, as we shall see, was a scheme of transposition and substitution using paper and pencil only. The latter covered

INNER SETTINGS FOR TRITON KEYS, JUNE 1945

FIGURE I-2 a

Schlüssel M "Triton"

Monat: Juni 1945 Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Allgemein
(Schl.T. M Allg.)

Innere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monats-tag	Innere Einstellung				
29.	B	Beta A	VII G	IV N	V O
27.	B	Beta A	II T	I Y	VIII F
25.	B	Beta A	V M	VI Q	I T
23.	B	Beta A	VI B	II H	III D
21.	B	Beta A	I W	VIII L	II E
19.	B	Beta A	VIII K	I U	IV G
17.	B	Beta A	IV U	VI Q	I H
15.	B	Beta A	VII D	I J	II N
13.	B	Beta A	I O	IV U	VII L
11.	B	Beta A	VI I	I L	II I
9.	B	Beta A	III X	IV C	VII R
7.	B	Beta A	V Z	I U	VIII A
5.	B	Beta A	II E	VI Z	I L
3.	B	Beta A	VIII Y	V F	II C
1.	B	Beta A	IV R	VII A	III X

Achtung! Umkehrwalze und Zusatzwalze beachten!

OUTER SETTINGS FOR TRITON KEYS, JUNE 1945

FIGURE 12 b

TOP SECRET-ULTRA

Schlüssel M "Triton"

Monat: Juni 1945

Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Allgemein

(Schl.T. M Allg.)

Äußere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monatstag	Steckerverbindungen	Grundstellung
30.	18/26 17/4 21/6 3/16 19/14 22/7 8/1 12/25 5/9 10/15	H F K D
29.	20/13 2/3 10/4 21/24 12/1 6/5 16/18 15/8 7/11 23/26	O M S R
28.	9/14 4/5 18/24 3/16 20/26 23/21 12/19 13/2 22/6 1/8	E Y D X
27.	16/2 25/21 6/20 9/17 22/1 15/4 18/26 8/23 3/14 5/19	T C X K
26.	20/13 26/11 3/4 7/24 14/9 16/10 8/17 12/5 2/6 15/23	Y S R B
25.	22/20 12/15 23/25 2/10 7/26 24/14 5/13 11/1 18/3 4/6	C L Z Q
24.	5/9 3/18 17/26 13/11 12/20 1/19 16/6 2/7 15/10 8/4	N E J C
23.	19/24 4/15 7/6 23/20 17/9 5/2 8/10 22/21 18/1 3/14	S X Q Z
22.	8/25 16/12 1/9 10/5 21/14 11/26 17/3 23/15 13/7 2/4	H R T J
21.	2/7 13/10 19/23 15/25 6/9 4/1 18/24 8/3 16/12 11/22	G B C E
20.	17/24 3/15 26/16 8/5 22/12 21/20 19/14 7/1 10/18 4/6	İ H L P
19.	20/10 18/22 1/2 4/13 3/7 16/25 8/11 9/15 23/17 24/26	Z K Y L
18.	11/19 17/13 24/22 14/20 8/1 6/9 18/16 2/5 3/10 12/7	D G E S
17.	23/25 15/20 7/4 17/12 19/18 3/2 10/8 26/24 6/21 9/5	R W U B
16.	12/18 9/3 2/21 11/24 8/16 4/14 22/13 25/19 23/20 5/1	M T P İ
15.	14/17 4/16 25/20 19/21 3/22 10/7 5/9 2/18 15/8 6/1	X A J O
14.	2/3 12/26 11/9 10/1 8/5 15/19 20/24 7/6 16/21 13/14	F N B M
13.	15/23 16/24 5/25 19/6 4/17 7/1 8/13 26/11 2/9 22/10	L J M F
12.	18/10 14/8 2/17 1/24 23/26 16/12 4/19 3/22 7/25 6/5	U Q İ T
11.	13/21 1/16 26/20 8/6 7/22 18/11 17/14 15/9 10/4 12/2	B H V Y
10.	20/15 3/5 14/7 19/12 9/4 25/26 8/2 1/16 24/21 18/23	P Z F A
9.	17/24 19/23 8/25 6/10 18/20 12/7 9/5 13/4 3/1 22/15	J D X W
8.	1/9 5/18 24/22 7/17 21/11 2/16 26/10 20/25 3/14 8/6	E U N K
7.	6/8 17/16 19/10 12/15 4/3 5/20 9/23 2/1 13/26 25/21	G O A U
6.	19/22 20/24 12/16 11/1 21/25 13/18 8/15 3/7 9/14 4/2	V S K G
5.	10/11 2/6 3/18 22/19 9/8 20/12 5/14 17/21 24/16 1/4	K İ O N
4.	22/18 23/13 9/4 10/6 21/14 24/15 19/26 8/1 2/3 7/5	Q R G Z
3.	7/10 3/19 16/11 26/4 5/17 6/2 20/9 21/14 15/12 8/24	N V C H
2.	15/20 18/8 7/21 14/25 22/12 23/11 16/10 13/1 9/2 4/6	A P W V
1.	3/12 22/24 18/26 5/20 9/7 4/1 15/13 6/14 16/10 11/8	W K H L

directions on how to generate new Keys out of those previously issued and on hand.

The various codes which could be reenciphered on the Enigma, including Short Signals, Weather Reports, etc., were enumerated in the Appendix to General Regulations.

IV - FLAWS OF PARTICULAR CRYPTOGRAPHIC AIDS

a) Introduction

There were two principal faults which haunted the German cryptographers throughout the War. The first was a decided abhorrence of complete change, even where a partial change was made and where going the whole way would have involved very little additional effort. The second was a persistent tendency, given a number of possibilities, to run through them in a systematic, rather than a random fashion. Both of these habits were of great help to Allied cryptanalysts.

b) General Key Sheets

These were the same in form, throughout the War in all areas. They were issued in sets of two for each month, in the form shown in Figures 12a and b, one sheet devoted to Outer, and the other to Inner, Settings. In preparing them, as always, the Germans were more conscious of danger from loss by capture, than by cryptanalysis. They printed the sheets with soluble ink, provided for secret teletype reports in the event of known or suspected capture, and ordered that changes in key should be only by secret, written directive, never to be sent by radio. In spite of this they made up the contents in typical "eins-zwei-drei" fashion.

The Inner Settings were those which gave the greatest unnecessary help to the Allies. A glance will show that though the form is constructed with ample room to change the Reflector combination in every entry, it is the same throughout the month. This spotted Allied cryptos odds of 4-1 every time the Wheel Order changed. Similarly, although this does not appear from the single sample shown, the usage of the four Reflector combinations from month to month within a given area and among the various areas during a given month was far from random. Repetitions which chance would give were deliveratel̥y suppressed, and Allied trials thereby eased.

The same faults pervaded the whole scheme of Wheel Order Lists. It was discovered by GYA as early as November 1943 that the German clerks preparing Wheel Order Lists had four very pronounced habits:

a) Not to repeat the identity of Medium or Fast Wheel in preparing successive Wheel Orders;

b) Not to repeat a full Wheel order over a given period;

c) To use each Wheel only once in the slow position before any one is used twice;

d) To follow each Wheel, when used in the Slow position, by the other Wheels in a fixed order of preference. <u>Figure 12a</u> illustrates all of these tendencies to a varying degree.

The reader will realize that the sheet is to be read from bottom to top, in chronological order.

a) In <u>no</u> position is any Wheel used twice in succession, although chance would produce about five cases.

b) There is no full wheel order repeated, although there is a 2 out of 3 chance that there would be one if the list had been prepared in true random fashion.

c) In the Slow position each Wheel is used just once before any one is used a second time. None are used three times. Again, quite unlikely by chance.

d) The tendencies of using Slow Wheels in given order is one which cannot be accurately observed in a single month.

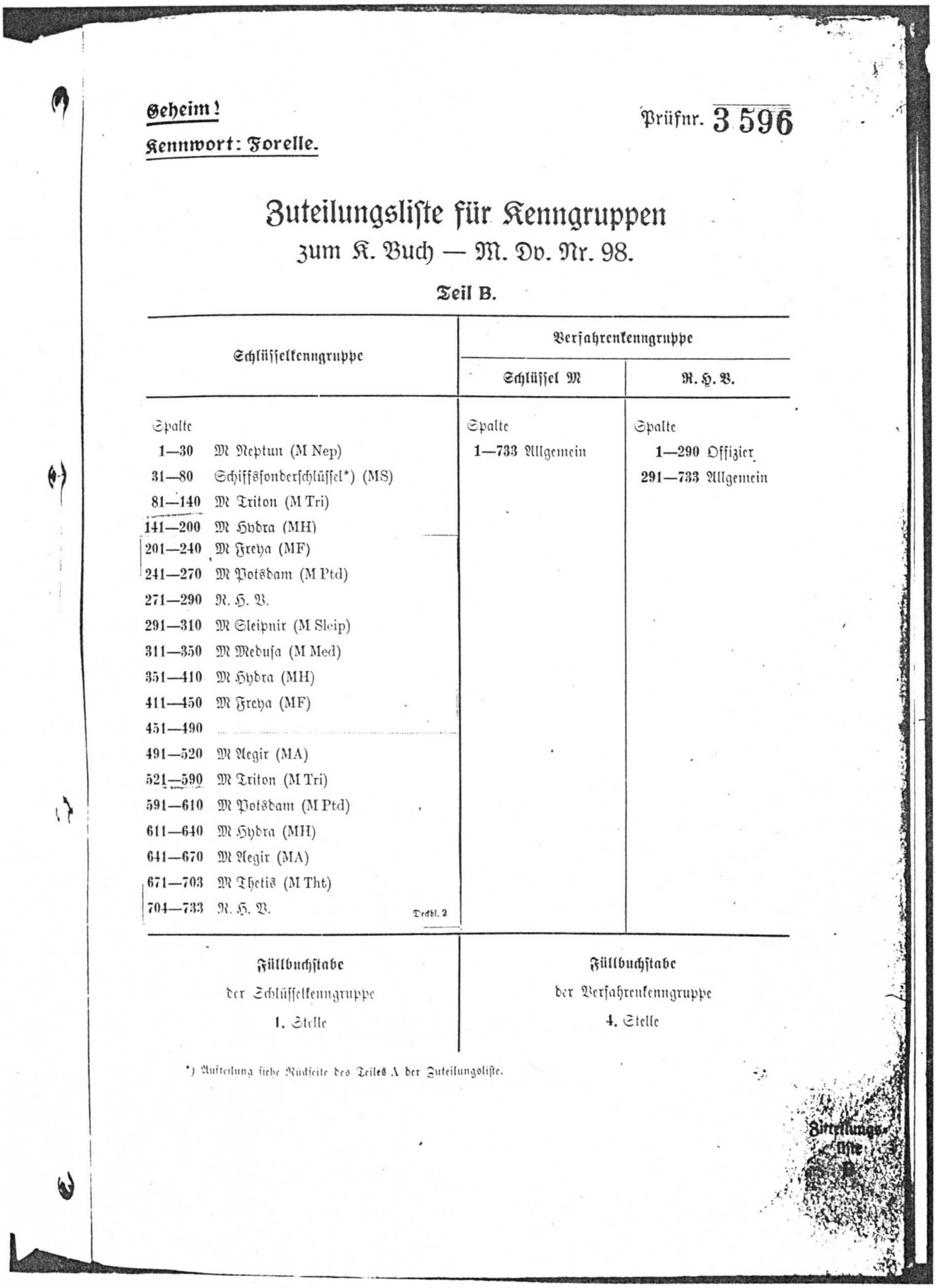
The technique of profiting from these German errors is discussed at length in ~~R.I.P.~~ 450, pps 276-279. The net result, as explained in ~~R.I.P.~~. 425, was to cut the work ~~which~~ of Allied cryptanalysts in half--or, conversely, to get double work out of their machinery and personnel. This crime of cryptography was one which the Germans committed in every cipher area, thus continually spotting the Allies odds of 1 to 2.

The Rings were also systematically made up by the German cipher clerks. The reader will note in Figure 12a that, although several would be expected, there are no vertical or horizontal repeats of adjacent letters. However, although another instance of faulty practice on the part of the Germans, no particular aid or comfort was given the Allies thereby. Actually, the recovery of Rings never presented a very great problem. However, there was one bit of stupidity or inertia in German cryptographers which was never explained. That was their persistence in not using the Ring on the Reflector Wheel except as an experiment in the closing days of the War in the Mediterranean. The reader will note that the letter under Beta is always A in Figure 12a. As a result, Short Signal traffic remained a three-, rather than a four-, Wheel problem and the Allies were here spotted odds of 1 to 26.

Turning to Figure 12b, we come to Steckers. We have several time heretofore mentioned their main weakness--the constant use of six Selfs. This, as we have seen, was of no direct help. Itdid cut down the number of possible Steckers, but the number remaining (over one hundred and forty trillion) was so great that it was necessary to devise an electrical circuit, discussed in ~~R.I.P~~. 450 that would te~~x~~st all reciprocal Steckers in the flash of a current. However, this test often suggested more than one (but very few) possible solutions. These could be further culled on the basis of the number of Selfs. We can, therefore, acquit the Germans on all but the "six-self" count.

The grunds were also systematically constructed in many cases, of which those in Figure 12b are an example. In each column it will be seen that there are 22 letters which each occur once and only once, while the remaining four each occur twice. This is not a random selection. However, as in the case of the Rings, grunds were usually so easy to recover by rapid "try-everything" methods, that little comfort was derived from their systematic construction.

As we have mentioned, the Germans stand indicted here, as elsewhere, on two charges: failure to construct random keys, and failure to make changes intelligently (sweepingly). These two Key Sheets (Figure 12a and b) show this quite well. They show on their face how the Reflector combination remained fixed for a month while the remaining Wheels changed every two days. They also illustrate the general German rule that a given Wheel order would span at least two Steckers. Later, in the discussion of areas, we will see that in some cases the span was even greater. The only attempt to arrange



Geheim!

Kennwort: Forelle.

Prüfnr. 3 596

Zuteilungsliſte für Kenngruppen

zum K. Buch — M. Dv. Nr. 98.

Teil B.

Schlüſſelkenngruppe	Verfahrenkenngruppe	
	Schlüſſel M	R. H. V.
Spalte	Spalte	Spalte
1—30 M Neptun (M Nep)	1—733 Allgemein	1—290 Offizier
31—80 Schiffsſonderſchlüſſel*) (MS)		291—733 Allgemein
81—140 M Triton (M Tri)		
141—200 M Hydra (MH)		
201—240 M Freya (MF)		
241—270 M Potsdam (M Ptd)		
271—290 R. H. V.		
291—310 M Sleipnir (M Sleip)		
311—350 M Meduſa (M Med)		
351—410 M Hydra (MH)		
411—450 M Freya (MF)		
451—490		
491—520 M Aegir (MA)		
521—590 M Triton (M Tri)		
591—610 M Potsdam (M Ptd)		
611—640 M Hydra (MH)		
641—670 M Aegir (MA)		
671—703 M Thetis (M Tht)		
704—733 R. H. V. Deckbl. 2		

Füllbuchſtabe der Schlüſſelkenngruppe	Füllbuchſtabe der Verfahrenkenngruppe
1. Stelle	4. Stelle

*) Aufteilung ſiehe Rückſeite des Teiles A der Zuteilungsliſte.

Zuteilungs-liſte B

CIPHER ALLOTMENT LIST FOR INDICATOR BOOK - COVERWORD "FORELLE"

FIGURE 13

NAME OF ALLOTMENT LIST	DAY/MONTH IN EFFECT
Zuteilungsliste (Appendix to K-Buch)	29/11/41
Forelle	10/ 2/43
Zander	7/11/43
Haifisch	1/ 2/44
Dorsch	21/ 4/44
Hering	20/ 6/44
Zander	10/ 8/44
Forelle	15/10/44
Haifisch	30/12/44
Hering	4/ 3/45

EFFECTIVE DATES OF ALLOTMENT LISTS

Figure 14

for more rapid changes was one that never was tried in the Atlantic. During the last month of the War the Mediterranean users had a table of grunds that changed from message to message. Considering the number of messages sent per day, it is easy to understand that the American and British tasks would have been tremendously more difficult had this practice been more generally used. Actual contents of the Key Sheets recovered or captured are to be found in ~~R.I.P.~~ 475.

c) The next Cipher Aid which our mythical Skipper used was the Allotment List. This was a single sheet of the form shown in Figure 13, (Library 86) with English equivalents of the various terms interlineated. It is to be observed that in this case the Atlantic U-Boats, which operated in what the Germans called the "Triton" area would use numbers from 81 to 140 or from 521 to 590 as discrimimants. The significance of the other covernames will be discussed below.

The construction of this Table shares the common fault of undue system. Instead of scattered, random numbers for each Key, consecutive blocks were used. As a result if the Bigram Table for a given day was known to be one, but not which, of a current set, of ten, all of the set could be tried in succession until the one giving grouped numbers for all the traffic in a given area was found.

In all, the Germans had five different Allotment Lists, named and used as shown in Figure 14. Comparing this with the similar schedule for the use of Bigram Tables, shown below, one finds another case of the Teutonic habit of gradual change--in that all five tables were used while the same Bigram Table (Muendung) was in use.

	721	722	723	724	725	726	727	728	729	730
1	JUA	EBO	SSJ	NHC	YJM	VFY	KTİ	ADU	GWE	OFS
2	NAG	KNL	XRİ	ZSY	UWC	QUM	FEB	DAK	BTM	QEO
3	YLH	AFG	OKZ	WBS	PEA	MVN	CXO	HKE	İGN	LQA
4	RYG	GAR	CCK	SFY	HXS	İEP	LOH	JOD	NOİ	FAD
5	VMC	MLX	İAQ	JJC	BYJ	DXG	PVK	OGP	YSN	AİQ
6	LCY	QGD	NST	EWK	FSZ	RKR	TWN	MJC	UPQ	DWL
7	BFP	ZQA	UİH	KVB	LHP	YEH	VİC	TEW	OZJ	İUD
8	FXK	TVL	WGM	ALG	QİV	GYQ	XAW	ZVK	SMA	VXV
9	PST	OMY	HUD	İTU	ZRC	CQU	RFN	WTB	JNR	PUH
10	TJN	JZP	EİV	QON	SCQ?	ATW	İRİ	RSX	FPX	XJP
11	WQT	CTW	BQT	XGU	NXİ	KMM	DPJ	LFA	MBT	UAV
12	HFZ	İJR	MYF	UXF	GFT	PİF	JİP	CLU	WFG	KZP
13	DBR	PBV	TPR	OUA	AMJ	ZHO	QLF	GRH	RVU	EHT
14	MTU	YXB	ZTE	FZF	DGW	WOA	UDV	SHS	HCF	BNH
15	SNQ	UEZ	VVB	BCN	JVT	NDJ	YNT	XXH	EJO	WEJ
16	İPX	LRD	PDL	HQL	WKL	FJB	MUA	UYT	KRH	NTB
17	COV	XDE	JFN	VRJ	TQD	BWV	AHG	NCO	ZES	SOF
18	AYE	RUX	GHM	CKU	OPX	LAY	ESZ	İWQ	XKB	YFL
19	KHY	DYP	RND	MAW	ENQ	TUZ	GLF	VBM	QSY	HLK
20	UZQ	BOF	KLW	TNH	İOY	JYL	SZT	YQP	DZL	CRB
21	ZGH	HOİ	YYS	PJK	CBG	EDC	WMD	QNX	ANC	GDİ
22	ODX	NPO	FRQ	GMW	RZK	UMS	ZKİ	KCE	LXE	MKR
23	XWB	SKT	ABO	LİA	VPE	OSN	NQS	FLG	VYB	RRD
24	EMP	WWN	QZL	DER	MCO	XBZ	HBY	BGW	PMJ	TDQ

	731	732	733
1	WZM	LLX	CYU
2	SAE	OBS	MNİ
3	NKT	VUC	QPA
4	PYE	YTL	THP
5	KJO	RCR	XQX
6	HZU	İDM	KWF
7	BİH	FWQ	PLX
8	DMV	AXF	ETV
9	JDW	KFO	
10	RGR	TKU	
11	YHZ	ZOJ	
12	UJS	PRB	
13	LVX	CUL	
14	FOM	HVZ	
15	CER	NYY	
16	APM	EPW	
17	GVZ	BAİ	
18	OQY	WHG	
19	XSG	UGK	
20	QBA	MQC	
21	ZCD	DİC	
22	VGK	JXN	
23	İİG	XMV	
24	ECR	SUZ	

SAMPLE PAGE PART I - K-BUCH (NUMERICAL)

FIGURE 15b

Since, given the Bigram Tables and the Kennbuch (which never changed), one could easily find the numbers assigned to any given area, the security value of changing Allotment Lists was minimum.

d) The next Cipher Aid which was used in enciphering the sample message was the Kennbuch. Its cover is shown in Figure 15a. Internally, it was divided into two sections, one numerical, of which a sample page is shown in Figure 15b, and the other alphabetical, shown in Figure 15c. In enciphering the discriminant, use would be made of 15b. The whole publication is to be found in the Section Library as Nr. 86 . It will be recalled that our Skipper would have made use of the numerical section in arriving at his Key Discriminant. Having selected any number in the span allotted to his area, he would find that there were 24 possible trigrams which he could substitute for it, and would pick any one which suited his fancy. At the other end of the transmission, the addressee would consult the alphabetic section and arrive at the number the Skipper had selected. This would be found by the Addressee to fall in the Atlantic Allotment.

The Kennbuch is one of the few German cryptographic documents which was never found to have any useful defects in construction. Its flaw lay in usage--since it was never changed in the whole duration of American participation in the War. Having been supplied with a copy by the British early in the game, American cryptanalysts were never faced with any problem as to this phase of Key Discrimination.

We have previously remarked that not all areas used the Kennbuch. The Southern (Sud) areas had a Discriminating System, based on a Kenngruppetafel, rather than a Kennbuch, which we shall encounter below in the discussion on the Reserve Hand System (Henno) in that area. In principle, however, the Discriminants were similar, in that, for numbers assigned to the various Keys in the Sued group, one substituted letters. In the Far Eastern Areas the keys (except for Aegir) used a table of random five letter groups assigned as Discriminants.

In neither case did these irregular discriminants afford any particular security. Most of the Kenngruppetafeln and all of the five-letter Indicators eluded capture throughout the War; yet the Allies had no difficulty in sorting the traffic by external characteristics, such as serial number, frequency and number of letters per group.

e) The final Aid employed in our hypothetical transmission was the current Bigram tables. These were always issued in sets of ten, named as sets and effective as follows:

Bach	- Brook	in effect	1 July 1940	
Fluss	- River	"	15 June 1941	
Stroem	- Stream	"	1 Nov. 1941	
Muendung	- Mouth	"	1 Mar. 1943	
Quelle	- Source	"	16 July 1944	
Meer	- Sea	distributed	May 1945	(never used)

A sample cover, calendar (see below), and portion of one table in a captured reserve set (Teich, "Pond"), which was never issued, are shown in Figures 16a, b and c. The tables actually used are found in the Library, No. 74.

Since, at any given time, there were a whole set of tables in effect, it was necessary for all originators to know which particular table to use at what time. This information was supplied by a calendar accompanying the Tables (Figure 16b).

ORIGINAL

The construction of these Tables show more than usual sloth and short sightedness. What was required from them was merely that the set of 676 different plain digraphs be substituted one-for-one into a similar set for cipher. This could, and should, have been accomplished by placing the 676 possible digraphs into a hat, pulling them out one by one and writing them down in the right hand columns of Figure 16c. Instead of this, the Germans cut their job in half by making all tables reciprocal. For example, in Figure 16c we see that AG = FD and FD = AG, DB = FT and FT = DB, etc. Thereby, the work of the Keymaker was cut in half, but the price paid was considerable in the assistance given the Allies in their work on the Muendung Set. Although the breaking of individual messages and recovery of their Settings only supplied data for one half of the Bigram Table (i.e. that dealing with Indicators), the reciprocal nature of the Tables enabled Allied cryptanalysts to reconstruct the other half (the Discriminants) and thus work into the numbers in the Allotment Lists.

The principal faults in the policy for using Bigram Tables were in regard to infrequency of change of Sets, and the continuance of a single set through the life of several Allotment Lists. Both can, perhaps, be excused on grounds of difficulty of distribution. The change of individual tables on a daily basis seems to have been adequate. The actual users, however, supplied a minor and indirect break.

It will be recalled that the Kennbuch gives only three letters for an Allotment number. The originators were instructed to add a fourth letter. Being provided with no means of making this choice

OFFIZIER KEY SHEET FOR JUNE 1945

TOP SECRET-ULTRA

FIGURE 17a

Schlüssel M "Triton"

Monat: Juni 1945 Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Offizier
(Schl.T. M Offz.)

I. Äußere Einstellung

Wechsel 1200 Uhr D.G.Z.

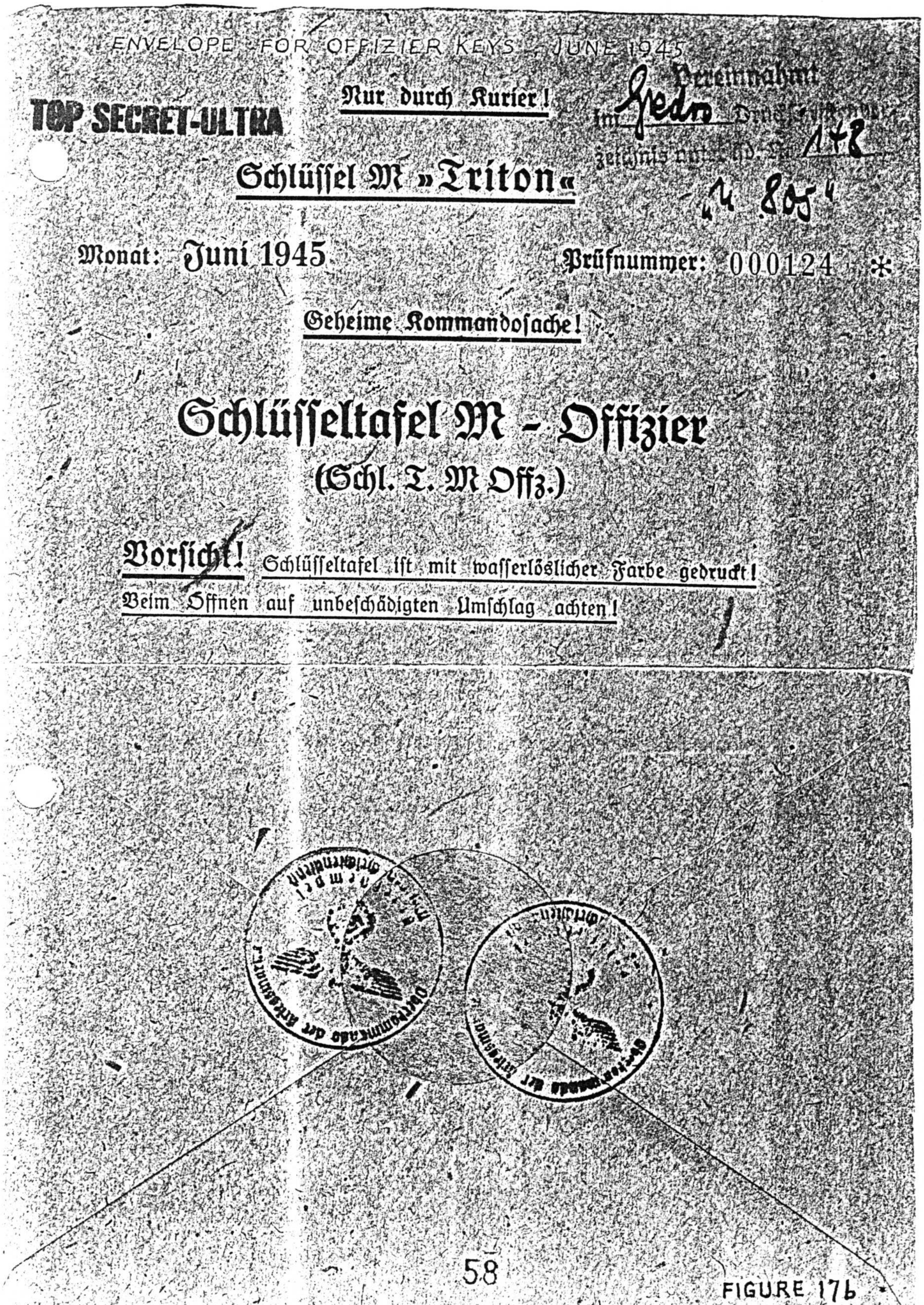
Spruchschlüssel:

Anton	= O M J Y	Jot	= S Q R U	Sophie	= R O K L
Bruno	= X Z E D	Karl	= W E W N	Toni	= K W U B
Cäsar	= H G D T	Lucie	= E N U C	Ulrich	= N F O P
Dora	= T S Y J	Max	= J B G M	Viktor	= D U C X
Emil	= B L P G	Nanni	= P T F S	Wilhelm	= Z D L U
Fritz	= N J M E	Otto	= C H Q R	Xant	= Q R İ Z
Gustav	= İ U S Q	Paula	= Y X H F	Ysop	= U Y X İ
Hans	= U A N A	Quatsch	= M C T W	Zet	= L K B A
Ida	= G P A O	Richard	= F İ Z K		

Monatstag	Steckerverbindungen
21.-30.	1o/15 23/26 11/2 20/24 7/3 9/16 17/12 18/21 22/25 8/5
11.-20.	4/25 18/24 3/10 8/6 22/26 2/21 20/5 14/19 16/11 13/7
1.-10.	3/2 13/5 23/19 21/14 7/1 17/15 18/12 9/24 8/10 26/20

II. Innere Einstellung: Als Innere Einstellung ist die Innere Einstellung M - Allgemein "Triton." für den Monat Juni 1945 anzuwenden.

ENVELOPE FOR OFFIZIER KEYS - JUNE 1945



TOP SECRET-ULTRA

Nur durch Kurier!

Vereinnahmt
im Gedo Druckſachenver-
zeichnis unter lfd. Nr. 148
„N 805“

Schlüſſel M »Triton«

Monat: Juni 1945

Prüfnummer: 000124 *

Geheime Kommandoſache!

Schlüſſeltafel M - Offizier
(Schl. T. M Offz.)

Vorſicht! Schlüſſeltafel iſt mit waſſerlöslicher Farbe gedruckt!
Beim Öffnen auf unbeſchädigten Umſchlag achten!

Oberkommando der Kriegsmarine

Oberkommando der Kriegsmarine

FIGURE 17b

random, they displayed marked tendencies to favor certain letters. One could tell the Bigram Table used, since it, and only it, would show up these tendencies when used to break out the enciphered dummy letters.

f) So much for the Cipher Aids used with general messages in which plain text was enciphered. We proceed next to the type of message of which the contents were to be restricted to selected individuals. These were what the Germans called Offizier (Officer), Stab (Staff), or Sonder (Special) Keys. In all these cases the message was first enciphered by one of the selected individuals. The resultant text, together with an Indicator written in plain text, was given to the regular communications personnel for re-encipherment on the regular Keys for the day. The addressee's radio personnel would break the message out, in full. Finding that they had one of the special Indicators ("Offizier" or "Stab" followed by a phonetic letter, or "Sonder" followed by a number and letter) and then gibberish, they would give it to the selected personnel for the second decryption needed to turn the gibberish into legible text.

The Aids needed for this limited traffic were Key Sheets of the type shown in Figure 17a, issued in envelopes of the type shown in Figure 17b. From the instructions at the bottom of the Sheet, it will be noted that the preliminary encipherment was done with the Daily Inner Settings (Wheel Order and Rings) but with a Stecker that changed three times during the month. Twenty-six Settings are provided. The originators are cautioned against using the same setting twice in a month. Full instructions are contained in the "Enigma Officer and Staff Procedure) Library No. 34. It is interesting to

66

note that no Staff messages were sent in the Atlantic traffic until January 1944, when Control prescribed use of normal Offizier procedure with special Settings and heading. Actually, this was precisely what was done in all areas. A typical form for such a message is shown in <u>Figure 17c</u>, sent from Group West to Fleet COMINCH using Setting C. English equivalents are shown for the German terms used in the Enigma General Procedure(Library No. 32.)

Analysis of the sample Key Sheet will show its obvious flaws, which in this case were not as flagrant as in some. The steckers, of course, shared the common fault of being reciprocal and always containing just six Selfs. There seems to have been no excuse except for sloth, in only changing them three times a month. Actually, prior to August,1943 , they had changed every two days in the Atlantic. On the other hand, in the Naval Attache traffic, no special Steckers whatever were supplied--merely special Settings.

It is in these Settings, however, that the real harm was done. In that only 26 were provided for a month, it was almost inevitable that, while individual originators might avoid repeats, someone was sure to use, during the second and third periods of each month, one or more Settings which someone else had used before. As soon as this occurred, the process of recovering the new Stecker was a relatively simple process--as discussed in ~~R.I.P~~. 450.

More than this, as always, the Settings were never mutually random. In the sample it will be noted that for the Reflector Wheel A is not used, one letter (N) is repeated, and all others occur just once. This was nearly always the case (see ~~R.I.P~~. 475). In numerous cases the error was even more glaring. The absence of repeats was

LIST OF SPECIAL (SONDER) KEYS ISSUED

Sonder No.	U-Boat	Skipper	Sonder No.	U-Boat	Skipper
7	U-309	Loeder	239	U-907	Cabolet
9	681	Gebauer	240	1017	Riecken
44	650	Zorn	241	1051	Holleben
47	764	VonBremen	244	1208	Hagene
60	285	Bornhaupt	245	1014	Glaser
64	857	Premauer	246	1058	Bruder
79	190	Reith	247	1203	Seeger
109	978	Pulst	249	927	Ebert
110	1004	Hinz	250	868	Turre
111	483	Morstein	251	327	Lembke
113	1199	Nollmann	252	683	Keller
118	1064	Schneidewind	253	1279	Falke
136	979	Meermeier	254	1019	Rinck
139	296	Rasch	255	2322	Heckel
143	248	Loos	256	879	Manchen
144	482	Matuschka	257	1302	Herwatz
154	548	Pfeffer	258	1104	Perleberg
161	St. Nazaire	U-Base	259	878	Rodig
173	866	Rogowski	260	1278	Mueller
200	245	Schuhmann	261	399	Buhse
206	1003	Struebing	262	873	Steinhoff
207	1230	Hilbig	264	953	Werner
209	1007	Raabe	265	1021	Holpert
211	722	Reimers	266	1169	Goldbeck
213	773	Baldus	267	260	Becker
214	1009	Zehle	269	249	Kock
215	1202	Thomsen	270	1015	Boos
216	806	Hornbostel	271	1005	Lauth
217	1232	Dobratz	274	714	Schwebky
218	775	Taschenmacher	275	530	Wermuth
219	870	Hechler	276	1024	Gutteck
223	1276	Wendt	282	242	Riedel
224	1020	Eberlein	401	La Pallice	U-Base
226	485	Lutz	702	313	Schweige
227	297	Aldegermann	709	668	Eickstedt
230	1233	Kuhn	713	315	Zoller
231	1172	Kuhlmann	715	965	Junverzagt
232	1055	Meyer	716	995	Hess
236	325	Dohrn	725	739	Kosnick
237	1018	Burmeister	726	278	Franze
238	825	Stoelker	853	853	Froemsdorf

Figure 18a

TOP SECRET-ULTRA

SPECIAL (SONDER) KEYSHEET

Schlüssel M " N i x e "

FIGURE 18b

Gültig für alle Monate

Prüfnummer: 1

Geheime Kommandosache!

Sonderschlüssel Nr. 1024

Wechsel 1200 Uhr D.G.Z.

Ausgegeben an U.Boot
U. ....

I. Äußere Einstellung

Spruchschlüssel:

Anton	=	U Z N W	Jot	=	H V Y L	Sophie	=	L E K G
Bruno	=	P F S C	Karl	=	R K C H	Toni	=	Y O B K
Cäsar	=	I R F M	Lucie	=	T B P R	Ulrich	=	E J Q S
Dora	=	M L W V	Max	=	G S M A	Viktor	=	Q T J F
Emil	=	C X O B	Nanni	=	O N H N	Wilhelm	=	K D T J
Fritz	=	K G E Q	Otto	=	D A U E	Xant	=	X W A O
Gustav	=	B Y V X	Paula	=	W Q D P	Ysop	=	F I Z T
Hans	=	V M X D	Quatsch	=	Z H R Y	Zet	=	S P L I
Ida	=	N U G Z	Richard	=	J C I U			

Monatstag	Steckerverbindungen
1. -10.	10/8 9/11 15/18 17/21 20/16 6/14 3/4 7/19 5/2 1/12
11.-20.	14/18 5/17 4/7 12/13 8/16 2/11 9/10 19/15 20/21 3/6
21.-31.	2/20 13/11 12/10 14/4 9/17 16/8 6/18 5/7 3/19 1/15

II. Innere Einstellung

Monatstag	Innere Einstellung				
1. -10.	B	Gamma A	IV A	I D	VI G
11.-20.	B	Gamma A	I T	VI V	II P
21.-31.	B	Gamma A	VI S	V F	VII Q

Beachten: Erst auf Befehl 2./Skl BdU op oder OKM 4/Skl II vernichten.

TOP SECRET-ULTRA

SPECIAL (SONDER) INSTRUCTIONS

FIGURE 18b

Merkblatt

über

Anwendung der Sonderschlüssel M "Nixe"

1.) Die Sonderschlüssel M Nixe sind auf Befehl des OKM 2./Skl BdU op ohne besondere Ankündigung anzuwenden.

2.) Der Sonderschlüssel M Nixe dient dem Nachrichtenaustausch zwischen BdU und einem Boot, ohne daß andere Boote und andere Kommandos mitlesen können.

3.) Jedes U.Boot hat seinen eigenen Sonderschlüssel mit einer laufenden Nummer, mit dem außer dem Boot nur Landstellen in der Heimat ausgerüststsind. Erforderliche Mehrausrüstung wird vom OKM befohlen.

4.) Mit einem Sonderschlüssel M Nixe verschlüsselte Funksprüche werden in zwei Arbeitsgängen verschlüsselt.

Im ersten Arbeitsgang durch Offiziere,

im zweiten Arbeitsgang durch die Funkmannschaft.

5.) Der erste Arbeitsgang entspricht dem Verfahren M Offizier und M Stab gem. M.Dv.Nr. 32/2 mit folgenden Abweichungen:

a) Die Innere und Äußere Einstellung sowie der Spruchschlüssel sind dem Sonderschlüssel zu entnehmen.

b) Statt des Wortes "Offizier" bzw. "Stab" ist das Wort "Sonder" mit der nachfolgenden Nummer des zum Verschlüsseln angewandten Sonderschlüssels M Nixe einzusetzen.

Beispiel:

$\underbrace{\text{uuu eins eins neun}}_{\text{Anschrift}}$ von $\underbrace{\text{bduuu}}_{\text{Unterschrift}}$ $\underbrace{\text{sonder eins eins } \overset{\text{nul}}{\cancel{\text{zwo}}}}_{\text{Sonderschl. Nr. 11 02}}$, $\underbrace{\text{caesar}}_{\text{Spruchschlüssel}}$,

6.) Im zweiten Arbeitsgang ist die im ersten Arbeitsgang verschlüsselte Nachricht wie ein Funkspruch nach Verfahren M Offizier und M Stab gem. M.Dv.Nr. 32/1, Zffrn. 81 ff, zu behandeln.

OKM 4/Skl IIcc 140/45 g.Kdos.

NOTES ON USE OF SPECIAL ENIGMA CIPHERS "NIXE"

1.) Special enigma ciphers NIXE are to be used at the order of OKM 2./Skl BDU op without special notice.

2.) Special enigma cipher NIXE serves for the exchange of communications between BdU and a boat without allowing other boats and other commands to read the messages.

3.) Each U-Boat has its own serially numbered special cipher, with which, in addition to the boat, only shore stations in the homeland are provided. Any necessary additional equipping will be ordered by OKM.

4.) Radio messages enciphered with a special enigma cipher NIXE are enciphered in two steps.

The first step by officers.

The second step by the radio crew.

5.) The first step corresponds to the procedure for enigma Offizier and enigma Stab as per M.Dv.Nr. 32/2, with the following differences:

a) The inner and outer setting, as well as the message setting, are to be taken from the special cipher.

b) Instead of the word "Offizier" or "Stab", the word "Sonder", followed by the number of the special enigma cipher NIXE used in encipherment, is to be inserted.

Example:

uuu one one nine	from bduuu	sonder one one zero two	east
Address	Signature	Special cipher Nr. 1102	Message Setting

6.) In the second step, the communication which has been enciphered by the first step is treated as a radio message according to the procedure for enigma Offizier and enigma Stab as per M.Dv.Nr. 32/1, paragraphs 81 ff.

OKM 4/Skl IIcc 140/45 Secret

Figure 18d

found in the Settings for all Wheels; and in other than the Reflector Wheel, A was used. The degree to which this simplified the problem of recovering settings toward the end of a month can be easily seen. Suppose 22 of them had been recovered. But for the non-repeating scheme used by the Germans, each of the remaining four would mean 26^4 or half a million tries. Instead, with no repeats, the tries would only be: for the 23~~,~~rd $4^4 = 216$; for the 24~~,~~th $3^4 = 81$, for the 25~~,~~rd $2^4 = 16$; and the last would be unique.

Similar to the Offizier and Staff procedure, and set up for the same reason, were the Sonderschluessel. Although the two principal ones, used by beleagured Fortresses, were broken by Allied cryptanalysts, no wartime Keysheets were captured. While only two wartime keys were broken, the list of those issued was obtained from reading the German traffic. It is shown in Figure 18a. The one shown in Figure 18b, with accompanying instructions, Figure 18c, and translation thereof, Figure 18d, were surrendered by U-234 before she was able to deliver them to the Far East.

As stated in paragraph 2 of the Instructions, the purpose of these ciphers was merely to achieve "compartmentation" in the German Navy. Certainly as a means of security against enemy cryptanalysis, they were filled with faults. One notes at once that they were "good for all months". Pure sloth, since they could have been issued with regular keys. In the next place, they carried to the illogical extreme the non-repetitive system noted in the Offizier example. In this case each setting of each Wheel was used just once except for the one repeat in the Reflector Wheel necessitated by avoiding A. The Steckers, as always, had six Selfs, were reciprocal, and only

TOP SECRET-ULTRA

changed three times a month. The Wheel Orders had the same fault of only tri-monthly change, and, incredibly enough, although the Reflector combinations were not that of the General Keys, all three were the same. Finally, the possibility of varying the Ring on the Reflector Wheel was again overlooked.

g) Key Changes were Compromised.

The above concludes the discussion of cipher aids as such. From it we can see how the Germans tossed security factors away and into the Allies' lap with a free hand. However, it is not to be inferred that they had thereby completely ruined the device. The most favorable situation which Allied cryptanalysts faced as a regular routine was that which was faced every other day, where the Wheel Order was known to be the same as the day before, but Setting and Steckers were unknown for every message. Here was still a problem involving 26^4 230, 230 x 684,729,075 trials. Even this was further cut down by the second form of German malpractice, discussed below under the topic of "Handling Text". Before reaching that we shall wish to consider the handling of Cipher Aids where security is endangered under such circumstances as shown in Figure 19. One straightforward and conventional method, used by all Navies, was the "Reserve on Board" method.

If the keys valid at any given time were no longer considered secure, then the keys for the next period were put into effect by order of High Command. If this was not possible, then the second alternative was used. The keys were changed by the Catchword Procedure. It is interesting to note at this point that this procedure was first considered an emergency measure, but it later became standard practice.

The Catchword Procedure consisted of three separate parts. The first was the catchword itself, which is a covername for the procedure and is the name of a star or constellation (Andromeda, Bellatrix, Venus, etc.). The second was the Catchword Orders (Stichwortbefehl) which told when a change was to be made. The third part, the Slideword (Kennwort) was a number or a word which gave the actual changes that were to be made in the Keys which would otherwise have been used.

One of the "number" type Catchword systems was that of Bellatrix (a star) used on the Atlantic Submarine (Triton) traffic. The typical case of the Key change which occurred on November 15, 1943, will illustrate the procedure. The U-boats had been issued Wheel Order B-10-714, Ringstellung ZOHT and Steckers A/A, B/F, C/C, etc., as the keys for that day. ComSubs issued an order "Stichwort Order Bellatrix 1336 effective 15 November". By previous instruction the U-boat skippers knew what to do. They looked up 13°36' in their five place navigational tables and took the last three digits of the logtan - in this case, 3,6, and 8. The first digit was added to the Slow, Medium, and Fast Wheels - giving 10, 4, 7. Ten being equivalent to 2, modulo 8, and the Reflector being unchanged, the actual Wheel Order became B-10-2-4-7. The second digit, 6, was added to the three right hand rings, giving ZUNZ. The last digit, 8, was added to all Steckers, giving I/I, J/M and K/K instead of A/A, B/F and C/C. For a discussion of the similar number systems on other keys, see [redacted]. 475, pp. 42-43.

The "name" systems were very similar. They used plain German words (Kennworter) after the Catchword (Stichwort). As an illustration of this, we have the change introduced in Steinbock keys on

17 September 1944. There ComSubs had ordered a change in accordance with the Kennwort, BOHNE. Converting the letters of this word into numerical equivalents, we get 2-15-8-14-5. These were applied as additives to the elements of the originally issued keys as follows:

Letter #1 of slideword (2) added to each wheel (Modulo 8)
Letter #2 " " (15) " " slow " ring
Letter #3 " " (8) " " middle " "
Letter #4 " " (14) " " fast " "
Letter #5 " " (5) " " each letter of plug connections (Stecker).

If the Slideword consists of three letters, as opposed to the normal five, it is handled as follows: Apply the numerical value of the first letter to each Wheel in the Wheel Order, the second letter to each Ring and the third letter to each Stecker. If the Slideword contained an umlaut, the umlauted letter was equal to two letters, (ü - ue, ä - ae, etc.).

Full rules for the classification, distribution, stowage and handling of Catchword Orders are set out in the General Regulations for the Enigma, paragraphs 100-128. The particular catchwords used in each Cipher Area are to be found following the Keys for that area in ~~R.I.P.~~ 475.

There is no major criticism to be directed against the principle of the Catchword. If one has no reserve on board, and distribution of new keys is impractical, no alternative remains but to generate new material from old. However, the means of generation could have been more thorough. Wheel Order and Stecker were all that really mattered for Allied cryptanalysts, and for these, with one slide for all Wheels and one for all Stecker pairs, there were only 8 x 26 = 208, new Keys which could be generated from the old; supposedly compromised ones. By the simple expedient of having a separate Slide for each Wheel, and rules to provide against using the same Wheel twice, the number of possible new Keys could have been increased by a factor of 42. Had the German crypto clerks been willing to meddle with the Sacred Cow, the Reflector Combination, an additional factor of 3 could have been gotten.

The Catchword procedure, moreover, like all other German Naval systems, was mishandled. Originally intended as an emergency method, it became a routine practice after Allied successes at sea began to inspire a fear of treason, rather than cryptanalysis. The result was that when "Venus" was introduced at the time of the invasion, the American cryptanalysts, having been fully conversant with the way navigational tables had been used for the preceding "Bellatrix" and "Bellatrix Alpha", were able to infer that Venus came from there, as well, and to break the emergency key in less than an hour.

Similar to the regular Catchword systems were the group of so-called Trick Offiziers which arose from the German alarm at the repeated Allied successes in breaking up refuelling rendezvous during the winter of 1943 and spring of 1944 (immediately following the start of American bombe operations). Fortunately the Germans, as usual, clung to their blind faith in the unbreakable Enigma, and attributed their losses to a combination of treason and Allied Direction Finding or Radar. To combat these, they assigned new rendezvous and tried to limit knowledge thereof to the actual subs concerned by use of special Keys, set up by messages of which the following is typical:

> "To: Queck ((U-92))
>
> Decipher an officer message to follow later
> under catchword 'Glocke' with following setting:

1) Form officer Message setting with following letters:

3rd letter of first name of mother of Oberleutenant Knof.

2nd letter of first name of 2nd watch officer.

2nd letter of family name of physician.

Last letter of family name of 3rd watch officer.

2) Add the following figure to officer stecker connection: 1st digit of street address of Seaman Scherber.

3) Destroy this message after noting contents."

Other such messages appeared under cover names like "Schatten" Shadows), "Glocke" (Bell), and "Maske" (Mask). This system was used to disseminate information about a new slide procedure to certain U-boats which were still out when the change was to go into effect. A similar method was used to pass special orders to a group of submarines operating off Norway under the covername of Group Fox (Gruppe Fuchs) in October 1944.

Another type of Special Key has occurred where it was impossible for the Central Cipher Administration to disseminate completely new Keys. They met the difficulty by mixing up elements of old inner and outer settings under covernames. "Fensterglas" procedure appeared in August of 1944 for reused Hermes Keys in the southern area. "Apfelsine" and "Eiche" appeared as covernames for lists of reused common Keys for Western France areas on 15 December 1944. Special Fortress Keys were issued under a series of covernames and allotted Aegir's former numbers in the Indicator Allotment List. Diplomatic traffic between Tokyo and Berlin also reverted to the expedient in 1945, when a whole year's Keys were made up, partly new and partly old, under the covername "Stempelkissen".

h) Reserve Hand Procedure

Again, as in the case of all other cipher aids, further harm was done by the use of standard phraseology. This we reserve till later. For the present we proceed to the Aids provided for the second type of emergency--breakdown of the machine.

In this case use was made of the R.H.V. (Reserve Hand System) in the Atlantic, or the similar systems, such as Henno in the other areas. All hand systems were designed to produce messages looking exactly like machine texts--as appears from the sample RHV message of 5 May 1944 shown in Figure 20. Furthermore, the first steps in breaking out these messages were identical with those in the case of Enigma.

In the present case we see the indicators to be XTHE MSTZ. The effective Calendar (MEUHDUNG), Library No. 74.6, tells us that the Bigram Table for the day is G. Using it we convert XT to JE, HE to TV, MS to QK and TZ to MR. This means we have JTQM and EVKR as our Book Indicator Groups, discussed above in the regular Enigma Procedure. As b efore, we strike out the first letter of the first group and consult the alphabetic section of the Kennbuch, Library No. 86, looking for TQM. There we find 651 as a numerical equivalent. Still repeating machine procedure, we consult the current Allotment Table (DORSCH), Library No. 86, and here get the first indication that we do not have a machine message. We find that 651 lies among the numbers (621-670) assigned to R.H.V.

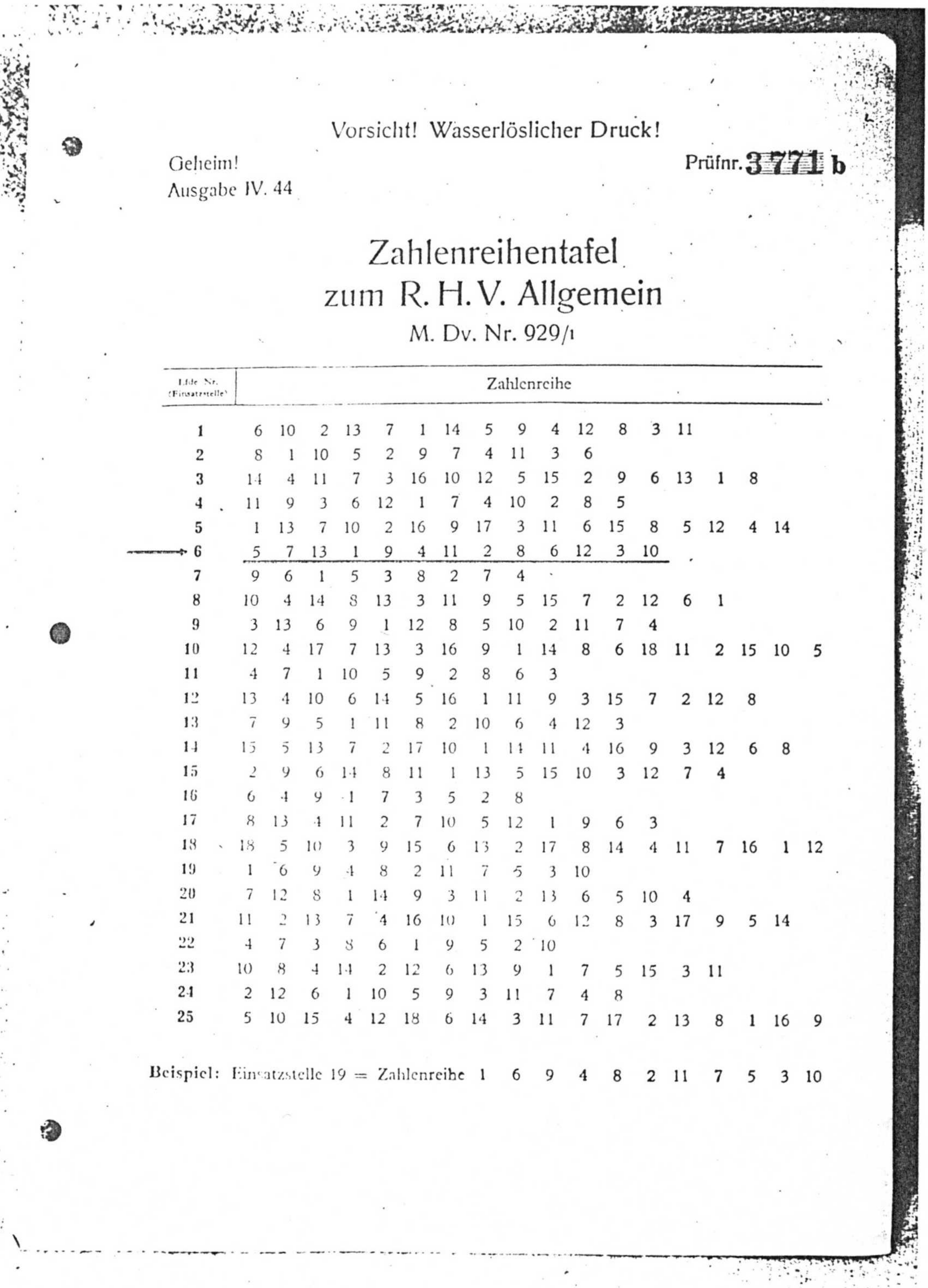
From this point on we proceed quite differently. We know that our second Book Indicator Group is in no way related to any machine setting. Instead we make use of both groups, in the fashion discussed below, to determine the particular ones of sets of substitution and transposition ciphers to apply by hand.

```
1207/5/213

XTNE MSTZ RPUF AFYM BVSQ WFOT WGAC SYUQ OBWS

POSZ BUYJ CTNP DBEP ZWVP NZDO HEBP WBVP CBRR

DKWL ELIU RQDL KQOT MVWY GVQX PKZG GAVI TIBP

FTTK XTWK HFHN JMPR QXRP SZJL MPFV ZMQF WFZJ

FVMW TFIN YESH CLSL JDMF KBDJ FMRT TFRY LACZ

HWQY BHHH HXHE XTNE MSTZ
```

SAMPLE R.H.V. MESSAGE

Figure 20

NUMERICAL KEY TRANSPOSITION TABLE FOR HAND SYSTEM



Vorsicht! Wasserlöslicher Druck!

Geheim!
Ausgabe IV. 44

Prüfnr. 3771 b

Zahlenreihentafel
zum R. H. V. Allgemein

M. Dv. Nr. 929/1

Lfde Nr. (Einsatzstelle)	Zahlenreihe																	
1	6	10	2	13	7	1	14	5	9	4	12	8	3	11				
2	8	1	10	5	2	9	7	4	11	3	6							
3	14	4	11	7	3	16	10	12	5	15	2	9	6	13	1	8		
4	11	9	3	6	12	1	7	4	10	2	8	5						
5	1	13	7	10	2	16	9	17	3	11	6	15	8	5	12	4	14	
6	5	7	13	1	9	4	11	2	8	6	12	3	10					
7	9	6	1	5	3	8	2	7	4									
8	10	4	14	8	13	3	11	9	5	15	7	2	12	6	1			
9	3	13	6	9	1	12	8	5	10	2	11	7	4					
10	12	4	17	7	13	3	16	9	1	14	8	6	18	11	2	15	10	5
11	4	7	1	10	5	9	2	8	6	3								
12	13	4	10	6	14	5	16	1	11	9	3	15	7	2	12	8		
13	7	9	5	1	11	8	2	10	6	4	12	3						
14	15	5	13	7	2	17	10	1	14	11	4	16	9	3	12	6	8	
15	2	9	6	14	8	11	1	13	5	15	10	3	12	7	4			
16	6	4	9	1	7	3	5	2	8									
17	8	13	4	11	2	7	10	5	12	1	9	6	3					
18	18	5	10	3	9	15	6	13	2	17	8	14	4	11	7	16	1	12
19	1	6	9	4	8	2	11	7	5	3	10							
20	7	12	8	1	14	9	3	11	2	13	6	5	10	4				
21	11	2	13	7	4	16	10	1	15	6	12	8	3	17	9	5	14	
22	4	7	3	8	6	1	9	5	2	10								
23	10	8	4	14	2	12	6	13	9	1	7	5	15	3	11			
24	2	12	6	1	10	5	9	3	11	7	4	8						
25	5	10	15	4	12	18	6	14	3	11	7	17	2	13	8	1	16	9

Beispiel: Einsatzstelle 19 = Zahlenreihe 1 6 9 4 8 2 11 7 5 3 10

FIGURE 21 c

TOP SECRET-ULTRA

CIPHER				BIGRAM EQUIVALENTS			
6	18	2	21	6	18	2	21
R	P	U	F	H	H	C	T
A	F	Y	M	U	A	R	C
B	V	S	Q	K	E	F	E
W	F	O	T	E	R	A	H
W	G	A	C	N	N	I	R
S	Y	U	Q	I	R	I	E
O	B	W	S	L	F	B	K
P	O	S	Z	E	S	G	E
B	U	Y	J	W	H	E	N
C	T	N	P	D	R	C	F
D	B	E	P	I	E	R	E
Z	W	V	P	W	E	D	F
N	Z	D	O	I	T	G	N
H	E	B	P	E	N	W	E
W	B	V	P	V	E	H	B
C	B	R	R	K	N	N	F
D	K	W	L	W	C	G	T
E	L	I	U	M	R	K	E
F	Q	D	L	X	I	R	H
K	Q	O	T	S	F	H	B
M	V	W	Y	N	S	E	S
G	V	Q	X	V	O	I	W
P	K	Z	G	I	E	D	D
G	A	V	I	R	O	K	E
T	I	B	P	U	S	N	N
F	T	T	K	G	S	D	O
X	T	W	K	C	I	S	E
H	F	H	N	S	L	E	U
J	M	P	R	I	E	E	S
Q	X	R	P	H	D	E	U
S	Z	J	L	E	H	I	I
M	P	F	V	A	I	Z	D
Z	M	Q	F	R	C	E	C
W	F	Z	J	I	E	N	D
F	V	M	W	E	E	H	S
T	F	I	N	E	R	S	C
Y	E	S	H	I	R	L	F
C	L	S	L	B	D	B	Z
J	D	M	F	L	S	O	C
K	B	D	J	B	X	G	D
F	M	R	T	E	C	U	E
T	F	R	Y	E	E	I	N
L	A	C	Z	V	I	R	C
H	W	Q	Y	A	E	S	E
B	H	H	H	D	E	L	T
H	X	H	E	N	M	E	O

PLAIN TEXT CAGE

5	7	13	1	9	4	11	2	8	6	12	3	10
V	O	R	H	E	R	S	A	G	E	B	E	R
E	I	C	H	S	E	C	H	S	X	X	S	C
H	W	A	C	H	W	I	N	D	I	G	G	E
B	I	E	T	D	E	R	N	O	R	D	E	C
K	E	S	U	E	D	L	I	C	H	E	W	I
N	D	E	A	U	F	F	R	I	S	C	H	E
N	D	D	R	E	I	B	I	S	F	U	E	N
F	R	E	C	H	T	D	R	E	H	E	N	D
W	O	L	K	I	G	B	I	S	B	E	D	E
C	K	T	E	I	N	Z	E	L	N	E	R	E
G	E	N	F	A	E	L	L	E	S	I	C	H
T	U	M	E	I	N	S	F	U	E	N	F	S
M	S	E	E	Z	W	O	B	I	S	V	I	E
R	N	O	R	D	E	C	K	E	V	I	E	R
K	N											

TRANSLATION:

Forecast for area 6: Weak winds in the region of the north corner; southerly winds freshening up to 3-5, shifting to the right. Cloudy to overcast; scattered rain showers. Visibility about 15. Sea 2-4, 4 in the north corner.

SAMPLE RHV (RESERVE HAND) WORKSHEET

Figure 21d

ORIGINAL

We eliminate not only the first, but also the last letter of the Book Indicator Groups. This leaves us with two trigrams, TQM, which we have used before, and EVK. These, again, are looked up in the Kennbuch. This time, however, we disregard the three-digit number in large print and, instead, take the small figures:- 5 and 2 in this case. These give the row and column in a double duty table (Tauchtafelweisser), of which a sample is shown in Figure 21a. We find in the case under consideration that in row 5, column 2 is the figure 6. This is our transposition key number (Zahlenreichen). Following the 6 on row 5 are 18, 2, and 21. These four numbers (6, 18, 2, and 21) are our substitution keys.

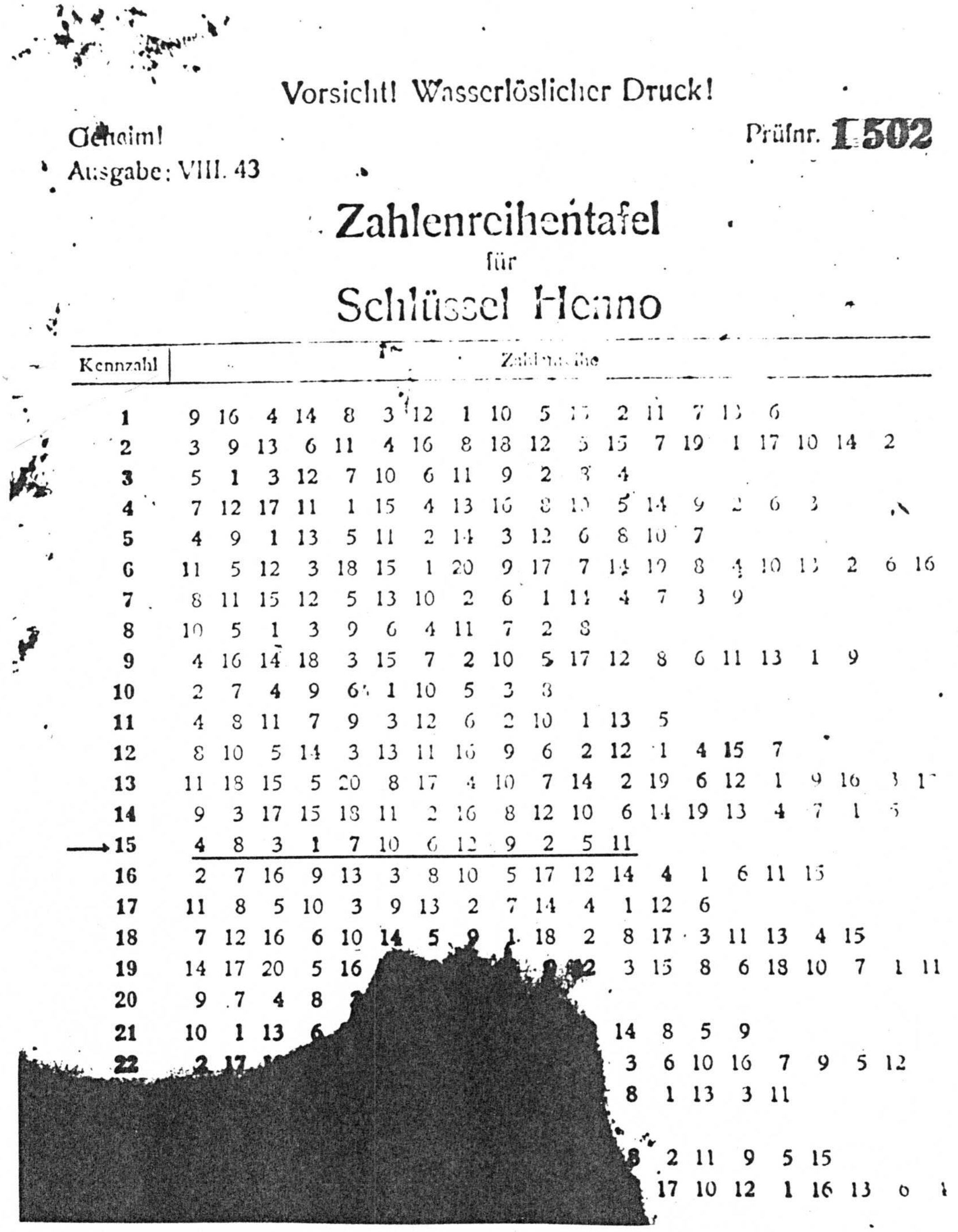
Actually, in deciphering, we make the substitution first, and follow it with the transposition. In enciphering, the process is reversed. To decipher, the groups after the indicators are written in columnar forms, and separated in pairs, as follows:

6	18	2	21
R	P	U	F
A	F	Y	M
B	V	S	Q
W	F	O	T

The figures at the head of the columns are the figures we obtained above. They mean that all the vertical digraphs in the first column are substituted according to Table No. 6, out of a set of 25, Library No. 260, those in the second column are substituted from Table No. 18, those in the third from Table No. 2, and those in the last from Table No. 21. In the second half of Table No. 6, of which the first half is shown in Figure 21b, we find RA = HU, here BW = KE; while in Table 18, PF = HA, VF = ER; Table No. 2 has UY = CR, SO = FA; and Table 21 shows FM = TC and QT = EH. The full results of substitution are shown in Figure 21d.

ORIGINAL

NUMERICAL KEY TRANSPOSITION TABLE FOR HENNO



Vorsicht! Wasserlöslicher Druck!

Geheim!
Ausgabe: VIII. 43

Prüfnr. 1502

Zahlenreihentafel
für
Schlüssel Henno

Kennzahl	Zahlenreihe																			
1	9	16	4	14	8	3	12	1	10	5	15	2	11	7	13	6				
2	3	9	13	6	11	4	16	8	18	12	5	15	7	19	1	17	10	14	2	
3	5	1	3	12	7	10	6	11	9	2	8	4								
4	7	12	17	11	1	15	4	13	16	8	10	5	14	9	2	6	3			
5	4	9	1	13	5	11	2	14	3	12	6	8	10	7						
6	11	5	12	3	18	15	1	20	9	17	7	14	19	8	4	10	13	2	6	16
7	8	11	15	12	5	13	10	2	6	1	14	4	7	3	9					
8	10	5	1	3	9	6	4	11	7	2	8									
9	4	16	14	18	3	15	7	2	10	5	17	12	8	6	11	13	1	9		
10	2	7	4	9	6	1	10	5	3	8										
11	4	8	11	7	9	3	12	6	2	10	1	13	5							
12	8	10	5	14	3	13	11	16	9	6	2	12	1	4	15	7				
13	11	18	15	5	20	8	17	4	10	7	14	2	19	6	12	1	9	16	3	13
14	9	3	17	15	18	11	2	16	8	12	10	6	14	19	13	4	7	1	5	
→ 15	4	8	3	1	7	10	6	12	9	2	5	11								
16	2	7	16	9	13	3	8	10	5	17	12	14	4	1	6	11	15			
17	11	8	5	10	3	9	13	2	7	14	4	1	12	6						
18	7	12	16	6	10	14	5	9	1	18	2	8	17	3	11	13	4	15		
19	14	17	20	5	16	[illegible]	[illegible]	[illegible]	[illegible]	9	12	3	15	8	6	18	10	7	1	11
20	9	7	4	8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]									
21	10	1	13	6	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	14	8	5	9					
22	2	17	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	3	6	10	16	7	9	5	12	
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	8	1	13	3	11				
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]									
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	8	2	11	9	5	15			
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	17	10	12	1	16	13	6	1

FIGURE 22c

SUBSTITUTION INDICATOR TABLE FOR HENNO

Vorsicht! Wasserlöslicher Druck!

Prüfnr. 1502

H. 43

Tauschtafelweiser
für
Schlüssel Henno

Kennzahl der Kenngruppentafel aus 4. Buchstabenpaar der Kenngruppen

Kenngruppentafel aus 3. Buchstabenpaar der Kenngruppen

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26				
1	5	18	29	10	19	6	26	17	22	1	11	28	15	7	25	2	21	12	3	16	23	14	20	4	13	9	24	27	8	1
2	13	26	6	19	24	14	3	20	7	12	18	8	21	15	2	30	9	23	17	29	5	22	27	10	25	16	4	28	11	2
3	1	22	15	29	3	16	23	14	28	4	17	13	24	6	26	18	5	12	21	8	10	25	7	30	27	20	9	11	19	3
4	9	2	13	26	8	29	25	18	6	24	20	7	17	27	5	12	19	28	4	21	14	30	16	22	23	11	15	1	10	4
5	16	5	25	12	23	21	6	15	13	22	1	11	7	24	20	8	10	14	19	30	26	28	3	18	29	9	27	17	2	5
6	23	13	4	3	27	9	19	2	17	29	12	22	18	8	16	11	24	30	21	7	15	1	25	10	6	26	20	14	28	6
7	3	18	30	17	2	27	10	16	25	1	9	11	19	14	4	8	5	15	7	21	20	12	29	26	13	24	28	22	23	7
8	8	14	29	22	9	3	4	28	20	10	26	2	5	24	18	13	21	25	16	6	12	19	27	23	17	15	11	30	1	8
9	4	19	26	1	2	18	29	25	10	22	28	9	17	30	13	11	3	20	27	21	5	12	24	15	7	23	14	16	6	9
10	23	26	6	20	28	13	7	1	19	8	5	24	12	2	16	21	14	27	4	30	18	15	10	29	22	11	3	25	17	10
11	8	13	29	30	7	26	22	18	2	21	14	6	27	17	3	9	25	5	20	12	16	1	24	11	4	28	19	15	23	11
12	29	22	15	12	27	14	20	28	5	23	21	6	4	26	13	18	7	3	2	1	8	24	16	30	10	19	17	9	25	12
13	4	27	21	9	22	6	14	5	20	26	3	13	30	23	19	8	29	18	10	15	2	28	25	11	16	24	1	7	17	13
14	21	7	28	6	10	16	27	19	22	30	14	26	8	5	20	25	12	15	1	11	23	9	3	17	4	2	24	18	29	14
15	8	16	11	27	22	30	6	9	26	12	1	5	25	15	4	2	28	21	[illegible]	13	20	29	18	7	3	17	10	23	24	15
16	19	22	5	9	29	4	20	26	14	25	16	12	[illegible]	21	6	17	8	13	24	2	27	11	7	18	23	10	30	28	1	16
17	3	10	[illegible]	23	15	18	6	4	13	[illegible]	9	[illegible]	[illegible]	[illegible]	[illegible]	30	26	2	5	19	8	12	21	7	20	14	1	11	25	17
18	14	26	24	8	20	5	29	9	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	11	28	4	16	22	30	18	3	23	12	25	13	18
19	[illegible]	12	17	24	13	10	15	21	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	5	6	20	14	27	4	22	8	29	3	23	7	19
20	8	5	12	16	6	28	18	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	20	2	23	4	1	26	24	25	27	10	13	30	20
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	12	27	18	22	5	2	7	13	6	26	14	21
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	30	12	3	19	28	23	4	14	27	17	9	22
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	8	16	24	1	4	18	29	13	7	19	30	23
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	18	9	2	25	7	13	4	11	26	3	12	24
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	21	10	28	4	16	22	11	5	19	25	17	25
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	4	19	7	26	15	9	3	29	24	22	8	26
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	20	21	22	23	24	25	26				

FIGURE 22d

The last stage is the transposition. The key for it we have seen to be 6. This means we take the first of the series of 25 numerical sequences in the ZAHLENREIHENTAFEL, shown in Figure 21c, and use them as column labels in a "cage" of the type shown in Figure 21d. Into this cage is written the results of the previous substitution, also shown in Figure 21d. We now have plain text, of which the translation is as given.

The Hand Systems in non-bigram (throw-on) traffic is similar in being, also, a combined substitution and transposition, but the details vary to some extent. As we have said before, the discrimination among Poseidon, Hermes, Uranus, machine keys on the one hand, and Henno, on the other, was not by the usual Bigram Tables. On the other hand, use was made of a special Discriminant Table, shown in Figure 22a and an Allotment List shown in Figure 22b.

Take a specific case of a message on August 1, 1944, with indicators EBHY UZQZ. The first letter of the first indicator group (E) tells us to look in Column E of the K-Table, Figure 22a. The first letter of the second indicator group (U) is found in line 2. This is seen from Figure 22b (the Allotment List) to be one of the numbers (2, 5, 12, 15, 20, and 22) assigned to Henno for that day. We now know we have a hand ciphered message.

The two second letters B and Z are now looked up in Figure 22a, as before. They give us the number 15. This means our columns at the top of the transposition cage receive the numbers shown on line 15 of the Transposition Table, Figure 22c, i.e., 4 - 8 - 3 - 1 - 7 - 10 - 6 - 12 - 9 - 2 - 5 - 4. For the substitutions to be used we are informed by the third letters of our indicators (H and Q) which

Figure give us 20, and by the fourth letters (F and Z), giving 3. This means we enter line 20, column 3 of the Substitution Table, Figure 22d, and find the number 5, followed by 12, 16, and 6. These (5, 12, 16, and 6) are the bigram tables used for the substitution in the manner of R.H.V.

Little can be said by way of criticism of these systems, other than in regard to the unnecessary reciprocal nature of the Bigram Tables. The volume and importance of hand traffic, fortunately, was slight in the Atlantic. The British found the remaining traffic to be quite useful in supplying leads into the machine.

This concludes the discussion of Cipher Aids and their usage as such. As the reader will have seen, the underlying principles and practices were largely universal the world over. However, as previously indicated, the contents of particular Keys varied from area to area. It is this scheme of subdivision which we now consider.

i) For convenience in administration and for internal security reasons, the High Command divided the Naval Service into Cipher Areas, all holders in a given area being issued the same keys--although they might not have regular direct communication with each other.

These areas were variously designated, generally by mythological names, such as Hydra, Aegir (Teutonic), Hermes, Poseidon, Uranus, Thetis, Neptun and Triton, in use at the beginning of the War. Others such as Tibet and Potsdam were merely place names, while BERTOK was a contraction of the two places (Berlin and Tokyo) involved.

Standard equipment for a given area would include the following types of material:

TOP SECRET-ULTRA

~~R.I.P.~~ No. 401

CIPHER EQUIPMENT CAPTURED FROM U-505
ATLANTIC AREA

GYA Library No.
(* denotes original;
otherwise photostat)

I. Machines and Gear (8 Items)

- Two Enigma machines (Schluessel M #3467 and 4473) — 16*
- Two Wheel Boxes (#M 3467 and 4473) — 15.1*
- Enigma Transformer (#MZSS No. 0698) — 17*
- Printer for Enigma Machine — 18*
- 21 Rolls of Unused Tape for Printer
- Board for Aircraft Recognition
- Five large and small metal discs (Recognition) with following names: (large) Schmidt, Schilling, Schneider, Schulze, Seidel; (small) Eberhard, Ernst, Erasmus, Egbert, Emil — 288*
- Two Folders for Cipher Aids (Sammelmappe fuer Schluesselmittel Nr. 1332 294/1) — 20*

II. Cipher Aids (36 Items)

1. General Regulations

a. Enigma General

- Enigma General Instructions - Berlin 1941 (Der Schluessel M-Allgemeine Bestimmungen) — 31*
- Enigma General Procedure (Der Schluessel M-Verfahren M-Allgemein M.D.V. Nr. 32/1) — 32*
- Instructions on Maintenance of Cipher Security (Bestimmungen zur Wahrung der Schluesselsicherheit bei Verlusten von Schluesselmitteln B.W.S.M.Dv. Nr. 949) — 35*

Figure No. 23

ORIGINAL

CIPHER EQUIPMENT CAPTURED FROM U-505
ATLANTIC AREA

GYA Library No.

b. Enigma Officer and Staff Regulations

- The Enigma Offizier and Staff Procedure (Der Schluessel M-Verfahren M Offizier und M Stab M.Dv. 32/2) — 34.3*

c. Reserve Hand Regulations

- Reserve Hand System Procedure - General Instructions (Reservehandverfahren #49 M.Dv. #929/1) — 258

d. Other Regulations

- Emergency Signal Procedure (E-bars) issued Oct. '39 (Signalschluessel fuer den Funksignaldienst - Funksignalschluesselgeheim. Ausgabe: October 1939. M.Dv. Nr. 114, Prf. Nr. 889) — 199.1*
- Standing War Orders (Communications) (Standige Kriegsbefehle des Bd.U. Nachrichtenbestimmungen zu M.Dv. Nr. 97) — 37*
- Weather Short Signal Instructions (Wetterkurzschluessel M.Dv. Nr. 443) — 22.1
- Aircraft Recognition Tables Instructions (E.S.-Tafeln zur E.S.-Vorschrift-zu.M.Dv.Nr.75) — 287.1*
- Extract from Recognition Signal Instructions and Instructions for U-boats, Recognition Service Berlin 1940. (Auszug aus der "E.S.-Vorschrift" und Vorschrift "Der Erkennungsdienst" fuer U-Boote, Berlin 1940 M.Dv. Nr. 75a) — 286*

2. Books, Tables and Keys

a. The Indicator Book and Allotment Tables (Kenngruppenbuch - K-Buch - M.Dv.Nr. 98 Ed.'41) — 86*

CIPHER EQUIPMENT CAPTURED FROM U-505
ATLANTIC AREA

	GYA Library No.
b. Bigram Tables	
- Bigram Table "Muendung" (Doppelbuchstabentauschtafeln fuer Kenngruppen, Kennwort: Muendung zu M.Dv. Nr. 98)	74.6*
- Bigram Table "Quelle" (Doppelbuchstabentauschtafeln fuer Kenngruppen, Kennwort: Quelle)	74.7*
c. Short Signal Books	
- Short Signal Code Book (Kurzsignalheft 1941)	182.1*
- Short Signal Indicator Book No. 5 (Kenngruppenheft Nr. 5 zum Kurzsignalheft 1941. M.Dv. Nr. 86. Pruef.-Nr. 441)	182.3*
- Secret Call Sign List (Geheime Marinefunknamenliste - M.Dv.Nr. 82 Ed. '42)	169.1*
d. Weather Books	
- Message Setting Table for Weather Short Signal Cipher (Spruchschluesseltafel fuer den Wetterkurzschluessel - 3rd Ed.)	220
- Cloud Tables for Weather Signals (Wolkentafeln fuer U-Boote - Beiheft zu M.Dv. Nr. 443)	222.2
- Call Signs and Flagnames for Weather Ships (Geheime Funknamenliste Wetterbeobachtung)	169.2
e. Enciphered Squares	
- Code Book (Schluesselheft F #49)	247.2*
- Naval Square Code (Addressbuch - Ed. Apr. 1943)	247.1

Figure No. 23 - Page 3

CIPHER EQUIPMENT CAPTURED FROM U-505
ATLANTIC AREA

	GYA Library No.
f. Recognition Signals, etc.	
- Recognition Signal Setting and Coastal Recognition Signals - June 1944 (E.S.-Einstellung und Kuesten E.S.--June 1944- Geheime Kommandosache - Prf.Nr. 0224)	289
- Recognition Signals Table #4 (E.S. Tafel 4)	287.2*
- Scouting and Fighter Plane Cipher Tables (Aufklaerungs- und Kampffliegertafel	283.1*
- Aircraft Grid Position Table (Standortschluesseltafel - A.Fu. Luft-Anlage 3)	238
g. Keys	
- Two sets Atlantic U-Boat General Key Tables for June 1944 (Schluessel M Triton - June 1944 - Pruf.Nr. 124 Geheime Kommandosache - Schluesseltafeln M-Offizier)	5
h. Log Books	
- List of Secret Documents destroyed at sea 31 May 1944	64.3*
- List of Cipher Aids (to be) destroyed 30 June 1944	64.4*
- Index of Secret Code Books from 12 August 1943 (Gkdos. Buecher Verzeichnis U-505 ab 12.8.43)	64.8*
- Confidential Notebook (Geheime Briefbuch U-505)	64.5*
- Confidential Notebook (Geheime Briefbuch U-505)	64.6*
- Secret Notebook (Gkdos. Briefbuch)	64.7*
- Index of Classified Material from June 1943 (Geheime Buecher Verzeichnis U-505 Begonnen June, 1943)	64.9*
i. Blank Cipher Sheets	
- Cipher Sheets (Schluesselzettel)	54*
- Cipher Sheets for Strip Writer (Schluesselzettel fuer Streifenschreiber)	54*

GERMAN CODE AND CIPHER AREAS AT THE TIME OF U.S. DECLARATION OF WAR

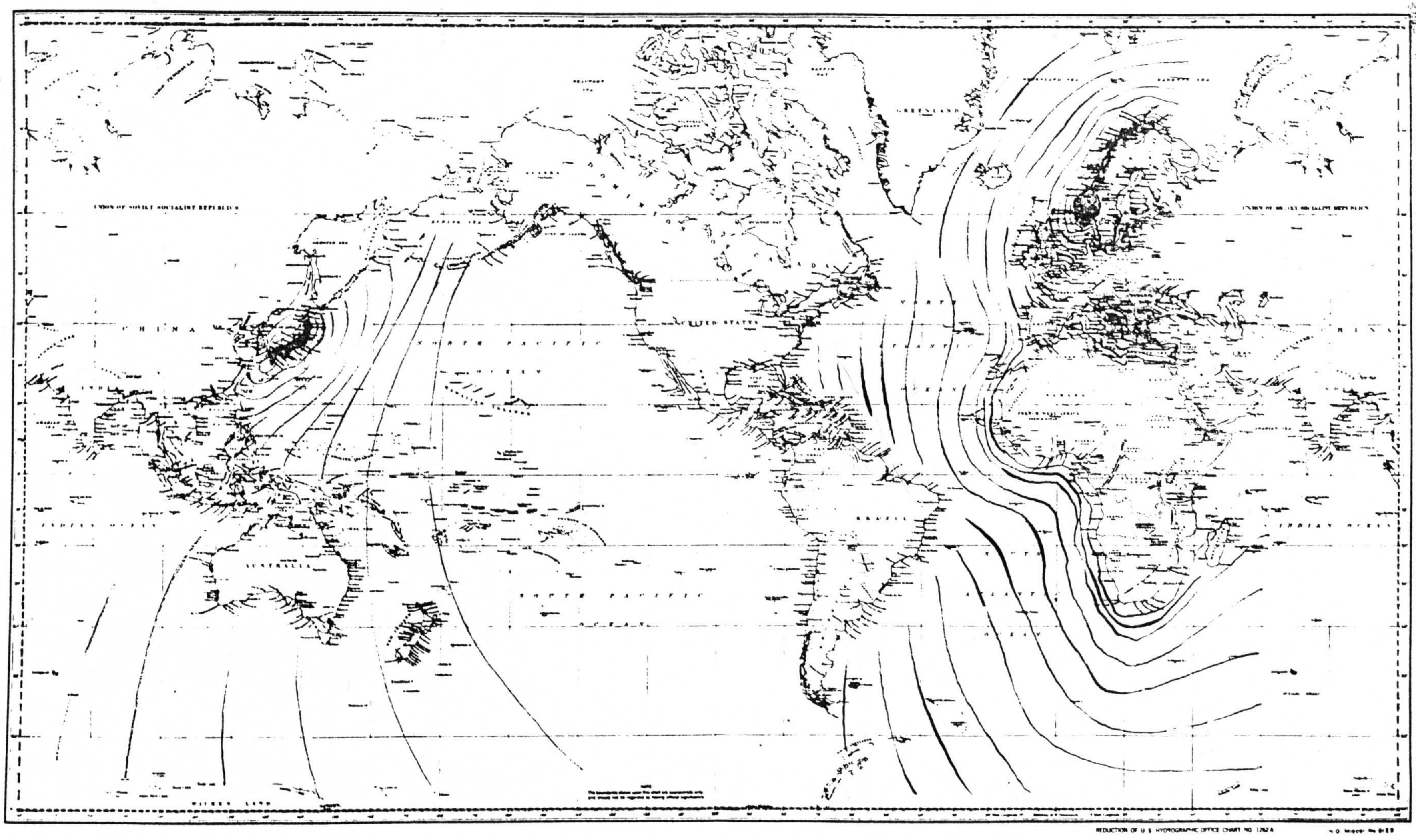


FIGURE 24a

■ HYDRA

▨ AEGIR, TIBET & TIBET SONDERSCHLUSSEL, BERTOK

■ HERMES, POSEIDON, URANUS

■ POTSDAM

■ THETIS, SLEIPNIR

■ TRITON

NEPTUN (FLAG OFFICERS – LARGE SURFACE CRAFT)

a) The machine with wheels and gear, such as printer and tape.
b) Code books for other than plain language traffic.
c) General, Offizier, Staff and Special Keys.
d) Setting and Indicator lists for code signals.
e) Bigram Tables for enciphering indicators.
f) Allotment List to determine which traffic was for one's area.
g) Reserve hand systems, including:
    i) Substitution Keys
    ii) Transposition Keys

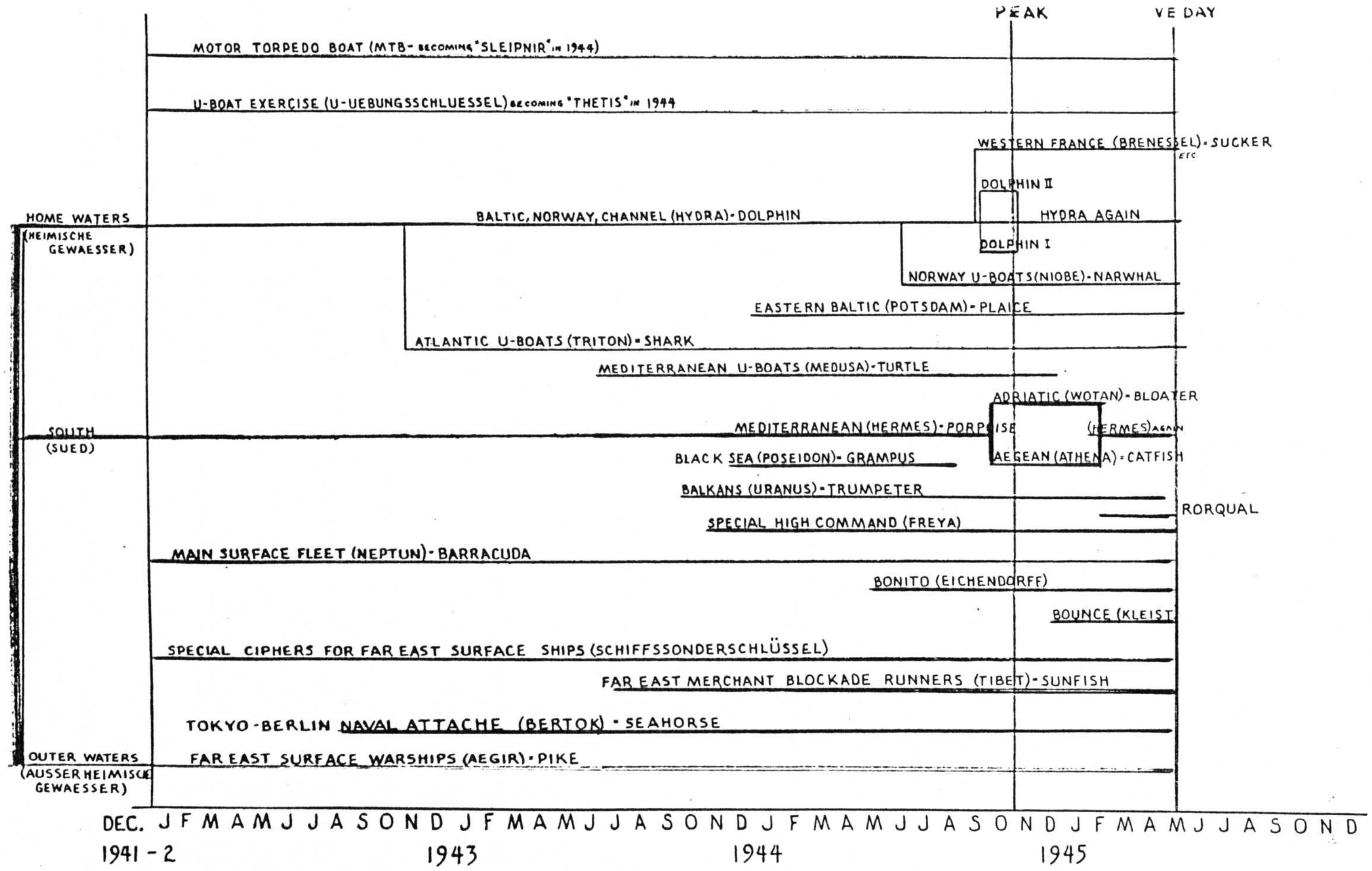
A more detailed list in the case of U-505 operating in the Triton (Atlantic) area is shown in Figure 23.

Before U. S. entry in the war (in 1941), the Cipher Areas consisted of three major divisions:

1. Home Waters (Heimesche Gewaesser)
2. Outer Waters (Ausserheimische Gewaesser)
3. South (Sued)

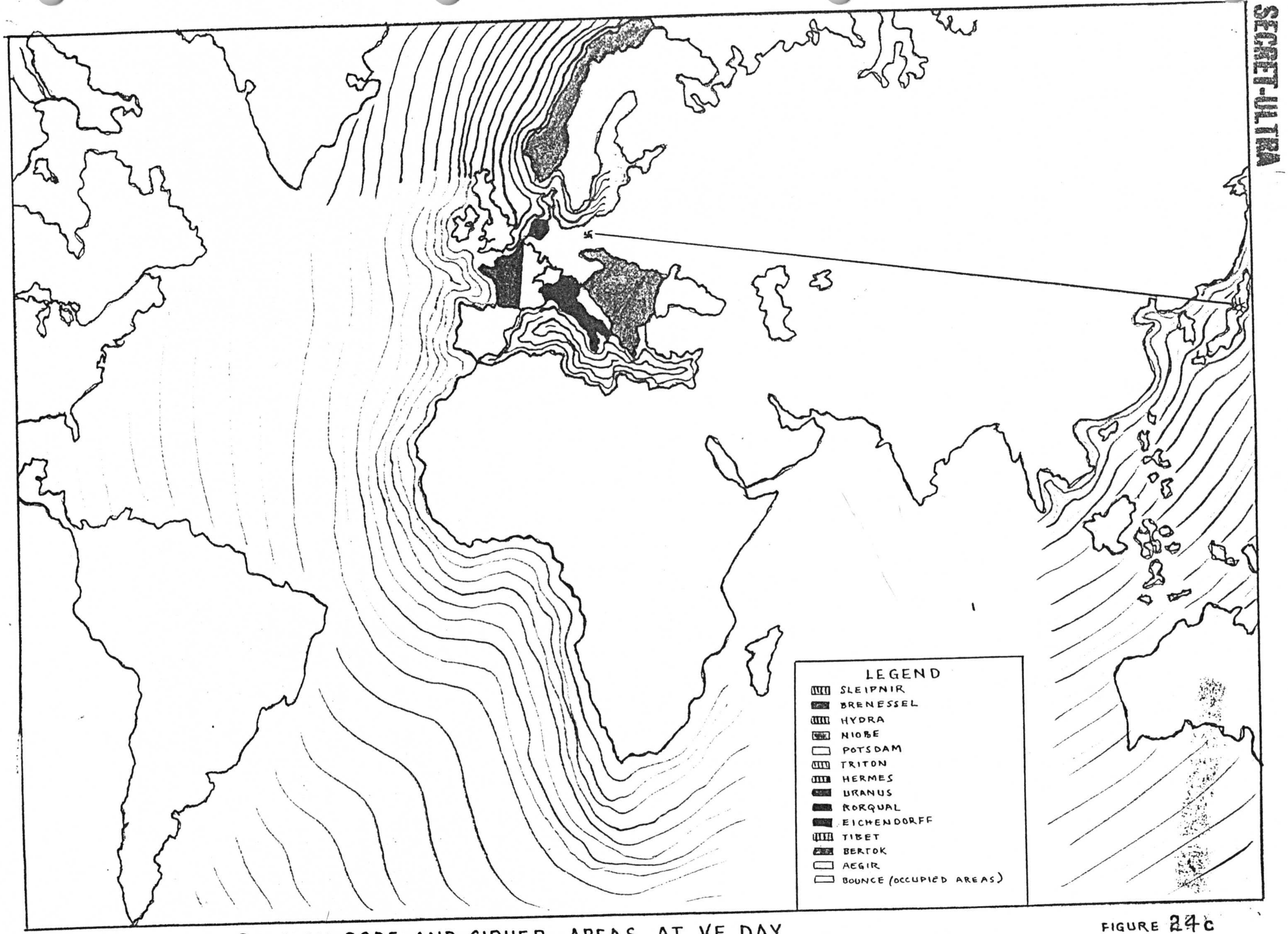
By December 8, 1941, the number of cipher areas had tripled. Home waters had broken into Motor Torpedo Boats, U-boat Exercise, and a key covering the Baltic, Northern Waters, and the Channel. There was also a key for the main surface fleet. Keys for the South remained general, but Outer Water Keys had broken into channels for Far East Surface Warships (with special ciphers for each ship in addition), a Key for Far East Merchant Blockage Runners, and a Diplomatic Key for Tokyo-Berlin Naval Attaches. See Figure 24a.

Home Waters Keys had split into two more branches by January 1943, covering the Eastern Baltic, one for Atlantic U-boats, while the parent stem covered a fairly general Northern Area (the North Sea, Norway, the Low Countries, Western France coast commands, the Channel, the Arctic, and the North Atlantic to Cape Verde (for surface craft only).



CHANGES IN GERMAN CODES AND CIPHERS - DECEMBER 1941 TO VE DAY

FIGURE 24b



GERMAN CODE AND CIPHER AREAS AT VE DAY

FIGURE 24c

Four more keys had appeared by January 1944, making a total of 15 major German Naval keys. In addition to the general areas mentioned above, the four new areas included a special High Command key and a key for U-boats in the Mediterranean. These two were additions to the Home Waters family. The Southern family had meanwhile broken into a Mediterranean key for all stations (except actual U-boats), a Black Sea key, and a Balkans key.

By the spring of 1945, five more keys had appeared, making a grand total of 19 major keys which had come into being. The Home family and the Southern Area had undergone further divisions. The former three split to cover the exigencies of the Western France retreat and to facilitate secure communications with the besieged fortresses which had been left on the French Coast. The latter had split into special areas allocated to the Adriatic and the Aegean. A graph showing the times and manners in which the original keys subdivided is shown in Figure 24b, showing both German and Allied cover-names.

On V.E. day the following cipher areas existed:

Sleipnir	-	Motor Torpedo Boats (Baltic)
Brenessel	-	Western France
Hydra	-	Norway Administrative
Niobe	-	Norway Operational
Potsdam	-	Eastern Baltic
Triton	-	Atlantic U/Boats
Hermes	-	Mediterranean
Uranus	-	Balkans
Eichendorff	-	Saboteur
Tibet	-	Far East
Bertok	-	Berlin-Tokyo
Aegir	-	Far East

But traffic in all channels had either dried up completely or dwindled to a mere trickle. The general boundaries of these areas are shown in Figure 24c.

TOP SECRET-ULTRA

This practice of having numerous Cipher Areas was one of the least unsound in which the Germans indulged. Their only error lay in the methods in which new areas were created. This was in many cases by having new Keys obtained by slides on old, which was subject to the criticisms given above. This technique was employed in the following cases:-

New Key	Old Key	Date
Triton	Heimische Gewaesser	November, 1942
Niobe	Hydra	June, 1944
Brenessel Schaltenhalm Strandustel Hydra I Hydra II	Hydra	September, 1944
Wotan Athena	Hermes	September, 1944
Tibet	Aegir	July, 1943

Constructing new Keys in this fashion considerably simplified the Allied task of getting into them, since a wholly new Key would have to be tried on all Wheel Orders and Steckers, while a slid Key reduced the Wheel Orders to be tried to 8. Another case of German cryptos casually tossing away odds of 42 to 1.

V - UNDERLYING TEXT - U-BOATS

a) Principal Codes

We have so far been concerned only with the problem of how the German U-boat originators used their machine, and with what cipher aids, to convey their messages to their addresses. We have not, as yet, considered what they might have to say, nor whether there were any special rules which varied with the contents of the signals. As the reader would imagine, the Germans, in common with all Navies, used both plain text and codes, both of which they enciphered on the

```
6675  KCS      (1)                     T.O.I.  2110B/26 Mar. '43  (2)


(3)     (4)      ---------(7)--------------
B'B'    E C J    P A K E     T K P T    C S
     (5)2 0 2    K D Z S     M C G W    B L
     (6)A E D    ---------(8)--------------
```

```
K D Z S     =     My position is              )
                                              )
M C G W     =     Square BE subsquare 88      )    (9)
                                              )
B L         =     U-154, Schuch, Commanding   )
```

1) Frequency
2) Time of Intercept
3) Traffic type Indicator
4) Enciphered Setting Indicator
5) Numerical Equivalent - See Allotment List to determine type of daily key.
6) Clear setting of Slow, Medium and Fast Wheels
7) Cipher Text
8) Plain Text
9) Translation

A TYPICAL FLEET SHORT SIGNAL MESSAGE (BETA)

Figure No. 25

Enigma. We shall consider the codes, and the special machine usages which accompanied them, first.

In general, these codes were not devised so much for additional security as for ease and speed in handling routine and stereotype traffic. The five most important were the Fleet Short Signal, Weather, Ursula, E-Bar and Z-Bar Systems, which will be discussed in some detail. The remainder can be dismissed with a few general remarks.

(i) Fleet Short Signal System.

The codes used in this system were mainly designed with an eye to brevity. Their purpose, as stated by German High Command, was to make more difficult the location of U-boats by enemy direction-finding.

The principal codes used were the"U-Bootes Kurzsignalheft" of 1940 (FEODOR), Library No. 184, and later edition, "Kursignalheft" 1941, Library No. 185, (these being used for communications between U-boats and Control), together with a short-lived code to be used in the opposite direction (Control to U-boats) called URSULA, Library No. 189, which appeared during the last half of 1944 and early 1945.

a) Type of Message.

The type of message sent in these codes is illustrated by the message shown in Figure 25, sent in FEODOR. In addition there were sighting and tracking, rendezvous and fueling, etc., reports. The Control-to-U-boat Code (Ursula) was designed for orders giving routing, attack area, rendezvous assignments, etc.

b) Type of Code.

All the codes were essentially (one-part". That is, the meanings and the code groups both followed each other in normal order. For example, in going through the section on positions, "Square AB" would be followed by "Square AC" and the two code groups for these meanings would be adjacent in normal alphabetic order.

All of the codes had a "Garble check" which, however, varied from code to code. For example, in the 1940 Short Signal Book, which used three-letter groups, the third letter was always twice as far from the first as from the second. Specifically, A K U would be a good group (U = 21 minus A = 1 is 20, while U = 21 minus K = 11 is 10); but B G S would not be. (19 minus 7 does not equal twice 19 minus 2.) The purpose of this arrangement was to enable an addressee who was able to intercept only a partial group to fill it out and look up the meaning.

The "Feodor" code involved changing from three to four letters in the code group, but again there was a "garble check". In its groups the difference between the first two letters was the same as that between the last two. For example, as seen in Figure 25, K minus D is the same as Z minus S and M minus C is the same as G minus W. The signatures, being only two letter, did not have this check.

Finally, in the Ursula Code, the same principle was followed, but with a minor change. Here the difference of the last two letters was twice that of the first two. For example, A B M O would be a good group.

However, Urusla was one of a series of codes, of which "China" (used for Far Eastern traffic) was another, which were ingeniously constructed in one respect. It was two part in a rather unusual sense. One part contained textual meanings in alphabetic order and numbered serially. This part was held by officers only, who, when they had prepared a message, presented the regular communications personnel with a series of numbers only. The radio personnel, in turn, held the second part of the code book, giving actual groups for the numbers. This, as usual, was set up, not so much for security vis-a-vis the enemy, as to restrict knowledge of message content within the German Fleet. Nevertheless, it could provide additional security if used as was proposed in a later edition of the Fleet ? Short Signal Book, Library Nos. 186 and 187, captured in 1944 before it was put into effect. In it arrangements were made to have an additive applied to the numbers before they were translated into groups.

c) Method of Enciphering.

The first step in preparing a message in any of these short signal codes was the selection of the meanings. This followed standard code practice. In most cases this gave code groups at once. In other cases, such as URSULA and CHINA, one only got numbers, which had to be changed to groups.

The next step was to add a signature, in the case of signals from U-boats to Control. These were contained in the Secret Call Sign List (Geheim Funknamenliste, Library No. 169). No signature was, of course, required in the signals from Control to U-boats, but in that case the addressees were designated by their U-number, for which special code groups were provided.

With this done, the message was ready to put through the machine. The regular Wheels, Rings and Steckers for the day were used; but the Grundstellung was ignored. Instead, the originator was restricted to a list of three-letter settings, shown in the U-Boat Short Signature List, Library No. 171. Each setting had associated with it a number and a trigram. The number was used in conjunction with the Allotment List to determine on what keys (Triton, Medusa, etc.) the message was enciphered. The trigram gave an automatic encipherment of the selected setting. The Indicators were characterized by the peculiarity of their first two letters being distinct and their third being derivable from the first two.

The final step, before the message went on the air, was to attach a preamble to indicate the type of message. For U-boat to Control it was B'B' (Morse equivalent -...-, -...-) and for Ursula, going in the reverse direction, LL (Morse .-.., .-..).

d) Method of Transmission and Acknowledgment.

In the early days of the War, Short Signals were sent by the U-boats without call sign or time/date group. Control receipted for them by retransmitting thrice in succession, prefixed with Control's call sign together with a T.O.O. and serial number, assigned by Control. Later in the war the units assigned their own T.O.O., and Control receipted by retransmitting the whole message with only the addition of a serial number in the heading. Messages were resent by the U-boats if no receipt was gotten from Control within thirty minutes.

In 1944 a system of "off-frequency" unit transmissions was introduced to make Allied interception more difficult. Short signals were, therefore, sent by units just once either on a normal U-boat frequency or on an "off-frequency". If a short signal was sent on a normal frequency, then Control receipted by retransmission

TOP SECRET TOP SECRET-ULTRA

~~R.I.P~~. No. 401 ORIGINAL

```
(1)     13560  KCS                  (2)  T.O.I.  1126/4 Apr. '44

  (3)    (4)       (5)
1105/4   WW'        J|R V N   Q S D Q   Y M F A   R O W O T    (6)
                   _T|Q L S  /Y F B H   H E E V   Y Q/P B N    (8)
                    A|(9)(10)(11)     (12)             (13)
                    I|
                   (7)
```

1) Frequency.
2) Time of Intercept.
3) Time-date of origin.
4) Traffic-type indicator.
5) Setting indicator.
6) Cipher text.
7) Plain setting of Slow, Medium and Fast Wheels.
8) Plain text.
9) North-South Indicator for Latitude of position. Here "North".
10) Degrees of Latitude - here = 57.
11) Degrees of Longitude, West, here = 29.
12) Enciphered Weather Synoptic (Library No. 222)
13) Signature PBN = U=672, Lawaltz, Commanding.

TYPICAL WEATHER SHORT SIGNAL (WW) MESSAGE

Figure No. 26

within thirty minutes, adding a serial number. If the short signal was sent on an "off-frequency", Control receipted within thirty minutes on a normal U-boat frequency by retransmitting the whole message and assigning a serial number. In addition to the receipt of the message as such, control acknowledged the contents of the "off-frequency" message by transmitting the plain text for the underlying code together with time of origin, signal strength, receiving station and frequency in the General Enigma Channel. Control handled unsolved short signals by receipting as usual and by indicating that the contents of the signal were unsolved in an acknowledgment sent out in the General Enigma traffic.

ii. Weather Short Signal System.

(Wetterkurzsignalheft 1940, Library No. 221
(Wetterkurzsignalheft 1942, Library No. 222

a) Type of Message

A typical weather short signal is shown in Figure 26. Weather messages are distinguishable from other types of messages by the prefix WW (.-- .--) and by their standard fixed length. The standard length varied from time to time during the War from as few as 12 letters to a length of 23 letters in 1945. Weather messages were, in general, sent from U-boats on explicit order from High Command. Occasionally they are sent out by the Naval Communications Officer from certain Norwegian ports, for example, Bergen. They served as quick summaries of weather conditions in operational areas.

b) Type of Code

The weather codes used by the Germans have all been similar in nature. Each code book has consisted of a series of codes, each made up of single letters of the alphabet and each used to give a different element of the weather, such as wind direction, clouds, sea conditions, etc.

c) Method of Enciphering.

Weather codes were enciphered on the Enigma machine. The time/date of transmission, as usual, determined the Wheel Order and Stecker to be used. The message setting is chosen from a special Weather Setting Table. In 1943, the Germans broke this table into five parts with separate Settings depending on the time at which the message was sent. The Allies designated these times as:-

Alpha	- 1900 to 0059
Beta	- 0100 to 0359
Gamma	- 0400 to 0659
Delta	- 0700 to 1259
Epsilon	- 1300 to 1859

Each table contained 26 settings equated to the letters A to Z, each letter designating a Setting (formerly a Three-Wheel but later Four-Wheel) and placed unenciphered at the beginning of the weather message. The second letter in a weather message, when deciphered, gave the general geographical area and also told whether the Barometer is rising, falling or steady. The third and fourth letters along with the second gave the position of the weather reporter in latitude and longitude. The subsequent letters of the deciphered weather message contained further meteorological data: barometric pressure in milibars; visibility and clouds; course of weather; wind, fog, sea and air conditions, etc. The last three letters (formerly, the last two letters) were the weather reporter's signature taken from the Secret Call Sign List mentioned above.

d) Method of Transmission and Acknowledgment.

Formerly, U-boats transmitted weather signals once on normal U-boat frequencies. Control receipted by a retransmission

TOP SECRET· TOP SECRET-ULTRA

R~~I.P~~. No. 401

ORIGINAL

```
2308  KCS    (1)                    (2)  2023B/11 Apr. 1944

(12)     (6)       (5)       ←-(3)-→ ←(4)→
E'E'    1 2 9     I W S      0125/11/773
        O U K
         (7)


 (8)      B O I E F R L D X T P H C T P G U B H I E G O Q B O
 (9)      L U C I E/D E L T A/Y G U S T A V/G E L B/Y/Q U A T
(10)          L         D'           G              ,      Q

 (8)      P Q G D G E R V L E O F C W N V X H V V O H Z O A R
 (9)      S C H/A C H T/Z W O/D R E I/S I E B E N/P I/C A E S
(10)               8      2      3         7      P'     C

 (8)      T J P I B B C F G I R O
 (9)      A R/Z W O/N E U N/L B S
(10)            2      9    Dummies

(11)      LD'      =    A/C Report
          G Gelb   =    Enemy convoy in sight
          Q 8237   =    Square 8237 = Lat. 71.27 N
                                      Long. 07.10 E
          P'       =    Sighed
          C29      =    ComSubs Artic
```

1) Frequency.
2) Time of Interception.
3) Time-date group.
4) Serial number.
5) Key-Type discriminant (here Dolphin).
6) Setting Indicator.
7) Plain setting of Slow, Medium and Fast Wheels. Reflector always at Z, Reflector Wheel at A.
8) Cipher text.
9) Plain text.
10) Figure-letter equivalents of 9).
11) Translation.
12) Type-of-traffic discriminant.

TYPICAL E-BAR SHORT SIGNAL MESSAGE

Figure No. 27

26

26

12
14

of the weather signal on a normal U-boat frequency, adding a time of origin but no serial number. When the DAN "off-frequency" system (to curtain Allied interception) was inaugurated in 1944-5, Control handled the weather signals like the Fleet Short Signals, that is, by receipting both normal and "off-frequency" weather messages by a retransmission on a normal frequency within thirty minutes. In the case of an "off-frequency" weather, however, an acknowledgment was added in the Enigma General Channel. For example:

0644/29/166 (January 1945)

"The WW received from CABOLET
just off 6 MCS at 0629A had
signal strength 2-3."

iii) E-Bar Signals.

a) Type of Message.

E-Bar messages were characterized by the prefix E'E' (Morse equivalent ..-..) following the time/date/serial number. A typical E-bar short signal message is shown in Figure 27. The three-digit number which followed the prefix was also an identifying element in this type of message.

b) Type of Code.

E-bar messages were encoded by a two part code book called The Visual Signal Book of the German Navy. (Signalbuch der Kriegsmarine, Library No. 209). The code part of The Visual Signal Book of the German Navy consists of spelled out German letter, numbers, Greek letters, and colors arranged in alphabetical order. Plain text meanings are arranged by type of operation in the second part and fitted various types of operational information.

c) Method of Enciphering.

The Enigma Machine was used with the regular Daily Wheel Order and Stecker to encipher the code groups and signature of an E-bar message. The message Setting and its indicator were obtained from the E-Bar Signal Book (Funksignalschluessel, Library Nos. 199.1 and 199.2). These Indicator Books were divided into two parts. Part I was a chart of valid Daily Tables for the calendar year. Part II consisted of 15 separate tables of 999 trigraphs, each numbered from 1 to 999, making a total of 14,985 possible three-letter message settings. Typical use consisted of taking the one table of 15 valid for the particular day, choosing any message setting therein to set in the windows of the machine, and placing the numerical equivalent (1-199) of the setting chosen as an unenciphered indicator on the message. See Figure 27 (6). The Reader will note an additional trigraph, IWS, shown as (5) in Figure 27. This was a Key-Type discriminant taken from the General Indicator Book (Kennbuch) in the fashion previously discussed and placed unenciphered in the heading of the message. The Germans started this practice of placing a trigraphic key discriminant during 1944, but the peak of E-bar traffic had been passed.

The signatures for this system were taken from the Naval List of Signatures (Marineliste, Library No. 209.2 and 209.3). This was the U-boat number plus a constant (formerly 500, later 600).

d) Method of Transmission and Acknowledgment.

As in the case of the Fleet Short Signal System and Weather messages, E-bar messages were transmitted once either on a normal U-boat frequency or on an "off-frequency" (for deception).

iv. Disguised Positions.

The reader will have observed that although the position of the originator of the Weather Message was reported in terms of Latitude and Longitude (57° N, 29° W), that of U-154 was reported as "Square BE, subsquare 88", and that of the E-Bar originator as "Square 8237". The two messages last mentioned are examples of a system widely employed by the Germans. It is so fully discussed and illustrated in Volume 2 of the R.I.P.'s of Op-20-GIA, as to require only very brief discussion here.

The basis of the cipher was a Grid System of the type used in all Navies. By it the entire water surface of the globe was divided into a series of rectangular mosaics, each designated by two letters, Figure 27a shows the division of the North Atlantic. From it we can see that U-154, being in Square BE, was in the area lying to the southwest of England. Needless to say, the report would have to be more accurate than that to satisfy control.

Greater and greater accuracy was obtained by a method of successive approximations. Each two letter square was divided into subsquares, each designated by two digits. The way in which this was done for Square AK is shown in Figure 27b. The process could be repeated by using two more digits to indicate the portion of the subsquare intended. The E-bar originator, being known by Control to be in a given general area, did not bother to report the letters for his square. He found it enough to say that he was in the upper right hand portion (37) of the south central (82) part of the large

Square which he knew Control understood.

To provide for additional security, ciphers were supplied to permit further disguise. The details varied from time to time as the War progressed, as discussed in the previously mentioned R.I.P. of GIA, but the principles remained the same. The letter designations were enciphered on one of a series of Bigram Tables, similar to those used for Setting Indicators and Key Designators. The numerical portion of the position was enciphered by an additive. The particular Bigram Table and Additive in effect for any given period were prescribed by an order of the "Address-Book" type, i.e. "Sophie Eberhardt, Wilhelmstrasse 72". This translated to mean, for example:

Sophie - Use Bigram Table No. 7.

Eberhardt - Write unenciphered square designations across top of columns in order, AA, AB ....

Wilhelmstrasse- The additive is to be applied to the first two digits only.

72 - The additive to apply is 72.

In each case the Christian name told the table to use, the Surname the method of using it, the Street the method of applying the additive, and the number what t he additive was.

The system was simple, easy to use, and quite effective.

ORIGINAL

b) Plain Text Usage

It is in this field that the worst of German crimes against themselves occurred. To make it clear, one must pause for a brief discussion of theory.

In all that we have seen heretofore by way of cryptographic abuse, we have noted that at worst for them and at best for the Allies, they only permitted the Allies, as a regular bidiurnal occurrence, to have a known Wheel Order and unknown Stecker and Setting confront them. The precise attack on this problem is quite complex, and is discussed in full in R[redacted]P. 450; but the principle involved is fairly simple. With an unknown Setting (of which 26^4, or roughly 450,000, are possible) some six Self Steckers (of which 230,000 are possible) and ten Stecker-Pairs (of which 624,000,000 are possible) we have a total of six and one half quintillion trials to make. This last figure is almost exactly twentysix to the 14th ~~power~~, and it is in this form that it is significant.

Suppose we took a given message, such as the sample previously shown in Figure 11 and had enough people and Enigmas to try deciphering it on the known Wheel Order with every possible Stecker at each possible Setting. We would then have to examine each decipherment to see whether it was gibberish or made sense. It is asking too much of a machine to expect that it analyze a set of supposed letters and see whether they make words, in general, and whether these words fit together. What a machine can do, however, is to detect whether a specified set of letters are produced in a specified order. Consequently, if we can tell the machine that it must find any Setting and Steckers with which Figure 11 will decipher to "Heil Hitler....",

we can expect it to do its job. However, there is one last fact to bear in mind. If we ask the machine simply to find the Settings at which there is some Stecker which would merely make the first letter of Figure 11 come out an H, we would find that there were innumerable Steckers at every setting which would do it. Having one letter produce another imposes a limitation of only 1 in 26. Two letters producing two others make the factor 1 in 26 squared, etc. Consequently, with 26 to the 14th possibilities, we need fourteen letters of plain text to be found, in order to get a unique answer! This is just the condition which made possible the use of the American and British counter machinery (Bombes) whose full practice is set out in ~~R.I.P.~~ 450.

Following along the same lines of reasoning, if one had both Wheel Order and Stecker known, the remaining unknown Setting (of which 26 to the 4th were possible) required a given assumption of only 4 letters of plain text to permit its recovery. Various other problems and conditions required correspondingly varying amounts of plain text to be supplied by the Germans. As usual, they constantly obliged, in the fashion next discussed.

The ground work was laid in the section of Enigma General Regulations, devoted to plain text. In it the reader was referred to "The Enigma General Procedure", Library No. 32.1.

In this latter manual one finds the details for handling general plain text messages. This included specific remarks about the exact way in which plain text is to be prepared, what kind of abbreviations are to be used, stress marks, designations of service stations, addressees and signatures, punctuation marks, numbers, summaries of text aids, urgency signs, making messages longer, how to pad and separate groups and, finally, still under the general heading of how to prepare plain text, a section on the method of subdividing messages. It is not necessary for the reader to know the details of all these subjects. It is important, however, to notice that German High Command went to great pains to be exact, rigid and formal in the smallest detail, especially as far as the actual wording of their messages is concerned. It was through this very fact that High Command tolerated no originality in the way in which plain text could be prepared, beyond the basic necessities of achieving clarity and avoiding confusion as far as originators and addressees were concerned, that the security of their machine system was eventually undone.

In every field, either from habit, or upon order, the Germans developed phrases or even whole sentences which remained fixed for varying lengths of time and were always to be found at or near the same spot in messages which could be identified by external characteristics (such as serial number, time of origin, etc.) Typical of the habitual type of phraseology were the weather reports out of the Bay of Biscaya and the beacon signals out of Norway. These and many others like them were long enough to break whole new Keys. Short bits of text such as "EINS" and "VON" abounded.

An example of a set language by command was the phraseology required to be used in Catchword Orders. The first step was formally

TOP SECRET-ULTRA

announced by a statement "the Catchword is being distributed". This meant that the Catchword was being sent to the commanding officers, but was not yet being used--because the order "readiness" has not yet been given. This first formal statement was followed by "Establish readiness for the Catchword"; "the Catchword is going into effect"; "the Catchword is going out of effect"; and finally, "the Catchword is invalid". Deviations from this phraseology, as usual, were made the subject of a specific order. How these portions of plain text were found and used is explained at length in [redacted]s 450 and 425, under the heading of "cribbing".

Worse than fixed phraseology, even, was the constant German practice of repeating in virtually unchanged form, the same text in both low and high grade systems, or in two or more high grade systems. Sometimes the fact that this had been done had to be inferred from collateral evidence; but the epitome of German stupidity came in those innumerable cases where even high ranking commands put out signals containing such phrases as "this is a repeat of my 0123/4/56 (which might not have been read)" or "to be rebroadcast on Series Arctic".

The frequency and regularity of this abuse of their machine is amply shown by an examination of the Keys tabulated in [redacted]. 475. More than 95 per cent of them were recovered by cryptanalysis--and always because the Germans made it possible to guess from four to fourteen letters of plain text. In these cases the Germans went just a bit too far in spotting the American cryptanalysts odds of 26^{14} to 1. However, even at this point, it was necessary for the Allies to use a battery of 115 counter-machines of the type shown in Figure 28, working 24 hours a day under the direction of a staff of expert cryptanalysts, employing the techniques described in [redacted]. 450.

The cryptographic crime of the German plain text usage was further intensified by the ease with which it could have been, and was not, remedied. The most obvious cure for the re-encodement practice was a rigid rule requiring paraphasing. This, of course, would not have obviated the harm done by standard phraseology. That, in turn, however, could have been made largely harmless by a simple practice employed by the Japanese and the Dutch - requiring that in writing up messages for sending they be started at random, varying points in the message blank - with the text being filled in till the end of the blank was reached, and then continued from the beginning. As for example:

In one case: "Fair with light winds -- Weather in the Bay of Biscay predicted for Tuesday:

And in the next "Predicted for Wednesday: Cloudy with dead calm -- weather in the Bay of Biscay"

Then, altho the standard phrase "Weather in the Bay of Biscay" could be counted on to occur, its location could not be bet upon. What would otherwise have been a single run on the Allied Analytical Machines, would thereby be magnified to as many runs as there were letters in the cipher text - since each (with few exceptions, discussed in [redacted]. No. 450) would be a possible location for the assumed plain text.

744Ø KCS (1)   27 February 1945   T.O.I. 1333 (2)

BOC (3)

(4) (5) (6)
2021/27/103

```
 (7)                                                      (Remaining
PFUEO CWWBS AFNXJ VGVNY FGWBU XYFML YNJUZ QAGVM ..... .....

Cipher Groups)     (7)
..... ..... ..... PFUEO
```

Underlying Message Translated:

FROM: 6th K Div
TO : KDK, K STAFF SOUTH, MOK SOUTH OP, ALSO TO 1st AND 8 DIV.

-PRIORITY-
-OFFIZIER N-

An attack with special explosives is planned by MEK 71 under covername 'L' against A/C and fuel stores on Ancona Airfield, as well as against oil pipe line along the coast. S-boat group will take 2 motor boats with raiding group of 10 men to a point about 15 to 20 miles abreast of Chiaravalle, approximately 6 miles Northwest of Ancona. From here the motor boats ((leaving S-boats)) will run in close to coast carrying rubber or collapsible boats and will disembark the raiding group.

1) Frequency on which heard
2) Time of Intercept
3) Call sign of Heiligenhafen, the Control Station
4) Time of Origin
5) Date
6) Serial Number
7) Indicator Group
8) Cipher Groups

TYPICAL NAVAL SABOTEUR (EICHENDORFF) MESSAGE

Figure 29

TOP SECRET-ULTRA

VI - NON ATLANTIC AND NON-U-BOAT SYSTEMS

This completes the discussion of the Atlantic U-Boat machine, accompanying Cipher Aids, and underlying codes, together with their related usages. These were the main assignments of the cryptanalysts of Op-20-GYA. As a collateral task, all Naval systems were jointly attacked by the Americans and the British. The following discussion is appended for the sake of completeness.

The code and cipher systems previously described are strictly naval in the sense that they were used by German Naval Warships, bases and other operational units. Certain other systems, such as Naval Saboteur, Merchant Marine, Naval Attache and Jap-German Liaison, were under Naval Control and made use, in part, of the Naval Enigma Machine. They differed in many features from the purely naval systems and supplemented them in that they were not originally designed for vessels or shore shations.

a. Naval Saboteur

(Eichendorff - ~~RIP~~ 475 page 35)
(Kleist - ~~RIP~~ 475 page 35)

Function - Naval Saboteur traffic was used in occupied countries by German units attempting sabotage and counterespionage behind British-American lines. The German covername for the general channel was Eichendorff, which appeared 7 May 1944. A special area key for Northern Italy called Kleist appeared 7 December 1944.

Type of Cipher - Both Eichendorff and Kleist were plain text encipherment on the Enigma machine.

Type of message - a typical Eichendorff message is shown in Figure 29. Unlike Naval Enigma proper, Eichendorff and Kleist messages were transmitted in five-letter groups.

Method of Enciphering - The indicator system for Eichendorff was first "throw-on". That is, an encipherment of the message setting two times, using the Grund (or Basic Setting for the day). The elements of the machine, (Wheels, Rings, Stecker, and Grund) were set up, and varied from day to day in the same fashion as in Enigma General Procedure. In October of 1944, the indicator system for Eichendorff changed to a singly enciphered message setting, using the Grund. Kleist also used a single enciphered message setting. Encipherment of the body of the message and the form for both Eichendorff and Kleist was made according to normal Enigma General Procedure.

Circuits Involved - About 75 stations in different areas were known to exist. The control station (BOC) was located at Heiligenhafen.

b. Merchant Marine

A) Coastal Waters - Although a large number of minor systems were used to communicate with merchant vessels in German Coastal Waters, no work was done on them by 20-G and very little is known here about the systems involved. It is known, however, that one of the primary systems was the "Schluessel H" or "Handelschiffe", the Merchant Navy Cipher System, which will be discussed below.

B) Distant Waters -

(Schluessel H or Handelsschiffe Lib. No. 315)
(Himalaya)
(Tibet [redacted] 475 page 35 and Lib. No. 140.2)
(Tibet Sonderschluessel [redacted] 475 page 35)
(Aegir [redacted] 475 page 35)

Function and Circuits Involved -

1. For Merchant ships in distant waters, the Germans relied at the beginning of the war on the powerful station "DAN" at Norddeich, supplemented by a set of transmitters at Nauen beamed to different areas in the world. This set-up remained in effect throughout the war, although German Merchant vessels have been gradually swept from the sea. In 1943 it was associated chiefly with blockade

runners between Germany and Japan. The attempt to safeguard the homecoming blockade runners in the winter 1943-44 led to the set-up of a station, MO'U in Paris, to send messages to those vessels as they approached the Biscay area. A considerable number of such messages were sent in 5-letter traffic enciphered by a system called Tibet, explained below. In order to hide the presence of these international messages the station continued to send a large volume of other signals, mostly dummies, which were not sent in the Tibet System, but in Hydra (see page), adapted to the appearance of 5-letter traffic with non-repeated indicators.

2. From 1942 on, the Germans extended their operations in the Far East. They were allowed by the Japanese to set-up transmitters of their own, first in Tokyo, later in Penang, Singapore, and Batavia in the "Southern Area". These stations were used originally to supplement the DAN service and employed the same ciphers. Later they began in independent net work handling traffic between the various German bases, as well as that to surface vessels. Messages sent in this manner were enciphered and deciphered by the Germans, prefixed by the cover words "SAKURA" (if sent by the Japanese Naval Radio) or "SYORI" (if sent by the Japanese Commercial Station). Both types of messages were sent with Japanese call signs and addresses. Sakura and Syori were abandoned in the summer of 1944, by which time the Germans had been allowed to set-up their own transmitters, first at Penang, then at Shonan (Singapore) and Djakarta (Batavia). Although the systems described above were created to handle Merchant Marine traffic, in 1943, U-boats operating in Far Eastern waters began to be included. Thus, we find in these ciphers a group

originally intended only for merchant vessels gradually became associated with purely naval operations.

Types of Codes and Ciphers used.

1. From the German Stations in Europe - In 1939 Dan Traffic to merchant ships was sent in a modification of the International Code with a very simple encipherment. In the course of the following year changes were made to more complex methods. Finally a complicated system of substitution-transposition was used and applied directly to plain text without any underlying code. This system was known as "Schluessel H" - "H" for "Handelsschliffe" (merchant ships). By 1942 "Schluessel H" had been superseded by another system known at "Himalaya". This system has not been broken, but it is known to have been likewise a transposition-substitution system similar in general pattern to its predecessor, and to the other hand systems, such as Henno and R.H.V. (see above) In November 1942 the Enigma Machine was introduced.

The Germans made no sharp demarcation between one merchant navy cipher system and the next one to go into effect. Normally, when a new key or system is introduced the old one is discontinued at the same day and hour. In the merchant navy traffic such was not the case. Merchant vessels were frequently out on cruises for long periods of time with the resultant impossibility of delivering new cipher data. As a result old keys often continued to be used on their original circuits and died out gradually. For example, several types of encipherment by the original Schluessel H were in use at the same time. These systems gave way gradually to Himalaya. In the late 1942 the Enigma Machine was introduced using "Schluessel M Tibet"; but a considerable portion of each day's traffic continued to be sent in Himalaya. The latter traffic diminished in volume and died out all together by August 1943.

The Tibet Enigma Keys continued to be used by DAN to the end of the war. In February 1945 messages out at DAN (evidently enciphered by a new system) began to appear. They continued intermittently along with Tibet, but were not accumulated in sufficient volume to make it clear just what sort of system was used. This system was tentatively called "EADSO" from one of the designators. It was probably a machine cipher.

In addition to the above main ciphers used by DAN the traffic carried at various times messages in "special ciphers". These special ciphers bore a general resemblance to the main ciphers with which they were associated. They used, however, one key table and were restricted in use to one particular ship for each special cipher. They were used for especially confidential messages and were so designed that compromise of the major cipher system would still make it possible to communicate securely with DAN and other ships.

2. From the German Stations in Japan.

Until July of 1943, the traffic from the German Stations in Japan was mostly enciphered in Tibet with a diminishing quantity of Himalaya. At the end of July 1943, however, a cipher called "Aegir" was introduced. Aegir was to be used for traffic between bases while Tibet would be used for messages to vessels at sea. This distinction between Aegir and Tibet continued to the end of the war.

A third cipher entered the Far Eastern pattern with the

~~R.I.~~P. No. 401 TOP SECRET-ULTRA ORIGINAL

```
(1)
8F6                                                      7 March '45
(2) (3) (4)                                              (5)
2100/7/NR24                                              W43


 (6)   (7)                                                     (8)
IITAM HBTBY ZKWOW AIQXQ CQLKS ZPFLN DDDLQ UZKOM MSMRH ZKIJJ
                    (7)   (6)
VIQRC ----- ----- KMHHR QGSFU
```

Underlying text translated:

To: A183

1) On the night of 3/3 a small Japanese vessel was lost in LS 7993 ((06.27° S - 112.57° E)). Possibly a mine.

2) At 1419A/6/3 There was an enemy boat (Submarine) in LS8875 ((06.33° S - 114.03° E))

1) Transmitting Station Tokyo
2) Time of Origin
3) Date
4) Serial Number
5) Group Count
6) Designators
7) Indicators
8) Cipher Text

TYPICAL FAR EAST (TIBET) MESSAGE

Figure 30

establishment of Penang as a base for U-boats operating in the Indian Ocean. Penang was supplied with the general U-boat cipher (Triton) and in July of 1944 began to send messages on a new circuit called "TAIFUN". These messages were sent in the general U-boat cipher (Triton) in the regular 4-letter form. U-boats in the Indian Ocean had previously been equipped with both Tibet and Aegir, in addition to Triton. In January 1944 U-boats had been ordered to destroy Aegir keys if they were not needed; but they continued to use Tibet in Japanese controlled waters east of Penang. By the end of 1944 activities were centered further eastward than before, with the resulting increase in the use of Tibet for U-boats. This led to two changes: First, in February 1945 Tibet was equipped with an officer (Offizier) inner encipherment, which it never had before. In April of 1944 the Taifun circuit was shifted over to Tibet with certain changes, introduced under a cover name "Stichwort Bremen". The exact fashion in which this change which differentiated the new traffic from regular Tibet is not known. These two changes affected the Far East only and were apparently devised by the authorities there, rather than in Germany, in violation of the strict rule that all responsibility for cipher innovations would be centered in Section IV of the Naval War Staff in Germany. The changes apparently took place during a series of misunderstandings on cipher matters between Berlin and Tokyo, caused primarily by delays and difficulties in communication.

Types of Messages and Illustrative Examples.

An example of a ciphered message sent in the Tibet System will be found in figure 30 . Since the special ciphers for Tibet

TOP SECRET-ULTRA

No. 401 ORIGINAL

```
9795  KCS.  (1)       23 January 1945      T.O.I. 1926 (2)

DGM (3)

 (4) (5)(6)
1410/23/1

   (7)
TQSYH LESQJ IQNVK LYHVG LCNSL HJCMS OMYKB HMPEL UFZDI .....

                              (7)
..... ..... ..... MRWQH FVBJR
```

Underlying Message Translated:

TO: 'RIO GRANDE' 56

--FOR SO ONLY--

1) On the 16th a Westbound convoy was in the North Channel and may today be in approximately SQ AK 57 ((54.09N-34.45W 'B')), or 73 ((53.15N - 36.15W 'B')).

2) Therefore proceed Northward at once; R/V is shifted 150 miles to the North. Boat has been ordered to wait for you until 1800A and then to go to the new R/V to the North.

3) If both vessels are ((already)) together the transfer is to be speeded up or a new R/V agreed upon.

1) Frequency on which heard
2) Time of Intercept
3) Call Sign
4) Time of Origin
5) Date
6) Serial Number
7) Indicators
8) Cipher Text

TYPICAL BLOCKADE RUNNER (TIBET SONDERSCHLUESSEL) MESSAGE

Figure 31

only involved a different indicator system, the form of the message, Figure 31, resembled that in Figure 30 for a normal Tibet message. Aegir was the one major system which was not broken during the active stages of the war. (Original break made 25 June 1945.)

Method of Enciphering.

I. Indicator System Himah

As a result of the practice of sending messages on the same circuit with different means of encipherment, plus the desire to keep them looking alike externally, an elaborate system of identification was set up to discriminate the various Merchant Marine and U-boat systems. It served the same function as the Bigram Tables for the Enigma general procedure, but operated quite differently. The first and last group of each five-letter message served as system "Designators". They were chosen from a list of pentagrams assigned to the particular cipher in which the message was enciphered. For list see ~~R.I.P~~. 475 pp. 925 to 928. The use of two groups from the same list provided a garble check. As care was taken not to choose identical groups for the same message, repeats were avoided and the existence of a system of discriminating groups was disguised. Schluessel H had only a few such groups at first. Later the list contained as many as sixty groups. Himalaya had some 450 designators. It is interesting to note that the Himalaya indicators differed from the others in that they were trigrams and not pentagrams. The trigrams were filled in to 5-letters before transmission by two extra letters which served to indicate the particular tables used. Tibet had over 800 indicators. This meant that Tibet traffic could go on for several months without repeats. The special ciphers which were less freely used had smaller lists. Nothing is known about those for Himalaya except that they existed. Those special ciphers for Tibet (Tibet Sonderschluessel) had lists of 10 designators each. In the winter of 1943-44, when several blockade runners were coming around from Japan at the same time, considerable use was made of these special ciphers to each one. In addition a "General Special Cipher" (Geheinsamer Sonderschluessel) was made up for use by all of them at once. This system combined several of the special designator lists into a major one and formed new settings for the machine by a slide on the main Tibet System.

2. Body of Messages.

The method used for enciphering plain text by Schluessel H (Handelsschiffe) was substitution-transposition, explained in a special report in Library No. 314. Since no such traffic was processed in America, details of encipherment are not necessary here. The same is true for Himalaya. This system, however, has not been broken.

Messages enciphering plain text by either Tibet or Tibet Sonderschluessel involved the Enigma Machine with the same variable elements as in normal general Enigma procedure. The basic setting (Grund) and Stecker changed daily at noon, the Wheel Order and Rings eight times a month, that is every four, or in some instances, five or three days. In both Tibet and Tibet Sonderschluessel the second and penultimate groups of any message were indicators determining the message setting. The machine was three wheel and the indicators are "throw-on", except that two dummy letters are necessary to make up a five-letter group. For example:

```
Text of message:  ABTIG LPGRZ ...........FGCRQ KNEOY
Decipherment:       (1)  **ABC ...........**ABC  (2)
```

where (1) and (2) are designators and * denotes nulls. The message setting in this case would be ABC.

Although no Aegir message was broken before V-E Day, it was known that the system involved (A) indicators which bigram in the fashion used in Enigma General Procedure and (B) the three (or four wheel) message settings were derived for the Enigma Machine according to Enigma General Procedure. It was conjectured that the variable elements of the machine change from day to day in the fashion prescribed by Enigma General Procedure.

Comparison of the Tibet and Aegir Cipher Systems.

A revealing comparison may be made between Tibet, the major machine cipher used on the Merchant Navy Circuit from 1942 on and Aegir, the regular Enigma Cipher used by war vessels in distant waters.

They resemble each other in that:

1. Both were transmitted on the same circuit from DAN.

2. Keys for both systems were issued well in advance. This was necessary for ships in distant waters.

3. Provision was made in both systems for "Special Ciphers" for independent ships. ("Schiffssonderschluessel" related to Aegir and "Tibet Sonderschluessel" related to Tibet). Each special cipher was held by only one ship and by its base. The special

ciphers were sent interspersed with messages on the regular keys and were not distinguishable from them externally.

4. After the gradual driving of the German surface vessels from the high seas, both types of DAN traffic continued to be sent. Both were directed to the Far East and contained chiefly routine messages to base personnel. At the same time both Aegir and Tibet came to be of increased importance for traffic within the Far East itself.

On the other hand the differences between these two systems were:

1. Aegir was sent in 4-letter groups like other naval Enigma traffic. The indicators were repeated at the end of the message and bigrammed. Tibet was sent in 5-letter groups with non-repeated indicators, but the first and last groups were designators chosen from a list.

2. Tibet used the standard Naval (3-Wheel) Enigma machine with the eight naval wheels. Only the Bruno Beta reflector and reflector wheel, however, was used. Steckers and Grunds changed daily, but the Wheel Order and Rings were valid for three or four days, giving a total of eight Wheel Orders a month.

3. Unlike other Naval Enigma Systems Tibet had no early provision for officer (Offizier) encipherments. Apparently no need for such was felt for merchant vessels. In February 1945 when the cipher had come to be used exclusively for U-boat operations in the Far East a provision was made for an officer (Offizier) encipherment. This was apparently done without authority from Berlin by the authorities in the Far East and was used only in that area.

c . Naval Attache Systems

Function and Areas Involved -

The German Navy regularly carried on cipher communication with attaches in various capitals. Little is known about most of the systems used. There is some evidence that the system in use in 1944 to various European cities (Madrid, Lisbon, Instanbul) was the same. The system used between Ber~~tok~~lin and Tokyo was known as "Bertok".

Types of Cipyer System.

Bertok used the Enigma machine. It was probably the successor of an old 5-letter code and therefore continued to be sent in 5-letter groups with no externally apparent indicators. The Enigma Machine was in use in 1940 in this system and continued throughout the war.

Type of Message.

Bertok messages were originally sent by International Circuits with Commercial headings. These used the plain language addresses "Diplogerma Maratt Tokio" ('German Diplomatic Naval Attache Tokyo') and "Kriegsmarine Berlin" ('Navy Berlin').

In July 1943 the German-Japanese communications agreement went into effect. Under it a direct circuit was set up with German radio personnel at one end and Japanese at the other. The Germans never found the circuit nor the Japanese operators satisfactory. Hence they continued to make supplementary use of the commercial circuits.

On all the transmissions, however, the Germans adopted at this time (July 1943) what became the characteristic external identifying

~~R.I.P.~~ No. 401 TOP SECRET-ULTRA ORIGINAL

DAJ DE JZ2 (1) May 1945

(2) (3) (4)
1726/5/PPA35

(5) (6)
JAPTN DGEOH DGEOH XUWZX SLCAI VJQGA RGIIK KXYUQ WVWLP HMAOC

RARUM .... ZLIGN

Underlying Message Translated:

((FROM: TOKYO)) FOR SO ONLY 87

((TO : BERLIN)) FOR GRAND ADM DOENITZ

--OFFIZIER L--

Combat action of East Asia U/B's has ceased. Return of U/B's impossible, since they are not ready for travelling.

((Signed)) WENNEKER

1) Call Signs
2) Time of Origin
3) Date
4) Serial Number
5) Indicators
6) Cipher Text

TYPICAL NAVAL ATTACHE (BERTOK) MESSAGE

Figure 32

symbols of the traffic. This consisted of the letters PPB for traffic originating in Berlin and PPA for traffic originating in Tokyo. Both symbols were followed by a two digit serial number. The symbols and the two digit serial number were prefixed to the text of the message heading of the indicators. See Figure 32.

Method of Enciphering.

Indicators

The bigram tables were not used, but the message setting was enciphered twice on the German Enigma Machine set at the Grund. The resultant two 4-letter indicators were filled out to 5-letter groups. This procedure is exactly like the indicator system for Tibet except that the settings involved for Tibet were 4-letter. An additional pecularity of the Bertok indicator system was the rule that Tokyo was to use only the first thirteen letters of the alphabet in making the first letter of the message setting while Berlin was only to use the last thirteen letters.

The two indicator groups were originally set at the beginning and end of the message, masquerading as message groups. Beginning 23 May, 1942 this was changed to the second and last groups. A new initial group apparently consisted of dummy letters; for no function for it was ever discovered.

For example:

Text of message:	PPA63 XDFWI LZSRH . . . . . MJGTV
Decipherment of indicators	*ABCD . . . . . *ABCD

On 10 January 1945 this system of "throw-on" indicators was given up. Instead the message was enciphered once and the indicator repeated as the second and third groups of the message. This was the first violation of the usual German rule against repeated

consecutive groups.

Body of Message.

The Enigma machine was used to encipher the body of the message. The Grund changed daily. The Stecker was valid for two days. The same Wheel Order and Rings held for a period of ten days. An officer (Offizier) encipherment was available using the same Stecker, Wheels and Rings as regular messages and having 26 special settings, designated by the phonetic Anton, Bruno . . . . . Zet.

Because of distances involved, Bertok keys were issued for a calendar year at a time.

d. German-Japanese Liaison Systems.

Function -

As part of the German-Japanese communications agreement, provision was made for direct radio traffic between German and Japanese vessels which happened to meet, mostly in the Indian Ocean. No great use was made of these systems, since communication by German vessels in the Far East was regularly with German stations ashore, and carried on whatever negotiations were necessary directly with the Japanese. Some traffic is known to have been sent by these systems from Germany to Japanese submarines which were being used in 1944 as blockade runners. According to the traffic between Berlin and Tokyo the systems involved were made up by the Germans and sent to the Japanese.

Systems -

Three types of cipher were used on the Naval Attache circuits. They were

1) A special variety of the Enigma, known by the covername of

```
     (1)
A)   DAN   C" C"                         6 March 1944

     (2) (3)(4)               (5)
     1814/6/27                 51

     HCHFZ JIISW NXFZQ JOHCG TSWYI FBHKD TJLJH XLHQT NZEXR YLIAE
     XHQHW LAYXW KGDRX FLDPC PYLSE XEBDP HPQTY YEKHN RGZVX XNZHP
     XGQPL ACDKI VUPGV NUSUZ HALMB ACBHI LVYVC HNOYU XIACT IVVKG
     UJEPJ BOJHX KHTFQ ZVVTZ VBDDA MLVPS ZMJCU AZMWU WSAXF ZVPUF
     LULIF EZATT ASOLY JRDVP HYVRE GSBBV OQJMN YPUMA IQWQJ

     12725 KCS (6)

     (1)
B)   DAN   C" C"                         6 March 1944
     (2) (3)(4)               (5)
     1947/6/28                 51

     DJYQT FKCHD JEBKM QZDFY QLHCP TLKUL RYIAA BDGEJ XWDBY BABMH
     LSVLF NCSUA BNBKW BRNRP XZOKE UJDLO QYYGV ZGHXG IGJLO ODTRC
     SQQOO GTBET RNGUP IVWGF JNGBW MISQY KVYJI GCTYO YLWWC CXFPM
     IKVHQ RRBJA ZLZAE SAMPF BJXOT QOYGQ TYQEI NHZYQ ZCWOP XBOUJ
     AOEIV GGJKG MKHNB PQKBI ZNVEH GENJU MNGEI FGJXU UMWRC

     12725 KCS (6)

     (1)
C)   DAN   C"  C"                        10 March 1944

     (2) (3)(4)               (5)
     0251/10/29                27

     IHXLP RWUIK IRCYP XNVSF ERKMK MNJZZ ZTDBF GMFBO JGADL KJSVG
     JKSGB JQFKU FXWVS MWGKO CPKNQ KFDDR MRDSQ OAOIU GAIRM ZZCBQ
     MEFMG ZVAOQ QWJXN JENOF DBHVK

     1907 KCS (6)
```

1) Call Sign
2) Time of Origin
3) Date
4) Serial Number
5) Group Count
6) Frequency

THREE SAMPLE UNBROKEN TIRPITZ MESSAGES
SENT TO JAP SUB "GENMATSU"

Figure 33

"Tirpitz".

2) A transposition-substitution hand system, known as "Sumatra" (Library No. 140.1).

3) A short signal code, known as "Togo" (Library No. 140.2).

A copy of the Enigma was captured in Western France in the summer of 1944, but at the time it was not known that this was, in fact, the machine in question. All that was then known was that it had been intended for shipment to Japan. Its positive identification was delayed until the fall of Germany. At that time the Japanese Diplomats in Europe were driven to emergency use of an Enigma which, in collateral traffic, they described as "Tirpitz". The messages which they sent read on the captured machine. It was an unsteckered, multiple-turnover device using three out of eight specially wired wheels and a rotatable reflector.

The full details of Sumatra were gotten by capture. It used the International Signal Code as a basis. The code groups were first treated by a 3-alphabet substitution. The results were put through a simple columnar transposition before transmission.

A short signal code known as "Togo". This system consisted of a list of over 800 meanings, each numbered. The numbers were to be enciphered into letters by tables which were changed periodically.

Sample Messages:

No actual samples of either Togo or Sumatra were ever identified. It is known that Tirpitz was used to communicate with the Jap Sub "Ginmatsu" or "Kiefer" when she tried to put into Lorient in 1944. The messages to her are copied in Figure 33, but have so far not been read.

GERMAN NAME	ALLIED NAME	CHANNELS OF USE	PURPOSE OF USE	USED FROM TO	NUMBER OF LETTERS IN GROUPS OF CODE	METHOD OF ENCIPHERING	INDICATORS	LIBRARY NO.
ORTUNGSFUNKSIGNAL	Z-BAR SIGNAL	BOULOGNE TO SHIPS IN CHANNEL	REPORTS OF D/F s IN CHANNEL	9/42 –		ENIGMA	2 FIGURE	4-200
FLUGZEUGSIGNAL	GERMAN NAVAL AIR CODE	AIRCRAFT TO BASE	REPORTS OF AIRCRAFT GRID POSITION	'41	3 LETTER	CODE		4-237
SEENOTFUNKSIGNAL	SN OR "SEA RESCUE"	UNITS TO SEA RESCUE SERVIC	REPORTS	'40-'43	3 LETTER	CODE	"SN"	4
HAFENSCHUTZFUNKSIGNA	HF OR "HARBOR DEFENSE"	SMALL VESSELS TO COASTAL AUTHORITY	REPORTS AND EMERGENCY	'40-	3 LETTER	CODE	"HF"	4
FUNKVERKEHR KUESTE	FK SIGNALS	FRENCH COASTAL BATTERIES	ANTI-INVASION	– '44	3 LETTER	CODE	FK	4-300-1
SCHNEPFE STURMVOGEL SCHWALBE		SMALL UNITS IN: HOME WATERS MEDITERRANEAN BLACK SEA	EMERGENCY	– '44	2 LETTER	CODE		4
	LL SIGNALS	SMALL CRAFT IN: MEDITERRANEAN AND ADRIATIC	SMALL CRAFT INTELLIGENCE		2 LETTER	CODE	LL	4
BEFEHLS UND MELDE VERFAHREN KANAL	PP SIGNALS	SMALL BOATS IN CHANNEL	EMERGENCY		2 LETTER	CODE	3 FIGURES FIRST Ø	4-39
BIBER		"	"		2 LETTER	CODE	QQ	4
	MI SIGNALS	BALTIC CRAFT	REPORTS OF SWEPT MINE WAYS		2 LETTER	CODE	MI; LATER ZZ	4
	BALTIC XX SIGNALS	FAST MOTOR BOATS IN BALTIC	PRACTICE	'43-PRES.	2 LETTER	CODE		4
	ABC SIGNALS	CHANNEL LIGHT HOUSES	REPORTS	'40-'42	3 LETTER	CODE		4
	DELTA SIGNALS	MINE SWEEPERS IN CHANNEL	REPORTS	'42-'43	2 LETTER	CODE		4
	3 FIGURE RADAR	RADAR STATION	RADAR REPORTS	'43 -	3 FIGURES	CODE		4
	BZ SIGNALS	RADAR INTERCEPTION CENTER	CENTRAL RADAR REPORTS	'44-'44	5 LETTER	CODE		4
MARINENOTSCHLUESSEL WEST	THE FORTRESS CHIS	BELEAGURED FRENCH FORTRESSES	FINAL STAGES OF EMERGENCY			KEY WORD TRANSPOSITION	TIME/DATE GROUP	4
KURIERSIGNALVERFAHREN	FREQUENCY DEVIATION PLAN	CONTROL→U-BOAT	AVOIDING ENEMY INTERCEPTION OF MESSAGES	'44-'45	2 LETTER	ENIGMA	INDICATOR BOOK (K-BUCH)	4
U-BOOTSKARTENSCHLUESSEL KENNWORT "ADDRESSBUCK"	ADDRESS BOOK SYSTEM	U-BOATS TO CONTROL	ENCIPHERING GEOGRAPHICAL NAVAL SQUARES		2 LETTER	ENIGMA		4-24-8

MINOR GERMAN NAVAL CODES AND CIPHERS

FIGURE 34

e. Minor Codes and Ciphers

Since the beginning of the war, the Germans have used a large variety of two and three letter codes for coastal traffic. See Figure 34, a chart of some of the more significant minor codes. Many experiments in different types have been made by the German High Command. Some of these codes were abandoned after a very short life. Those which did survive were modified from time to time, always in the direction of greater complexity and security.

There were, in addition, several other second class ciphers used by the German Merchant Navy and by subsidiary vessels. One such cipher is known as the German Merchant Navy Cipher (Schluessel H-Nordwest). The ciphering process used here is similar to the Reserve Hand Procedure described above. The plain text is first transposed and then enciphered by vertical bigrammatic substitution on five different bigram tables. Formerly, before August 1943, the plain text was encoded on the International Signal Book and the code groups were then transposed and substituted. The number of bigram tables used for the later substitution process is not known with certainty, but it is assumed that there are twenty. The transposition sequence is no greater than seventeen. For indicators, 5-letter groups are taken at random from the International Signal Book. Traffic in this channel was never very heavy, about fifteen to twenty signals a week, and it is probable that the major portion of them contained information sent in major machine channels.

Another second class cipher used by guard ships, mine sweepers, aircraft recovery vessels, tugs, pilot boards and by the shore authorities and ships for communications with small craft is called Werftschluessel. In this cipher, as in the German Merchant Navy Cipher, plain language is enciphered by vertical bigrammatic substitution, and keys are valid for periods between four and eight weeks.

VII. The Indictment of German Cryptographers.

a) A Preview of the Counts.

In legal terms, the German Cryptographers did carelessly and recklessly with great lack of forethought, and inspired by overconfidence, during the period of World War II, in the Atlantic Waters and elsewhere, both by omission and commission disastrously impair the security of a first rate cipher device to the great detriment of the German Navy and did thereby give great aid and comfort to the enemies of the Reich, contrary to the rules of sound communications practice, IN THAT

1. They did fail to employ on the Naval Machine the device of multiple-notched Rings, which would have greatly increased the irregularity of the motion of the machine, had been successfully employed in Commercial Models, and could have been issued without difficulty.

2. They did fail to vary their Steckers as greatly as possible, and instead, adhered to a needless practice of always having Six Selfs and ten Pairs - all reciprocal.

3. They did fail to adopt the Pluggable Reflector, successfully employed by the German Air Force.

4. They did prepare their cipher aids in systematic, rather than random fashion, so that cryptanalysis need not be complete, but could

stop when the system had been detected, and decryption proceed from there.

5. They did make their changes in Cryptographic aids in such manner that each new element appeared in company with old elements as well, thus weakening, and in some cases destroying the usefulness and security of the new elements.

6. They did not only permit, but, as well, instructed the users of the Enigma and its Cipher Aids consistently to repeat identical phraseology in such fashion that Allied Cryptanalysts were enabled to surround the Problems facing them with sufficient conditions to insure the recovery of the unique, correct solutions.

7. They did fail to provide their Communicators with the simple and effective safeguards against their natural habits - namely, the variation of starting point of their text.

b) <u>The moral</u> to be drawn can be fairly simply stated in terms of sound Cryptography, in terms of the following points:-

1. All that any cipher machine can do is to generate a certain number of the 26 factorial possible monoalphabetic substitutions and to generate them in a certain number of different orders.

1a. Any modifications in design which can be made to increase the number of substitutions and to vary the order of their generation should be made whenever the cost does not overbalance the return.

2. The number of substitutions which can be generated by a machine and of the ways in which they can be varied is always less than all possible - generally by a very considerable factor, and generally so slight that with enough high speed machinery all possibilities can be

tried by cryptanalysts.

2a. One should never permit sufficient plain text to be paired with corresponding cipher text so that the two combined impose sufficiently rigid conditions to determine a unique solution.

3. In preparing instructions or collateral aids for use with a machine, the use of system in filling in the variable elements can always be detected by an examination of a part of the whole field.

3a. Repetitions which would occur from chance in filling out an assigned list of variable key or collateral aid elements should be freely permitted.

4. Rigid and formal rules of phraseology or of selection of variable elements are analogous to the points covered in 2 and 3.

4a. Originality in expression, so long as clarity is not sacrificed should be encouraged; the practice of starting text at varying points within the text should be required; and originators should be supplied with a simple device (such as a small plastic top with letters and digits marked around the edge) to be used in making random selections of variable elements.

5. A new portion of a Key, or one new element in a set of simultaneously used Cipher Aids, is made worthless to a varying degree by the continuance in effect of the remaining portions of the Key or of the other Cipher Aids in the set.

5a. Whenever one element in a system is changed, all should be changed.