H. Dv. g. 14
M. Dv. No. 168
L. Dv. 14

Test = No.

Secret!

keying instructions
for the
Enigma Cipher machine

Berlin 1937
Printed at the Reich Printing Office

This guide is secret. Abuse will be punished according to the law of 3 June 1914 against the betrayal of military secrets, unless other criminal penalties come into question.

Berlin, 1937.

The chief of the army command.

Table of Contents.

			Page
I.		Explanation of Terms and Designations.	3
II.	1.-2.	General ……...	3
III.	3.-5.	Cipher materials ……..	3
IV.	6-9.	Encryption ……...	5
V.	10.-12.	Identification of the Cipher Key ……..	6
VI.	13.-15.	Deciphering …….	7
VII.	16.	Emergency key..……	7
VIII.	17.-26.	Example ……	8

I. Explanation of Terms and Designations.

Plaintext (Klartext) is text written in an unconcealed language.
Ciphertext (Echimtext) or key-text is plaintext that has been transformed according to a specific key.
Encrypting (Berichlüsslen) means transforming plaintext into ciphertext.
Decrypting (Entschlüsseln) means transforming ciphertext into plaintext.
Keying (Schlüsseln) can refer to either encrypting or decrypting.
Key (Schlüssel) is the variable configuration used for a cryptographic method (e.g., the settings for a cipher machine).
Cryptographic tool (Schlüsselmittel) is the device or resource required to apply the key—for example, a cipher machine.

II. General

1. The use of the Enigma cipher machine is mandated by a separate order from the Reich Ministry of War.

2. General cipher regulations can be found in the manual "Army Ciphers (H. Dv. g. 7)," Section IX; instructions for operating the Enigma cipher machine are contained in the "Operating Manual for the Enigma Cipher Machine (H. Dv. g. 13)."

III. Cipher Materials.

3. The cipher changes daily (daily key). The keys and their identifiers (cf. IV.)—comprising the individual daily keys and identifiers—are generally issued for a one-month period in the form of a "key sheet," (Schlüseltafel) which includes a printed table of indicator groups and an indicator group selector.

4. For the purpose of setting the cipher machine, the key contains the following information, which changes daily:

a) Rotor arrangement (Walzenlage) (in Roman numerals),
b) Ring setting (Ringstellung),
c) Initial position (Grundstellung),
d) Plug connections (Steckerverbindungen).

With the exception of (a), the key settings are expressed using either letters or numbers, where the numbers correspond to the position of the letters 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	15	16	17	18	19	20	21	22	23	24	25	26

(Note that, in addition to I, the letter J is present as a distinct letter in the cipher machine, meaning the alphabet consists of 26 letters!) In the following examples, the key settings are provided as letters, with the corresponding numbers included in parentheses below them message, which has been encrypted using the message key.

5. Example of:

4a) The Walzenlage specifies the sequence in which the individual cipher rotors are to be inserted into the cipher machine, from left to right (cf. H. Dv. g. 13, sections 10a and 12)

e.g. II I III;

4b) The Ringstellung indicates the adjustment of the letter or number rings on each individual rotor (cf. H. Dv. g. 13, sections 10b and 13)

e.g.	II	I	III
	M	H	K
	(13)	(08)	(11)

4c) The Grundstellung prescribes the numbers or letters that are to be set in the 3 windows of the cipher machine, from left to right (cf. H. Dv. g. 13, sections 10c and 14)

e.g.	W	E	P
	(23)	(05)	(16)

4d) The plug connections indicate which pairs of sockets are to be connected to one another using the double-ended patch cords (cf. H. Dv. g. 13, sections 10d and 15). Each letter or number designates a specific pair of sockets; two letters placed together, or two numbers joined by a forward slash, indicate the pairs of sockets that are to be connected to each other—for example:

AO	EH	KW	RY	QT	MU
(1/15)	(5/8)	(11/23)	(18/25)	(17/20)	(13/21).

IV. Encryption.

6. The cipher machine is set up according to the key specifications. This configuration is identical for all stations operating with the same key (e.g., the Wehrmacht machine key).

7. Each message must be encrypted using a specific "message key," (Spruchschlüssel) which the cipher clerk selects from the available letters or numbers for the three rings (AAA through ZZZ, corresponding to 01 01 01 through 26 26 26). When selecting these message keys, it is strictly forbidden to use identical letters (e.g., AAA), whole words (e.g., "ist"), abbreviations (e.g., "Rgt"), call signs belonging to one's own communication network, standard operating signals (e.g., QRM), sequences of letters as they appear on the cipher machine's keyboard (e.g., ERT), or sequences in alphabetical order (forwards or backwards, such as ABC or CBA).

A new message key must be used for every individual message—and for each part of a multi-part message—on any given day.

8. Once the cipher machine has been set according to the prescribed daily key (see section 6), the message key chosen by the cipher clerk (e.g., XFR, corresponding to 24 06 18) is entered into the machine twice in succession. The resulting six letters are then placed at the beginning of the message that is to be encrypted using that key.

9. The cipher clerk then sets the chosen message key—for example, XFR (24 06 18)—in the machine's display windows and proceeds to type in the plaintext. The letters that light up on the machine are recorded following the letters obtained from the initial entry of the message key; these are then grouped (see Section 10, the "deployment location") is to be omitted in this context.

V. Identification of the Cipher Key.

10. The cipher key used for a given message is identified by a five-letter indicator group. The first two letters of this group (filler letters) may be chosen arbitrarily and must be changed for every message to disguise the indicator group. The last three letters (key-identifier letters) are taken from the "indicator table" printed on or provided with each cipher key. For each key range and each day, several three-letter indicator groups are available. These individual letter groups are to be used in rotation; furthermore, the sequence of the letters within these groups must be varied for each message.

In the case of multi-part messages, each part must be identified separately, using different key-identifier letters and different filler letters.

The indicator group (consisting of 2 filler letters and 3 key-identifier letters) is inserted into the encrypted message—which is otherwise organized into five-letter groups—at a pre-designated, reserved position (cf. Section 9). The five letters of the indicator group are to be included in the total letter count specified in the message header. The "insertion point" for the indicator group, which changes daily, is determined using the "indicator guide" provided alongside the daily cipher key.

The indicator groups are not encrypted themselves; instead, they are inserted into the already encrypted message and are removed prior to decryption—once the relevant key range has been identified (cf. section 13).

If the first group is specified as the insertion point for the indicator group, the indicator group is placed at the very beginning of the message, preceding the encrypted message key.

The indicator group must be appended to the encrypted message as the final group if the specified insertion point cannot be used due to the message having an insufficient number of letters. In such a case, if the final text group of the encrypted message contains fewer than 5 letters, it must be padded with filler letters—which must not alter the meaning of the message and must all be distinct from one another—to form a complete group before the indicator group is added.

11. There is no minimum length for a message encrypted using the cipher machine. The maximum length of a message prepared for transmission must not exceed 180 letters.

12. The message header does not contain any indication of the encryption method used; it consists only of:

a) A four-digit date, e.g., 0405 (May 4th),
b) A four-digit time, e.g., 1755,
c) The total number of letters, including the 6 letters of the message key and the 5 letters of the indicator group.

VI. Deciphering.

13. Based on the intercepted ciphertext, the key used must be determined by referring to the indicator tables and indicator guides provided with the individual key sheets; the indicator group should then be crossed off (cf. Item 10).

14. To decipher, the operator must first determine the message key that was used. After setting the cipher machine according to the daily key in effect (see the date in the message header), the first 6 letters are entered; these yield the three-character message key, repeated twice.

15. The operator then adjusts the rotors in the machine’s windows to match the message key obtained in this manner and enters the ciphertext, starting from the 7th letter. The letters that light up during this process are recorded, revealing the plaintext.

VII. Emergency Key.

16. A replacement key is issued for every machine key; this replacement is to be used in accordance with the Wehrmacht "manual cipher procedure" (Handschlüsselverfahren) (H. Dv. g. 15a and 15b). In the event that a machine key is compromised or lost, the replacement key shall take its place at all stations that utilize the same key table (cf. H. Dv. g. 7, section 10).

In the event of malfunctions in the cipher machine, it serves as a substitute key.

VIII. Example.

17. Valid daily key:
(Excerpt from the key table used for enciphering the plaintext, e.g., "...…"
Machine key for the month of May.)

Datum	Walzenlage	Ringstellung	Grundstellung
4	I III II	16 11 13	01 12 22
Steckerverbindung		Kengruppen- Einfassftelle …….. Gruppe	Kenngruppen
CO DI FR HU JW LS TX		2	ndq nuz opw vxz

A. Encryption.

18. Message to be encrypted:
Date: May 4,
Time of dispatch: 17:55
VI Corps Command
Attacking the enemy near Maisach on May 5 at 03:45 with the 3rd and 10th Divisions. Command Post: northern exit of Milbertshofen.

19. For the purpose of encryption, the plaintext of the message must be written down in accordance with H. Dv. g. 7, Section 40, as follows:

korpskommando roem x seqs angreift fuenften mai null drei
vier fuenf uhr mit dritter und zehnter div x feind bei maisach x
gef stand x milbertshofen nordausgang

20. On the message form, the person performing the encryption indicates the insertion point for the "indicator group" (in this example, the 2nd group)—as prescribed by the daily key—and leaves this space blank when entering the message key or the encrypted text.

21. The keyholder chooses the key for the message, e.g. B. XFR (24 06 18), and press these 3 letters twice in succession, resulting in the letters hfi klb, which, taking into account the subsequently inserted key group (see section 20), are to be written down as the first letters of the message to be encrypted.

22. From now on, with the cipher machine's setting remaining constant, the cipher operator enters the letters XFR (24 06 18), chosen as the message key, into the front slots and taps the plaintext. The resulting letters are written down following the 6 letters that resulted from tapping the message key. At the same time, groups are formed to Each 5 letters are formed.

This results in the following key text:

hfikl	.....	bsgex	nnfop	(hfikl .... b
rsalm	cydrj	qqarz	ubhfe	encrypted
mooxz	lgred	lfijy	aeivd	key)
gnhye	xmjyr	aqztl	ssiwf	
uwfhe	lnarz	qeduw	jvsfa	
bskqu	dihxg	ncjpf	afohw	
egaim	fojrl	ekhhd	lpbme	
binge				

23. To identify the key used for deciphering the message, one of the four key groups, e.g., "nuz", is taken from the daily key, which is then converted to znu, for example, and, after prefixing two filler letters, e.g., "ul", is entered as the key group at the designated position.

With the message header (cf item 12) also included at the beginning, the message, ready for transmission, reads as follows:

0405 -- 1755 -- 145 --

hfikl	ulznu	bsgex	nnfop
rsalm	cydrj	qqarz	ubhfe
mooxz	lgred	lfijy	aeivd
gnhye	xmjyr	aqztl	ssiwf
uwfhe	lnarz	qeduw	jvsfa
bskqu	dihxg	ncjpf	afohw
egaim	fojrl	ekhhd	lpbme
binge			

B. Deciphering.

24. Let the message to be deciphered be the one mentioned above (Section 23).

25. According to the key tables for the month of May, the 2nd group is the designated starting point for the 4th day of the month. Consequently, after removing the two filler letters and arranging the remaining 3 letters alphabetically, the resulting indicator group is "nuz."

Using this indicator group, the appropriate key is determined, and the cipher machine is set according to the daily key.

After removing the indicator group, the first 6 letters—"hfiklb"—are to be keyed in and subsequently deleted from the message. The deciphered message key is: "xfr xfr."

26. The operator then sets the letters of the message key "XFR" (24 06 18) in the windows of the cipher machine and keys in the ciphertext. This yields the following letters:

korpskommando roem x seqs angreift fuenften mai null drei
vier fuenf uhr mit dritter und zehnter div x feind bei maisach x
gef stand x milbertshofen nordausgang

The final plaintext of the message is:

Korpskommand VI.
angreift 5. Mai 0345 Uhr mit 3. und 10. Div. Feind bei Maifach.
Gef. Stanb. Milbertshofen Nordausgang.

Berlin, June 8, 1937

The Reich Minister of War
and Commander-in-Chief of the Armed Forces.

By order,
Fellgiebel.