Secret! **No.**

Key instructions
for the
Cipher machine "Enigma I"

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, May 1930.

The chief of the army command.

Contents.

			Page
1.-2.	I.	Key distribution	3
3.	II.	Key	3
4.-9.	III.	Key setting	3
10.-15.	IV.	Example: Encrypt	4
16.19.		Decrypt	6
20.	V.	Emergency Key	6
21.	VI.	Example of a key list	8

I. Key distribution.

1. Within a certain range (for example, Reichsheer, group, division, maneuvers, etc.), an army M. key applies. In general, the Reichsheer is considered an area and receives only 1 key. In exercises from divisional units, the command authorities have the right to set up and issue Army M. keys for the practice area.
2. If there is message traffic between areas in which different Army M.Key keys exchange the area for the cross traffic or set up and provide special Army M.Key for the cross traffic by the superior command authority.

II. Key.

3. An army M. key contains all necessary information to set the encryption machine for one month, namely:

a) indication of the rotor order (Walzenlage), changing every three months,
b) indication of the ring position (Ringstellung), daily changing,
c) indication of the basic position (Grundstellung), daily changing,
d) indication of plug connections (Steckerverbindungern), daily changing.

III. Key setting. (Key pattern for page 8).

4. The specification of the rotor order indicates the order in which the individual rotors are to be inserted from left to right, for example:
II I III.
5. The indication of the ring position indicates the setting of the rings for each individual roller, e.g.
II: 24 I: 13 III: 22.

6. The specification of the basic position prescribes the numbers to be set in the three windows from left to right, for example:

   06 15 12.

7. The specification of the plug connections determines which pairs of sockets are to be connected to each other by means of double plug cords, for example:

   1/13 6/9 14/22 16/19 20/21 23/26,

Each one identifying a particular pair of sockets and the slash separating the numbers of pairs of sockets to be connected; It is therefore to connect socket pair 1 with 13, 6 with 9, 14 with 22 and so on.

8. Each message key is encrypted according to a special position (Grundstellung). This message key is chosen arbitrarily from the number range 01 01 01 to 26 26 26. For every message key on the same day, use a single message key as the starting position. It is forbidden to encrypt two or more messages in one day using the same message key.

9. The recipient of the award will be notified of the chosen message key (f. III, 9). The numbers of the message key are indicated by the letters corresponding to them on the plug board, e.g. l replaced by a, 13 by m, etc. Replaced and keyed twice in succession using the initial setting (III, 7). The 6 letters that result from this are placed before the message, which has been encrypted using the message key.

IV example.

Encrypt.

10. A spell to encode at 10 35 reads:
    "Feindlich Infanteriekolonne beobachtet, Aufang Südausgang Eichwlalde, Rnde 3 km oftwärts Keuftadt."
    ("Enemy infantry column observed. Beginning at the southern exit of Eichwalde, ending three km east of Neustadt..")

Since according to section 18 of the "Gebrauchsanweifung Enigma I" for the spelling of numbers, sat. Ufw. The rules of the "Double Transposition Cipher" apply, the sentence is encoded as follows:

"feindliqe infanteriekolonne beobaqtet x anfang sued-
ausgang eichwalde x ende drei km ostwaerts neustadt"

11. Valid day key:

Rotor order	II	I	III
Ring position	II 24	I 13	III 22
Basic position	06	15	12
Plug connection	1/13 6/9 14/22 16/19 20/21 23/26		

12. The sender chooses the message key 19 02 11. The numbers correspond to the letters a b l on the plugboard. They are keyed twice in succession according to Fig II, with the basic position 06 15 12, whereby the letters h k t f x d result. These are written down in the following form, as the message to be transmitted in five-digit groups immediately follows, in the following form: h k t f x d

13. Then the plaintext to be encrypted after setting the message key 19 02 11 is keyed. The letters that light up are written behind the previously obtained 6 letters. The 4 first letters are combined with the last of the 6 letters (d) mentioned in 12 to form the second five-digit letter group and the rest are also divided into groups of 5 letters:

```
hktfx dviaa yrxaf soafq vxfcq
wyzte mbtzp hljdp jamjs rmiiw
vrxla ltlvo eodic mpgyb gajms
aarwg dkubj nnttj njqpl j
```

14. Precede the encrypted content:
    a) Date group (four digits)
    b) Time group (four digits),
    c) Number of letters (two or three digits),
    d) Code, four-digit, to be selected from a number plate according to the "Instructions for Use of the Number Chart".

The encrypted message reads as follows:

```
      3005  1035  96   7341
hktfx dviaa yrxaf soafq vxfcq
wyzte mbtzp hljdp jamjs rmiiw
vrxla ltlvo eodic mpgyb gajms
aarwg dkubj nnttj njqpl j
```

If a message is longer than 180 letters, it may be subdivided.
The 2nd or 3rd part must be encrypted each time with another message key to be concealed in the manner described.

15. After completing the encryption, the last numbers appearing in the windows are to be changed by any rotation of the rotors.

Decrypt.

16. The encrypted message is:

```
      3005  1035  96   7341
hktfx dviaa yrxaf soafq vxfcq
wyzte mbtzp hljdp jamjs rmiiw
vrxla ltlvo eodic mpgyb gajms
aarwg dkubj nnttj njqpl j
```

17. The information before the message and the daily key determined by it indicate the rotor position, ring position and plug connections valid for the day; the machine is adjusted accordingly. With the basic position, the first 6 letters p k p j x i keyed. The result is: a b l a b l.

18. The letters a b l are found on the plug board, replaced by the numbers 1 2 12 corresponding to them, thus indicating the key 01 02 12 selected by the sender.

19. Now the numbers 19 02 11 are set in the windows and the coded spell is scanned after deleting the first 6 letters (h k t f x d). This results in the letters.

```
feindliqeinfanteriekolonnebeobaqtet
xanfangsuedausgangeichwaldexendedre
ikmostwertsneustadt
```

the final, clear statement is as follows:

"Feindlich Infanteriekolonne beobachtet, Aufang Südausgang Eichwlalde, Rnde 3 km oftwärts Keuftadt."

V. Replacement and Emergency key.

20. In the event that the army machine cipher key is lost or compromised, a manual cipher method shall be used in place of the machine-based method. A replacement key—the communications cipher key—must be brought into use immediately, either on one's own initiative or by order of a superior authority. Should this key also be lost or compromised, the emergency cipher key must be used.

VI. Key rules.

21. If a message contains more than 180 letters, it should be subdivided. The parts must always be different lengths. Each item shall be encrypted with another message key as described in paragraph 8 above. Before the first part is bribed except date and time, in front of each part its number, you number of letters of the relevant part and a nominal number set, for example:

    before the first part: 3005 1835 3rd part 1st part 169 5231
    before the second part: 3005 1835 2nd part 142 9276
    before the third part: 3005 1835 3rd part 113 7358

    The same message should never be encrypted by two different keys, nor should it be divided differently in repetitions. When repeating, the messages must be given in the same encrypted form as the first of May. If this is impossible for any reason, the wording of the sentence must be completely transformed before the new rounding up.