H. Dv. g. 14 Copy No.

M. Dv. Nr. 168

L. Dv. g. 14

Secret!

Key Instructions

for the

Enigma Key Machine

From the 13. 1. 40

B e r l i n 1940
Printed at the Imperial Printing Office

The Chief of the High Command of the Armed Forces Berlin, 13 January 1940

I approve the regulation H. Dv. g. 14 – M. Dv. 168 – L. Dv. g. 14

“Keying Instructions for the Enigma Cipher Machine dated 13 Jan. 1940”

I. A.

Fellgiebel

Table of contents.

			Seite
I.		Explanation of Terms and Designations……..	5
II.	1.-4.	General.....……...	5
III.	5.-7.	Key Documents.....……	6
IV.	8.	Identification of the key.....…….	7
V.	9.-12.	Encryption….....…	8
VI.	13.-15.	Decode .....….....…..	9
VII.	16.	Spare and emergency keys.....…..….....…	10
VIII.	17.-26.	Example.....….....…….	10
IX.	27.-30.	Guideline for the Creation of Training Machine Keys …….	13

I. Explanation of Terms and Designations.

Plaintext, or open text, is text written in ordinary, unconcealed language.

Ciphertext, or encoded text, is plaintext that has been transformed according to a specific key.

Encryption is the process of converting plaintext into ciphertext.

Decryption is the process of converting ciphertext back into plaintext.

Coding can refer to either encryption or decryption.

A **cryptographic system** is the set of rules or the logic according to which encryption is performed.
A **key** refers to the variable materials used to prepare the specific cryptographic tools required for a given method.

A **key table** is a collection of individual keys intended for use over an extended period.
A **cryptographic tool** is any device or resource required for encryption—for example, a cipher machine.

A Key identifier is a code group used to identify which specific key was applied to a given message.

II. General.

1. The scope of use for the Enigma cipher machine shall be ordered separately by the Armed Forces High Command (Oberkommando der Wehrmacht) for each branch of the Armed Forces.

2. General cipher procedures are set forth in the regulation "General Cipher Rules for the Armed Forces" (H. Dv. g. 7, M. Dv. 534, L. Dv. g. 7), while instructions for operating the Enigma cipher machine are contained in the "Operating Manual for the Enigma Cipher Machine" (H. Dv. g. 13 – L. Dv. g. 13).

3. There is no minimum length for a message encrypted using the Enigma cipher machine. The maximum length of a message prepared for transmission must not exceed 250 letters.

4. The message header contains:

a) Time, in four-digit format, e.g., 1755;

b) The number of letters, including the 5 letters of the indicator group;

c) The selected initial setting and the encrypted message key, e.g., wep hfi

III. Key Documents.

5. The key changes daily (daily key) at 00:00 hours. The keys and their identifiers (cf. IV) are issued—typically for a period of one month—in the form of a “key table” that compiles the individual daily keys and their corresponding identifiers.

6. To configure the Enigma cipher machine, the key provides the following information, which changes daily:

a. The rotors order (in Roman numerals),

b. Ring settings (in Arabic numerals or letters),

c. Plug connections (in letters).

In cases where key settings are expressed using either letters or numerals, the numerals may replace the letters—or vice versa—based on their respective positions in the alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	16	17	18	19	20	21	22	23	24	25	26	27

(Note that, in addition to I, the letter J is present as a distinct letter on the cipher machine, meaning the alphabet consists of 26 letters!)

7.Examples of:

6a) The rotor order refers to the sequence in which the individual cipher rotors are to be inserted into the Enigma cipher machine, from left to right (cf. H. Dv. g. 13, sections 10a and 12).

z.B. II I III

6b) The ring setting indicates the adjustment of the letter or number rings on each individual rotor (cf. H. Dv. g. 13, sections 10b and 13),

z.B.	II	I	III
	13	08	11

6c) Specifying the plug connections identifies the pairs of sockets that are to be connected to one another using the double-ended patch cords (cf. H. Dv. g. 13, sections 10d and 15).

Each letter designates a specific pair of sockets, and two letters placed together indicate the pairs of sockets that are to be connected to one another—that is,

AO BI DV EH GZ KW LX MU RY QT.

IV. Identification of the key.

8. The key used for a message is identified by a five-letter code. The first two letters The (filler letters) for this group may be chosen at will and should be changed for each message to disguise the indicator group. The final three letters (indicator group letters) are taken from the “indicator group table” that is either printed on or enclosed with each key. For each key range and day, several three-letter indicator groups are available. These individual letter groups are to be used in rotation; furthermore, the sequence of the individual letters within these groups must be altered for every message.

For multi-part messages, each part must be identified individually using a unique set of indicator letters and filler letters. The indicator group (consisting of 2 filler letters and 3 indicator letters) is placed at the very beginning of the message, preceding the encrypted message key. The 5 letters of the indicator group must be included in the total character count specified in the message header. These indicator groups are not encrypted; instead, they are written onto the message form as the first group before the message itself is encrypted. Once the appropriate key range has been determined, these groups must be struck through prior to decryption.

V. Encryption.

9. The Enigma cipher machine is set according to the specifications of the daily key. This setting is identical for all stations operating with the same key (e.g., a Wehrmacht machine key).

The cipher clerk selects three indicator letters from the key table, adds two freely chosen filler letters at the beginning to form a five-letter group, and writes this down as the first group of the message to be transmitted on the message form. Subsequently, the cipher clerk selects a specific initial setting for each message and adjusts the cipher machine accordingly. The initial setting specifies the numbers or letters that must be set in the three windows of the cipher machine, from left to right (cf. H. Dv. g. 13, sections 10c and 14).

Z.B. W E P – 23 05 16.

The initial setting must be different for every message—or, in the case of multi-part messages, for each individual part. For multi-part messages, the setting that appears in the three windows of the cipher machine at the end of the preceding part must under no circumstances be chosen as the initial setting or the message key for the following part. When selecting the initial setting, the instructions provided for the selection of message keys must be followed (cf. section 10). The initial setting and the message key must not be identical.

10. Each message must then be encrypted using a specific message key, which the operator selects themselves using letters or numbers for the three rings—ranging from A A A to Z Z Z (or 01 01 01 to 26 26 26). When choosing individual message keys, it is prohibited to use identical letters (e.g., A A A), actual words (e.g., "ist"), abbreviations (e.g., "Rgt."), call signs from one's own communication sector, standard operating signals (e.g., Q R M), sequences of letters as they appear on the cipher machine's keyboard (e.g., E R T), or sequences in alphabetical order (forwards or backwards, such as A B C or C B A). A new message key must be used for every message and for every part of a multi-part message.

11. The message key chosen by the operator—for example, X F R (24 06 18)—is entered once into the Enigma cipher machine (which has already been configured according to the daily key and the selected initial setting); the three letters that

light up as a result (the encrypted message key) are appended to the three letters inserted into the message header.

12. The operator now sets the letters chosen as the message key—for example, X F R (24 06 18)—in the windows and keys in the plaintext. The letters that light up in the process are written onto the message form—following the five letters of the indicator group—as the 6th, 7th, 8th, etc., letters; all the letters are then grouped into five-letter blocks.

VI.Decode.

13. Based on the indicator tables printed alongside the individual code tables, the specific code used must be determined from the intercepted ciphertext, and the indicator group must then be struck through (cf. Para. 8).

The cipher machine must be set according to the daily key currently in effect; the initial rotor setting is to be taken from the header of the intercepted, encrypted message.

14. To decrypt, the operator must first determine the specific message key used (cf. paras. 10 and 11). To do this, the three letters appended to the three-letter initial setting in the message header—which represent the encrypted message key—are entered into the machine; this yields the three-character message key.

15. The operator then adjusts the rotors in the machine's windows to match the message key obtained in this manner and proceeds to enter the ciphertext, starting from the 12th character (or the 6th character, depending on the specific procedure). The letters that light up during this process are recorded, revealing the plaintext.

VII.Spare and emergency keys.

16. For every machine key, a replacement machine key or a manual key is issued —the latter in accordance with the Wehrmacht manual-key procedure (H. Dv. g. 15a and 15b). In the event that a machine key is compromised or lost, the replacement key shall take the place of the original machine key at all offices that utilize the same key table.

VIII.Example.

17.Valid daily key:

(Excerpt from the key table to be used for encrypting the plaintext, e.g., “Wehrmacht machine key for the month of May”)

Datum	Walzenlage	Ringstellung
4	I III II	16 11 13

Steckerverbindung	Kenngruppen
BN KE VZ CO DI FR HU JW LS TX	adq nuz opw vxz

The cipher machine must be set according to this daily key (cf. sections 6 and 7).

For reasons of secrecy, the key text used in the example below was not entered into the cipher machine; instead, it was chosen arbitrarily.

A. Encrypt

18.Message to be encrypted:

May 4,
Time of dispatch 17:55
General Command VI

Attacks the enemy near Maisach on May 5 at 03:45 with the 3rd and 10th Division s. Command Post: Milbertshofen, northern exit

19. For the purpose of encryption, the plaintext of the message is to be written down in accordance with H. Dv. G. 7 – M. Dv. 534 – L. Dv. G. 7 as follows:

```
gen kdo roem s e q s angreift fuenften mai null
drei vier fuenf uhr mit dritter und zehnter div
feind bei  maisach x gef stand milbertshofen
nordausgang
```

20. The cipher clerk sets the Enigma cipher machine according to the daily key for May 4th. He then enters the indicator group (see section 9) as the first group on the message form; for each message—or for each part, if a message consists of multiple parts—he selects a specific initial setting (ground setting), for example, "wep" (23 05 16), and sets this configuration in the windows of the Enigma machine (see section 9).

21. The cipher clerk selects a message key, for example, "X F R" (24 06 18), and presses the keys for these three letters once. This produces the letters "H F I," which are to be written down in the message header following the three letters of the initial setting ("W E P").

22. Next, while keeping the rest of the Enigma machine’s settings unchanged, the cipher clerk sets the letters chosen as the message key—"X F R" (24 06 18)—in the windows and proceeds to type in the plaintext. The resulting letters are recorded following the five letters of the indicator group and the six letters of the encrypted message key (occupying the 12th, 13th, 14th, etc., positions). Throughout this process, the output is organized into groups of five letters each.

The following key text emerges:

ulznu	sgexu	nfopr	salme
ydrjg	qarzu	bhfem	ooxzl
gredl	fijya	eivdg	nhyex
mjyra	qztls	siwfu	wfhel
narzq	eduwj	vsfab	skqud
ihxgf	nejpa	fohwe	gaimf
ojrle	khhd		

23. With the header (cf. item 4) placed at the beginning, the message—ready for transmission—reads as follows:

1755 129 wep hfi

ulznu	sgexu	nfopr	salme
ydrjg	qarzu	bhfem	ooxzl
gredl	fijya	eivdg	nhyex
mjyra	qztls	siwfu	wfhel
narzq	eduwj	vsfab	skqud
ihxgf	nejpa	fohwe	gaimf
ojrle	khhd		

1755 = Time group
129 = Number of letters, including the 5 letters of the identifier group
wep = Basic position chosen by the cipher clerk
hfi = Encrypted message key
ulnzu = Kenngruppe

To identify the key used for enciphering the message, one of the four indicator groups—for example, "nuz"—is selected from the daily key (cf. section 17). This group is then rearranged (e.g., into "znu") and, with two filler letters (e.g., "ul") prefixed to it, is entered as the first group.

sgexu nfopr . . . . . = enciphered plaintext.

B.Decode.

24. The message to be decrypted is as stated above (item 23).

25. The first group of the ciphertext is the indicator group. After removing the two dummy letters and arranging the remaining two letters in alphabetical order, the following indicator group letters are obtained: nuz. Using these indicator group letters, the appropriate key is determined, and the Enigma cipher machine is set according to the corresponding daily key.

The initial setting used is taken from the message header—for example, "wep" (23 05 16)—and entered into the windows of the Enigma cipher machine. Next, the three secret letters of the message key (hfi)—which follow the three letters of the initial setting (wep) in the message header—are keyed into the machine. The letters that light up—xfr—represent the message key.

26. The operator then sets the letters of the message key—X F R (24 06 18)—into the windows of the cipher machine and keys in the ciphertext. This yields the following letters:

```
gen kdo roem s e q s angreift fuenften mai null drei
vier fuenf uhr mit dritter und zehnter div feind bei
maisach x gef stand milbertshofen nordausgang.
```

The final, plain-text version of the statement reads:

Gen. Kdo. VI angreift 5. mai 0345 Uhr mit 3. und 10. Div. Feind bei Maisach. Gef. Stand Milbertshofen Nordausgang.

IX.Guideline for the Creation of Training Machine Keys.

When setting up practice keys, the following points must be observed:

27. The rotor position must be changed daily. Rotors I through V are to be used.

28. To determine the ring setting, it is practical to prepare 26 small cardboard slips (similar to those used in a lottery game) and mark them with the numbers 1 through 26. In this way—much like a lottery draw—one can determine 8 sequences (representing 8 days) for the "ring setting" column (naturally, 2 numbers will be left out each time); for example:

Tag	Ringstellung	Tag	Ringstellung
31.	24 13 08	27.	16 05 11
30.	17 01 13	26.	23 03 07
29.	25 15 19	25.	02 22 21
28.	26 12 10	24.	18 09 06

This accounts for all numbers except 04 and 20. The ring setting for the remaining days of the month is determined in the same manner.

29. To establish the 10 plug connections, 26 small cardboard slips are prepared, each labeled with a letter of the alphabet; 20 of these are selected at random and paired up to form plug connections. They are recorded in such a way that, within each pair, the letters appear in alphabetical order—for example:

KV IT BY FG CO EJ DP MR QS LX

30. To identify the type of key, four groups of three letters each must be appended to the daily key. While the identifier groups for keys used in classified communications (cf. H. Dv. g. 7, M. Dv. 534, L. Dv. g. 7, section 27) are determined by the commanders-in-chief of the respective branches of the Armed Forces, those for training keys may be chosen freely by selecting four sets of three letters at random. E.g.

BLV KUX RTZ S W Y.

The commanders-in-chief of the branches of the Wehrmacht are authorized to assign indicator groups for training and special ciphers as well.

April 1940 No.

Secret

Corrected: Doppelfeld, Senior Lance Corporal (Ogefr.)
July 20, 1942

Cover sheets nos. 1–8

Zu H. Dv. g 14 – M. Dv. Nr. 168 – L. Dv. g 14

“Keying Instructions for the Enigma Cipher Machine
dated 13 Jan. 1940”