

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

Prüf-Nr. 5 734

Geheim!

Schlüsselanleitung
zur
Schlüsselmaschine Enigma

Tom 13. 1. 40

Berlin 1940

Gebrucht in der Reichsdruckerei

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

Prüf-Nr. 5 734

Geheim!

Schlüsselanleitung
zur
Schlüsselmaschine Enigma

Vom 13. 1. 40

Berlin 1940
Gedruckt in der Reichsdruckerei

**Der Chef des Oberkommandos
der Wehrmacht**

Berlin, den 13. Januar 1940

Ich genehmige die Vorschrift H. Dv. g. 14 -- M. Dv. 168
-- L. Dv. g. 14

**»Schlüsselanleitung zur Schlüsselmaschine Enigma
vom 13. 1. 40.«**

J. H.
Fellgiebel

Inhaltsverzeichnis.

		Seite
I.	Erläuterung von Begriffen und Bezeichnungen	5
II.	1.—4. Allgemeines	5
III.	5.—7. Schlüsselunterlagen	6
IV.	8. Kennzeichnung des Schlüssels	7
V.	9.—12. Verschlüsseln	8
VI.	13.—15. Entschlüsseln	9
VII.	16. Ersatz- und Notchlüssel	10
VIII.	17.—26. Beispiel	10
IX.	27.—30. Merkblatt für das Aufstellen von Übungs- Maschinenschlüsseln.	13

1. Erklärung von Begriffen und

Klartext oder offener Wortlaut ist ein in offenem Text.

Geheimtext oder Schlüsseltext ist ein nach einer Umwandlung umgewandelter Klartext.

Verchlüsseln heißt Umwandeln eines Klartextes.

Entchlüsseln heißt Umwandeln eines Schlüsseltextes.

Schlüsseln kann sowohl Ver- als auch Entchlüsseln bedeuten.

Schlüsselverfahren ist das Gesetz, nach dem geschlüsselt wird.

Schlüssel bezeichnet die wechselnden Unterlagen, die bei jedem Verfahren das Schlüsselmittel zum Schlüsseln bilden.

Schlüsselkarte ist die Zusammenstellung einzelner Schlüssel für einen längeren Zeitraum.

Schlüsselmittel ist der zum Schlüsseln erforderliche Apparat (bisher Chiffriermaschine bezeichnet).

Kenngruppe dient zur Kennzeichnung des in einem Schlüssel.

II. Allgemeines.

1. Der Umfang der Verwendung der Schlüssel ist durch das Oberkommando der Wehrmacht für die einzelnen Teilmächte befohlen.

2. Die allgemeinen Schlüsselregeln sind in den »Schlüsselregeln« für die Wehrmacht (II. Dv. g. 7) und die Anweisung für die Bedienung der Schlüsselmaschinen (I. Dv. g. 13) enthalten.

3. Die Mindestlänge eines mit der Schlüsselmaschine verschlüsselten Spruches ist unbegrenzt. Die Höchstlänge eines fertigen Spruches darf 250 Buchstaben nicht überschreiten.

4. Der Spruchkopf enthält

- a) Uhrzeit, vierstellig, z. B. 1755,
- b) Buchstabenanzahl einschl. der 5 Buchstaben der Schlüsselmaschine,
- c) die gewählte Grundstellung und den verschlüsselten Spruchkopf, z. B. wep hfi.

Sachblatt Nr. 1

III. Schlüsselunterlagen.

5. Der Schlüssel wechselt täglich (Tageschlüssel). Die Schlüsselmaschine und ihre Kennzeichnungen (vgl. IV) werden in der Beschreibung der einzelnen Tageschlüssel und Kennzeichnungen als »Schlüsselkarte« in der Regel für einen Monat ausgeben.

6. Zur Einstellung der Schlüsselmaschine Enigma folgende Angaben, die täglich wechseln:

- a) Walzenlage (in römischen Zahlen),
- b) Ringstellung (in arabischen Zahlen oder in Buchstaben),
- c) Steckerverbindungen (in Buchstaben).

Soweit die Schlüsselangaben durch Buchstaben oder Buchstabenpaare gedrückt werden, treten die Zahlen an Stelle der Buchstaben und sind umgekehrt gemäß ihrer Reihenfolge im Alphabet.

A	B	C	D	E	F	G	H	I
01	02	03	04	05	06	07	08	09
N	O	P	Q	R	S	T	U	V
14	15	16	17	18	19	20	21	22

(Beachte, daß neben I der Buchstabe J als besondere Kennzeichnung der Schlüsselmaschine vorhanden ist, so daß das Alphabet aus 26 Buchstaben besteht!)

You can buy a complete copy on www.superborg.de!!!

7. Beispiele zu:

6a) Die Walzenlage bezeichnet die Reihenfolge, Schlüsselwalzen von links nach rechts in dem Enigma einzusehen sind (vgl. H. Dv. g. 13, S. 10)

z. B. II I

6b) Die Ringstellung zeigt die Einstellung der Buchstabenringe jeder einzelnen Walze an (vgl. H. Dv. g. 13, S. 10 und 13),

z. B. II I
13 08

6c) Durch die Angabe der Steckerverbindungenpaare gekennzeichnet, welche durch die Doppelsteckerpaare zu verbinden sind (vgl. H. Dv. g. 13, S. 10)

Jeder Buchstabe bezeichnet ein bestimmtes Buchstabenpaar, die zusammenstehende Buchstaben diejenigen Buchstabenpaare bezeichnen, die verbunden werden sollen, also

AO BI DV EH GZ KW LX M

IV. Kennzeichnung des Schlüssels

8. Der in einem Spruch angewendete Schlüssel wird durch eine fünfstellige Buchstabenkenngruppe gekennzeichnet. Die Buchstaben (Füllbuchstaben) dieser Gruppe sind bei der Tarnung der Kenngruppe für jeden Spruch zu ändern. Die Buchstaben (Kenngruppenbuchstaben) werden der jeweiligen Kenngruppe druckten oder beigegeführten »Kenngruppentafel« entnommen. In diesem Bereich und Tag stehen mehrere Kenngruppen zu je einer Kenngruppe zur Verfügung. Diese einzelnen Buchstabenkenngruppen sind bei der Tarnung zu ändern; dabei ist die Reihenfolge der einzelnen Buchstabenkenngruppen bei jedem Spruch zu ändern.

You can buy a complete copy on www.superborg.de!!

Bei mehrteiligen Sprüchen ist jeder Teil für verschiedene Kenngruppenbuchstaben und verschlüsselt zu kennzeichnen.

Die Kenngruppe (2 Füllbuchstaben und 3 Kennbuchstaben) wird als erste Gruppe an den Anfang des Spruchs gesetzt. Der Spruchschlüssel besteht aus 5 Buchstaben der Kenngruppe. Die 5 Buchstaben der Kenngruppe im Spruchkopf enthaltene Buchstabenanzahl mit einzuzählen werden nicht mit verschlüsselt, sondern vor der ersten Gruppe auf das Spruchformular geschrieben. Die Schlüssel nach Feststellung des Schlüsselbereiches

V. Verschlüsseln.

9. Die Schlüsselmaschine Enigma wird an den Angaben des Tageschlüssels eingestellt. Diese Angaben sind demselben Schlüssel (z. B. Wehrmacht-Maschine) zu entnehmen. Stellen die gleiche.

Der Schlüssel entnimmt der Schlüsselkarte die Buchstaben und füllt sie durch Voranstellen zweier, frei gewählter Buchstaben Gruppe von 5 Buchstaben auf und schreibt sie übermittelnden Spruches auf das Spruchformular. Der Schlüssel für jeden Spruch eine besondere Schlüsselkarte entsprechend ein. Die Kennbuchstaben oder Zahlen vor, die in den 3 Fenstern der Schlüsselmaschine einzustellen sind (vgl. S. 13 und 14).

Z. B. W E P — 23

Die Grundstellung muß bei jedem Spruch, bei jedem Teil, verschieden sein. Bei mehrteiligen Sprüchen sind die am Ende des vorhergehenden Teiles in den 3 Fenstern der Schlüsselmaschine die Grundstellung für den folgenden Teil gewählt. Die Grundstellung sind die für die Auswahl der Buchstaben zu beachten (vgl. S. 10). Grundstellungen dürfen nicht gleich sein.

10. Jeder Spruch ist sodann nach einem besondern Schlüssel verschlüsselt, den sich der Schlüssel selbst aus dem Spruchkopf für die 3 Ringe A A A bis Z Z Z (01 01 01 bis 26 26 26) durch die Wahl der einzelnen Spruchschlüssel Buchstaben (A A A), Wörter (ist), Abkürzungen (ist), eigenen Verkehrsbereiches, Verkehrszeichen (ist), Tastaturreihenfolge der Schlüsselmaschine (E R I) und die Reihenfolge (vorwärts oder rückwärts: A B C).

Für jeden Spruch und für jeden Teil eines Spruchs ist stets ein neuer Spruchschlüssel zu benutzen.

11. Der vom Schlüssel gewählte Spruchschlüssel wird auf der nach dem Tageschlüssel und dem Schlüssel eingestellten Schlüsselmaschine Enigma einmal durch die leuchtenden 3 Geheimbuchstaben werden den im Spruchkopf stehenden 3 Buchstaben der Grundstellung angefügt.

12. Der Schlüssel stellt nunmehr in den Zeichen des Spruchkopfs die gewählten Buchstaben, z. B. X F R (24 06 18) fest. Die hierbei aufleuchtenden Buchstaben werden in einem Formular hinter die 5 Buchstaben der Kenngruppe der Buchstaben geschrieben und alle Buchstaben zu Gruppen zusammengefaßt.

VI. Entschlüsseln.

13. Aus dem aufgenommenen Schlüsseltext ist durch die einzelnen Schlüsselkarten bei gedruckten Kenngruppen der Schlüssel festzustellen und die Kenngruppe zu streichen.

Die Schlüsselmaschine ist nach dem gültigen Schlüssel in die Grundstellung ist aus dem Spruchkopf des einzelnen Spruches zu entnehmen.

14. Zum Entschlüsseln muß der Schlüssel den Spruchschlüssel (vgl. Ziff. 10 und 11) feststellen. Der Spruchkopf hinter den 3 Buchstaben der Grundstellung des verschlüsselten Spruchschlüssels getastet werden, um den richtigen Spruchschlüssel zu finden.

15. Nunmehr stellt der Schließler die Spruchschlüssel in den Fenstern der Maschinenschlüssel ab den Schlüsseltext. Die hierbei aufgeschrieben und ergeben den Klartext

VII. Ersatz- und M

16. Zu jedem Maschinenschlüssel wird ein Ersatzschlüssel oder Handschlüssel ausgegeben, letzterer nach dem Verfahren (H. Dv. g 15a und 15b). Bei dem Ersatz eines Maschinenschlüssels tritt der Ersatzschlüssel an die Stelle des Maschinenschlüssels der gleichen Schließtafel arbeiten, an die

VIII. Beisp

17. Gültiger Tageschlüssel:

(Ausschnitt aus der für die Verschlüsselung in Betracht kommenden Schließtafel eines Maschinenschlüssels für S

Datum	Walzenlage
4.	I III II

Steckerverbindung

BN KE VZ CO DI FR IIU JW LS

Nach diesem Tageschlüssel ist die Schließtafel (S. 6 und 7).

You can buy a complete copy on www.superborg.de!!!

Der im nachfolgenden Beispiel eingesezte S
haltungsgründen nicht mit der Schlüsselmasch
fürlich gewählt worden.

A. Verschlüsseln.

18. Zu verschlüsselnder Spruch:

Tag 4. 5.,

Abgangszeit 17,55 Uhr

Gen. Kdo. VI

angreift 5. Mai 03.15 Uhr mit 3. und 10

Gef. Stand: Milbertshofen Nordausgang

19. Für die Verschlüsselung ist der Klartext
g. 7 — M. Dv. 534 — L. Dv. g. 7 wie folgt n

gen kdo roem seq s angreift fuer

fueuf uhr mit dritter und zehnter div

stand milbertshofen nordausgang

20. Der Schlüssel stellt die Schlüsselmaschine
schlüssel vom 4. 5. ein. Sodann trägt er auf
1. Gruppe die Kenngruppe ein (vgl. Ziff. 9), wo
bei mehreren Teilen eines Spruches für jeden P
stellung, z. B. wep (23 05 16), und stellt di
Fenstern der Schlüsselmaschine Enigma ein (vgl

21. Der Schlüssel wählt einen Spruchschlü
und tastet diese 3 Buchstaben einmal, wobei
ergeben, die im Anschluß an die 3 Buchstaben
in den Spruchkopf niederzuschreiben sind.

22. Nunmehr stellt der Schlüssel bei sonst g
der Schlüsselmaschine in den Fenstern die als
Buchstaben X F R (24 06 18) ein und tastet d
gebenden Buchstaben werden im Anschluß an d
gruppe ~~und die 6 Buchstaben des verschlüsselten~~
~~13, 14, usw. Buchstaben niedergeschrieben.~~
Gruppen zu je 5 Buchstaben gebildet.

Es ergibt sich folgender Schlüsseltext

ulznu	sgexu	nfopr
ydrjq	qarzu	bhfen
gredl	fijya	eivdg
mjyra	qztls	siwfu
narzq	eduwj	vfsab
ihxgl	nejpa	fohwe
ojrle	klhd	

Erdbeben Nr. 5

23. Unter gleichzeitiger Voransetzung
lautet der zur Übermittlung fertige Spruch

1755 ... 129 ... wep

ulznu	sgexu	nfopr
ydrjq	qarzu	bhfen
gredl	fijya	eivdg
mjyra	qztls	siwfu
narzq	eduwj	vfsab
ihxgl	nejpa	fohwe
ojrle	klhd	

1755 = Zeitgruppe

129 = Buchstabenanzahl einschl. der 5

wep = vom Schlüssel gewählte Grund

hfi = verschlüsselter Spruchschlüssel

ulznu = Kenngruppe

Zur Bezeichnung des für die Schlüssel-
Schlüssels ist aus dem Tageschlüssel (w
gruppen, z. B. »nuz«, gewählt, die z. B.
Voransetzen zweier Füllbuchstaben, z. B. »u

sgexu nfopr = verschl

B. Entschlüsse

24. Der zu entschlüsselnde Spruch lautet

25. Die erste Gruppe des Schlüsseltextes
dung der beiden Füllbuchstaben und nach
lichen 3 Buchstaben ergeben sich folgende
Mit Hilfe dieser Kenngruppenbuchstaben
ermittelt und die Schlüsselmaschine nach de
eingestellt.

You can buy a complete copy on www.superborg.de!!!

Die verwendete Grundstellung wird dem »E
z. B. wep (23 05 16) und in den Fenstern der E
eingestellt.

Merkblatt Nr. 6

Sodann werden die im Spruchkopf den 3
stellung (wep) nachgesetzten 3 Geheimbuchstaben
getastet. Die aufleuchtenden Buchstaben xlr stelle

26. Nunmehr stellt der Schlüssel in den Fenste
die Buchstaben des Spruchschlüssels X F R (24 0
Schlüsseltext. Dabei ergeben sich die Buchstaben:

gen kdo roem s e q s angreift fuenften n
uhr mit dritter und zehnter div feind be
milbertshofen nordausgang.

Der endgültige Klartext des Spruches lautet:

Gen. Kdo. VI angreift 5. mai 0315 Uhr mi
bei Maisach. Gef. Stand Milbertshofen No

IX. Merkblatt für das Aufstellen Maschinenschlüsseln

Bei dem Aufstellen von Übungsschlüsseln ist fol

27. Walzenlage muß täglich wechseln. Es sind
wenden.

28. Zum Aufstellen der Ringstellung ist es zu
blättchen (wie beim Pottospiel) herzustellen und
bis 26 zu versehen. Auf diese Weise können in
8 Zeilen (also 8 Tage) in der Spalte Ringst
(2 Zahlen fallen naturgemäß jedesmal aus), z. B.

Tag	Ringstellung	Tag	?
31.	24 14 08	27.	1
30.	17 01 13	26.	2
29.	25 15 19	25.	0
28.	26 12 10	24.	1

You can buy a complete copy on www.superborg.de!!!

Hiermit sind alle Zahlen außer 04 und 20
In gleicher Weise wird die Ringstellung für d
gelegt.

29. Zum Festlegen der 10 Steckerverbindun
Buchstaben des Alphabetes beschriftete Pappbl
wahllos 20 herausgegriffen und zu zweien
sammgelegt werden. Sie werden so aufgesch
Buchstabenpaares die Buchstaben alphabetisch

KV IT BY FG CO EJ DI

30. Zum Kennzeichnen der Schlüsselart sind
gruppen zu je 3 Buchstaben anzufügen. Wä
Schlüssel für den geheimen Nachrichtenverkehr
534, L. Dv. g. 7 Ziff. 27) durch die Oberbefehl
festgelegt werden, sind sie für Übungsschlüssel
3 Buchstaben wahllos zusammengestellt werden

BLV KUX RTZ

Den Oberbefehlshabern der Wehrmachtteile
Übungs- und Sonderschlüssel Kenngruppen zug