

Kriegsmarine

M4-UKW = B

M4-UKW = C

OFFICER-TO-OFFICER PROCEDURE

Decrypting a Kriegsmarine 4-rotor Officer-to-Officer message

Note: This procedure takes for granted that you already know the Basic Enigma 3-rotor Wehrmacht operating procedure and the Basic Enigma 4-rotor Kriegsmarine operating procedure. This procedure presents the new challenge of double encryption. Officer-to-Officer messages were reserved for only the most secret communications—so secret that even the ship’s regular radio/Enigma operator could not know the contents.

Enigma World Code Group (EWCG) Note: For EWCG purposes, the receiver of this message will have to play the roles of both the Officer and the Radio Operator. The sections of this procedure are clearly labeled as to which role the operator is to play, and when.

1. Print-out a paper copy of all of these Kriegsmarine documents by clicking on the links:
 - This Procedure
 - Inner Settings
 - Outer Settings
 - Bigram Table
 - “Offizier” (German for “Officer”) Key Sheet

Radio Operator

2. Follow the “Basic Procedure: Decrypting a Kriegsmarine 4-rotor message,” from step 2 (with the addition of some “Officer-to-Officer” material shown in step II, below) through step 25, to put the daily key into the Enigma machine, then stop. Basic Procedure steps 2 – 25, in Roman numerals, are reprinted here for your convenience:

- II. Note: If you do not have a 4-rotor Enigma “Officer-to-Officer” message already provided for you, we will use your encrypted message from “Encrypting and Sending a Kriegsmarine 4-rotor Officer-to-Officer message” for this decrypting exercise. Notice the first and second 4-letter groups in the message. The Message Indicators that we need for decryption are hidden inside these letter groups. Write these letter groups, one above the other, as shown:

K I B L

K C L H

- III. Re-group the letters following this pattern:

K-----I B----L

K----C L----H

You get: KI BL KC LH

IV. Now, write-out the pairs of letters like this:

KI = BL = KC = LH =

V. Get your printed-out bigram table. Read the instructions on how to use it.

VI. Using the bigram table, decrypt the pairs of letters you have just written, like this:

KI = LV BL = PR KC = IM LH = ZQ

VII. Write-out the decrypted pairs of letters, like this:

LV PR IM ZQ

VIII. Add a short arrow and a long arrow to each pair of letters, as follows:

L V P R I M Z Q
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
L V P R I M Z Q
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
L V P R I M Z Q

IX. Write the short-arrow letters, in order, from left to right:

L P I Z

X. Drop the first letter:

P I Z

XI. Write the long-arrow letters, in order, from left to right:

V R M Q

XII. Drop the last letter:

V R M

Write down this trigram so that you can use it again in Step XXIV.

- XIII. Look at the trigram from step X: PIZ. Using the "Inner Settings" table, scan-down the "Key Ind." (Key Indicator) column and verify that the Key Indicator matches the correct date on the Message Header. We are using date 27.
- XIV. The "UKW" column shows "B," which means that we will be using the Kriegsmarine M4-UKW = B machine. If you will be using a Key Indicator that has a "C" in this column, select the M4-UKW = C machine.
- XV. Open the cover of the Enigma simulator. Click on the letter "B" located at the left end of the rotor shaft until it shows either "Kriegsmarine M4-UKW = B" or "Kriegsmarine M4-UKW = C," depending on which machine you are using.
- XVI. Remove rotors I, II, and III from the rotor shaft and store them in the box, in order.
- XVII. The "Inner Settings" table gives you the rotor settings you will use. Click on the Beta or Gamma rotor (depending on which machine you are using) in the box, check the end of the rotor to ensure it shows the letter "A," then install the rotor on the left end of the rotor shaft.
- XVIII. Then select rotor II, set it to the letter "T," and install it next to the Beta or Gamma rotor on the shaft.
- XIX. Working from left to right, set and install the last two rotors onto the shaft. Close the Enigma cover.
- XX. Click on the Stecker plugboard. You will notice that the plugboard is numbered, not lettered.
- XXI. Using the "Outer Settings" table, scan down the "Key Ind." (Key Indicator) column until you have located the Key Indicator and date of the month you are using. We are using Key Indicator PIZ on date 27.
- XXII. Set the Stecker plugs as indicated. Stecker settings are reprinted here for your convenience:

16/2 25/21 6/20 9/17 22/1 15/4 18/26 8/23 3/14 5/19

Return to the Enigma top view.

- XXIII. The last column on the “Outer Settings” table is labeled, “Basic Start Position.” Dial-in the “Basic Start Position” letters into the 4 rotors, in order, from left to right. The Basic Start Position is T C X K.
- XXIV. Using the Enigma keyboard, slowly type-in the trigram from step XII: VRM. As each letter is typed, a letter will illuminate on the Enigma lightboard. Write-down the three letters as they illuminate, in order. For our practice message, they should read KKZ.
- XXV. Set these three illuminated letters into the three “regular” rotors, from left to right. Don’t touch the Beta/Gamma rotor. The setting now is T K K Z. This is called the “Final Start Position.”

- 3. Decrypt the entire message. Do not try to decrypt the two 4-letter Message Indicators at the beginning and end of the message.
 - a. You may do this in the original way by keying-in each letter on the Enigma keyboard and writing down the letters that illuminate on the Enigma lamp-bulb panel.
 - b. Another method is presented in steps 26 – 34 in the “Basic Procedure: Decrypting a Kriegsmarine 4-rotor message.” Steps 26-34 from the “Basic Procedure: Decrypting a Kriegsmarine 4-rotor message,” are reprinted here for your convenience, numbered in Roman numerals:

- XXVI. Go back to your Enigma keyboard. Click on the small metal plate at the bottom of the Enigma that displays, “Show textbox.”
- XXVII. The two trigrams from step XXIV (VRM and KKZ) will already be in the textbox. Ignore these for now.
- XXVIII. Hover over the box at the top right-hand corner of the Enigma simulator. Click on “Auto typing.” A box entitled “Enigma Auto Typing” will appear.
- XXIX. Find the message that you want to decrypt. Highlight only the text portion of the message, not the two 4-letter Message Indicators at both ends of the message, and not any 3-letter trigrams that may be hanging around.
- XXX. Right click and copy the message text.
- XXXI. Right click and paste the message text into the “Enigma Auto Typing” box.
- XXXII. Do you see the “Start” button? Click it!
- XXXIII. After the message is finished printing, hover over the textbox and click when, “Click here to Copy Output to Clipboard” is displayed.
- XXXIV. Your decrypted message will appear on the screen.
- XXXV. Highlight and copy the text from the clipboard screen.
- XXXVI. Open a blank word document and paste the decrypted message onto the screen. This will be used in the next section.

3. (Continued)

The results should look like this:

BERG MANX VONX KULP XOFF IZIE RXKA RLRH KKOC DUZB CUGL GSFH VAVG
PLIX HTAB LYXL TIXK ALHR DNFM XWRQ DYHU RGUV IBMJ ZQ

4. Notice if there is a Plain-Language Heading at the beginning of the message. Do this by looking for the “Offizier” flag word, followed by an **X**, followed by a code name.
5. If a Plain-Language Heading is present, contact an officer and give him the hand-printed message.

Officer

6. Verify with the radio operator that the daily key settings for the Enigma have been properly set into the Enigma machine.
7. Secure private use of the Enigma machine from the radio operator.
8. Verify that the “receiver” and “sender” entries appear to be correct in the Plain-Language Heading.
9. Find the code name in the Plain-Language Heading. We are using “Karl” as our example.
10. Minimize the word document.
11. Click on “Close” on the Smart Clipboard.
12. Now find the matching code name on the “Offizier” Key Sheet. The random 4-letter group that corresponds with the code name Karl is called the “Message Start Position.” Our Message Start Position is W E W N.
13. Dial-in the “Message Start Position” letters, W E W N, into the 4 rotors, in order, from left to right.
14. Again using the “Offizier” Key Sheet, select the correct row of Stecker settings you will use according to today’s date. We are using date 27.
15. Click on that part of the Enigma simulator that displays the Stecker settings.



16. Click on each black number to clear the existing daily key’s Stecker settings.

17. Replace the daily key's Stecker settings with the "Offizier" Key Sheet Stecker settings. "Offizier" Key Sheet Stecker settings are reprinted here for your convenience:

10/15 23/26 11/2 20/24 7/3 9/16 17/12 18/21 22/25 8/5

18. Return to the Enigma top view.

19. Decrypt the "still-encrypted" portion of the message using either of these methods:

- a. You may do this is the original way by keying-in each letter on the Enigma machine, one letter at a time, and recording the lamp-bulb letters that illuminate, in sequence, on a piece of paper. Begin with the first letter **after** the code name in the Plain-Language Heading.

The "still-encrypted" portion of the practice message is reprinted here for your convenience.

RHKK OCDU ZBCU GLGS FHVA VGPL IXHT ABLY XLTI XKAL HRDN FMXW RQDY
HURG UVIB MJZQ

- b. Another method to decrypt the "still-encrypted" portion of the message uses the power of "Auto type."
(Note: See the October 2013 Enigma newsletter

http://media.wix.com/ugd/abb462_2cca03b7c8b720634b3d1780a978bacd.pdf for a quick introduction to Auto Type.

- Open the word document that you created in Step XXXVI.
- Highlight and copy the "still-encrypted" portion of the message. Begin with the first letter **after** the code name in the Plain-Language Heading.
- Go to the Enigma top view.
- Click on "Auto Type."
- Click on "Get Clipboard."
- Click "Yes." This will replace the old message with the new message.
- Click "Start."
- After the message is finished printing, hover over the textbox and click when, "Click here to Copy Output to Clipboard" is displayed.
- Your message will be displayed on the clipboard screen.

20. The decrypted portion of the message should read like this:

FOUR TORPEDOES FAILED TO EXPLODE. SUSPECT SABOTAGE. CHECK ALL
DETONATORS.

21. When finished, scramble the rotors, and scramble or delete the Stecker plug settings.

22. Return to the Enigma top view.

23. Return control of the Enigma machine back to the radio operator.

Radio Operator

24. Return the rotors and Steckers to their “Final Start Position.” For us, the “Final Start Position” for the rotors is T K K Z (the same as in step Roman numeral XXV). The regular daily settings for the Steckers are:

16/2 25/21 6/20 9/17 22/1 15/4 18/26 8/23 3/14 5/19

Return to the Enigma top view.