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

B e r l i n 1940
G e d r u c k t i n d e r R e i c h s d r u c k e r e i

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”

I. A.
Fellgiebel

Inhaltsverzeichnis.

I.

II.Erklärung von Begriffen und Bezeichnungen.

Klartext oder **offener Wortlaut** ist ein in offener Sprache geschriebener Text.

Geheimtext oder **Schlüsseltext** ist ein nach einem bestimmten Schlüssel umgewandelter Klartext.

Verschlüsseln heißt Umwandeln eines Klartextes in Schlüsseltext.

Entschlüsseln heißt Umwandeln eines Schlüsseltextes in Klartext.

Schlüsseln kann sowohl Ver- als auch Entschlüsseln sein.

Schlüsselverfahren ist das Gesetz, nach dem geschlüsselt wird.

Schlüssel bezeichnet die wechselnden Unterlagen, nach denen bei den einzelnen Verfahren das Schlüsselmittel zum Schlüsseln vorbereitet wird.

Schlüsseltafel ist die Zusammensetzung einzelner Schlüssel für einen längeren Zeitraum.

Schlüsselmittel ist der zum Schlüsseln erforderliche Behelf, z.B. Schlüsselmachine (bisher Chiffriermaschine bezeichnet).

Kenngruppe dient zur Kennzeichnung des in einem Spruch angewedenten Schlüssels.

III.Allgemeines.

1.Der Umfang der Verwendung der Schlüsselmaschine Enigma wird vom Oberkommando der Wehrmacht für die Wehmachtteile gesondert befohlen.

2.Die allgemeinen Schlüsselregeln sind in der Vorschrift “Allgemeine Schlüsselregeln” für die Wehrmacht (H. Dv. g. 7, M. Dv. 534, L. Dv. g. 7), die Anweisung für die Bedienung der Schlüsselmaschine Enigma ist in der “Gebrauchsanleitung für die Schlüsselmaschine Enigma” (H. Dv. g. 13 – L. Dv. g. 13) enthalten.

3.Die Mindestlänge eines mit der Schlüsselmaschine Enigma geschlüsselten Spruches ist unbegrenzt. Die Höchstlänge des zur Übermittlung fertigen Spruches darf 250 Buchstaben nicht überschreiten.

4.Der Spruchkopf enthält

a) Uhrzeit, vierstellig, z.B. 1755,

b) Buchstabenzahl einschl. der 5 Buchstaben der Kenngruppe,

c) die gewählte Grundstellung und den verschlüsselten Spruchschlüssel, z.B. wep hfi

IV.Schlüsselunterlagen.

5.Der Schlüssel wechselt täglich (Tagesschlüssel) um 0000 Uhr. Die Schlüssel und ihre Kennzeichnungen (vgl. IV) werden unter der Zusammenfassung der einzelnen Tagesschlüssel und Kennzeichnungen in einer “Schlüsseltafel” in der Regel für einen Monat ausgegeben.

6.Zur Einstellung der Schlüsselmaschine Enigma enthält der Schlüssel 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 durch Zahlen ausgedrückt werden, treten die Zahlen an Stelle der Buchstaben oder umgekehrt gemäß ihrer Reihenfolge im 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

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

7.Beispiele zu:

6a) Die Walzenlage bezeichnet die Reihenfolge, in der die einzelnen Schlüsselwalzen von links nach rechts in die Schlüsselmaschine Enigma einzusetzen sind (vgl. H. Dv. g. 13, Ziff. 10a und 12),

z.B. II I III

6b) Die Ringstellung zeigt die Einstellung der Buchstaben oder Zahlenringe jeder einzelnen Walze an (vgl. H. Dv. g. 13, Ziff. 10b und 13),

z.B. II I III
13 08 11.

6c) Durch die Angabe der Steckerverbindungen werden die Buchsenpaare gekennzeichnet, welche durch die Doppelsteckerschnüre miteinander zu verbinden sind (vgl. H. Dv. g. 13, Ziff. 10d und 15).

Jeder Buchstabe bezeichnet ein bestimmtes Buchsenpaar und zwei zusammenstehende Buchstaben diejenigen Buchsenpaare, die miteinander verbunden werden sollen, also

AO BI DV EH GZ KW LX MU RY QT.

V.Kennzeichnung des Schlüssels.

8.Der in einem Spruch angewendete Schlüssel wird durch eine fünfstellige Buchstabenkenngruppe gekennzeichnet. Die beiden ersten Buchstaben

(Füllbuchstaben) dieser Gruppe sind beliebig zu wählen und zur Tarnung der Kenngruppe für jeden Spruch zu wechseln. Die **3 letzten** Buchstaben (Kenngruppenbuchstaben) werden der jedem Schlüssel aufgedruckten oder beigefügten "Kenngruppentafel" entnommen. Je Schlüsselbereich und Tag stehen mehrere Kenngruppen zu je 3 Buchstaben zur Verfügung. Diese einzelnen Buchstabengruppen sind abwechselnd zu verwenden; dabei ist die Reihenfolge der einzelnen Buchstaben innerhalb dieser Buchstabengruppen bei jedem Spruch zu ändern.

Bei mehrteiligen Sprüchen ist **jeder Teil für sich** unter Verwendung verschiedener Kenngruppenbuchstaben und verschiedener Füllbuchstaben zu kennzeichnen.

Die Kenngruppe (2 Füllbuchstaben und 3 Kenngruppenbuchstaben) wird als erste Gruppe an den Anfang des Spruches vor den verschlüsselten Spruchschlüssel gesetzt. Die 5 Buchstaben der Kenngruppe sind in die im Spruchkopf enthaltene Buchstabenzahl mit einzurechnen. Die **Kenngruppen** werden **nicht mit verschlüsselt**, sondern vor dem Verschlüsseln des Spruches als erste Gruppe auf das Spruchformular geschrieben, und sind vor dem Entschlüsseln nach Feststellung des Schlüsselbereiches zu streichen.

VI. Verschlüsseln.

9. Die Schlüsselmachine Enigma wird auf Grund der Schlüsselangaben des Tagesschlüssels eingestellt. Diese Einstellung ist für alle mit demselben Schlüssel (z.B. Wehrmacht-Machinenschlüssel) arbeitenden Stellen die gleiche.

Der Schlüßler entnimmt der Schlüsseltafel 3 Kenngruppenbuchstaben, füllt sie durch Voranstellen zweier, frei gewählter Füllbuchstaben zu einer Gruppe von 5 Buchstaben auf und schreibt sie als erste Gruppe des zu übermittelnden Spruches auf das Spruchformular. Anschließend wählt der Schlüßler für **jeden** Spruch eine **besondere** Grundstellung und stellt die Schlüsselmaschine entprechend ein. Die Grundstellung schreibt die Zahlen oder Buchstaben vor, die in den 3 Fenstern der Schlüsselmaschine von links nach rechts einzustellen sind (vgl. H. Dv. g. 13, Ziff 10c und 14).

Z.B. W E P -- 23 05 16.

Die Grundstellung muß bei jedem Spruch, bei mehrteiligen Sprüchen bei jedem Teil, verschieden sein. Bei mehrteiligen Sprüchen darf unter keinen Umständen die am Ende des vorhergehenden Teiles sich ergebende Stellung in den 3 Fenstern der Schlüsselmaschine als Grundstellung oder Spruchschlüssel für den folgenden Teil gewählt werden. Bei der Wahl der Grundstellung sidn die für die Auswahl der Spruchschlüssel gegebenen Weisungen zu beachten (vgl. Ziff. 10). **Grundstellung und Spruchschlüssel** dürfen **nicht gleich** sein.

10. Jeder Spruch ist sodann nach einem besonderen Spruchschlüssel zu verschlüsseln, den sich der Schlüssler selbst aus den Buchstaben bzw. Zahlen für die 3 Ringe A A A bis Z Z Z (01 01 01 bis 26 26 26) wählt. Bei der Wahl der einzelnen Spruchschlüssel ist es verboten, gleiche Buchstaben (A A A), Wörter (ist), Abkürzungen (Rgt.), Rufzeichen des eigenen Verkehrsbereiches, Verkehrszeichen (Q R M), Buchstaben in

Tastaturreihenfolge der Schlüsselmaschine (E R T) oder in alphabetischer Reihenfolge (vorwärts oder rückwärts: A B C – C B A) zu verwenden.

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

11.Der vom Schlüßler gewählte Spruchschlüssel, z.B. X F R (24 06 18), wird auf der nach dem Tagesschlüssel und der gewählten Grundstellung eingestellten Schlüsselmaschine Enigma einmal getastet, die dabei aufleuchtenden 3 Geheimbuchstaben werden den im Spruchkopf eingesetzten 3 Buchstaben angefügt.

12.Der Schlüßler stellt nunmehr in den Fenstern die als Spruchschlüssel gewählten Buchstaben, z.B. X F R (24 06 18), ein und tastet den Klartext. Die hierbei aufleuchtenden Buchstaben werden auf das Spruchformular hinter die 5 Buchstaben der Kenngruppe als 6., 7. 8. usw. Buchstaben geschrieben und alle Buchstaben zu fünfstelligen Buchstabengruppen zusammengefaßt.

VII.Entschlüsseln.

13.Aus dem aufgenommenen Schlüsseltext ist auf Grund der den einzelnen Schlüsseltafeln begedruckten Kenngruppentafeln der verwendete Schlüssel festzustellen und die Kenngruppe zu streichen (vgl. Ziff. 8).

Die Schlüsselmaschine ist nach dem gültigen Tagesschlüssel einzustellen; die Grundstellung ist aus dem Spruchkopf des empfangenen, geschlüsselten Spruches zu entnehmen.

14.Zum Entschlüsseln muß der Schlüßler zuerst den verwendeten Spruchschlüssel (vgl. Ziff. 10 und 11) feststellen. Dazu werden die im Spruchkopf hinter den 3 Buchstaben der Grundstellung angefügetn 3 Buchstaben des verschlüsselten Spruchschlüssels getastet; sie ergeben den dreistelligen Spruchschlüssel.

15.Nunmehr stellt der Schlüßler die Walzen nach dem so gewonnenen Spruchschlüssel in den Fenstern der Maschine ein und tastet vom ~~12.~~ 6. Buchstaben ab den Schlüsseltext. Die hierbei aufleuchtenden Buchstaben werden aufgeschrieben und ergeben den Klartext.

VIII.Ersatz- und Notschlüssel.

16.Zu jedem Maschinenschlüssel wird ein Maschinen-Ersatzschlüssel oder –Handschlüssel ausgegeben, letzterer nach dem Wehrmacht-Handschlüsselverfahren (H. Dv. g. 15a und 15b). Bei Bloßstellung oder Verlust den Maschinenschlüssels tritt der Ersatzschlüssel bei allen Dienststellen, die mit der gleichen Schlüsseltafel arbeiten, an die Stelle des Maschinenschlüssels.

IX.Beispiel.

17.Gültiger Tagesschlüssel:

(Aussschnitt aus der für die Verschlüsselung des Klartextes in Betracht kommenden Schlüsseltafel, z.B. “Wehrmacht-Maschinenschlüssel für Monat Mai”)

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

Nach diesem Tagesschlüssel ist die Schlüsselmaschine einzustellen (vgl. Ziff. 6 und 7).

Der im nachfolgenden Beispiel eingesetzte Schlüsseltext ist aus Geheimhaltungsgründen nicht mit der Schlüsselmaschine getastet, sondern willkürlich gewählt worden.

A. Verschlüsseln

18.Zu verschlüsselnder Spruch:

Tag 4.5.,
Abgangszeit 17,55 Uhr
Gen. Kdo VI
angreift 5. Mai 0345 Uhr mit 3. und 10. Div. Feind bei Maisach. Gef. Stand: Milbertshofen Nordausgang

19.Für die Verschlüsselung ist der Klartext des Spruches nach H. Dv. g. 7 – M. Dv. 534 – L. Dv. g. 7 wir folgt niederzuschreiben:

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.Der Schlüßler stellt die Schlüsselmaschine Enigma nach dem Tagesschlüssel vom 4.5. ein. Sodann trägt er auf dem Spruchformular als 1. Gruppe die Kenngruppe ein (vgl. Ziff. 9), wählt für jeden Spruch bzw. bei mehreren Teilen eines Spruches für jeden Teil eine besondere Grundstellung, z.B. wep (23 05 16), und stellt diese Grundstellung in den Fenstern der Schlüsselmaschine Enigma ein (vgl. Ziff. 9).

21.Der Schlüßler wählt einen Spruchschlüssel, z.B. X F R (24 06 18), und tastet diese 3 Buchstaben einmal, wobei sich die Buchstaben H F I ergeben, die im Anschluß an die 3 Buchstaben der Grundstellung (W E P) in den Spruchkopf niederzuschreiben sind.

22.Nunmehr stellt der Schlüßler bei sosnt gleichbleibender Einstellung der Schlüsselmaschine in den Fenstern die als Spruchschlüssel gewählten Buchstaben X F R (24 06 18) ein und tastet den Klartext. Die sich ergebenden Buchstaben werden im Anschluß an die 5 Buchstaben der Kenngruppe ~~und die 6 Buchstaben des verschlüsselten Spruchschlüssels als 12., 13., 14.,~~ als 6., 7., 8., usw. Buchstaben niedergeschrieben. Dabei werden gleichzeitig Gruppen zu je 5 Buchstaben gebildet.

Es ergibt sich folgender Schlüsseltext:

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.Unter gleichzeitiger Voransetzung des Spruchkopfes (vgl. Ziff. 4) lautet der zur Übermittlung fertige Spruch:

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 = Zeitgruppe
129 = Buchstabenzahl einschl. der 5 Buchstaben der Kenngruppe
wep = vom Schlüßler gewählte Grundstellung
hfi = verschlüsselter Sprchschlüssel
ulnzu = Kenngruppe

Zur Bezeichnung des für die Schlüsselung des Spruches verwendeten Schlüssels ist aus dem Tagesschlüssel (vgl. Ziff. 17) eine der 4 Kenngruppe, z.B. “nuz”, gewählt, die z.B. in “znu” umgestellt und unter Voranstellen zweier Füllbuchstaben, z.B. “ul”, als 1. Gruppe eingetragen ist.

sgexu nfopr . . . . . = verschlüsselter Klartext.

B. Entschlüsseln.

24.Der zu entschlüsselnde Spruch lautet wie vorstehend (Ziff. 23).

25.Die erste Gruppe des Schlüsseltextes ist die Kenngruppe. Nach Streichung der beiden Füllbuchstaben und nach alphabetischer Ordnung der restlichen 2 Buchstaben ergeben sich folgende Kenngruppenbuchstaben: nuz. Mit Hilfe dieser

Kenngruppenbuchstaben wird der angewandte Schlüssel ermittelt und die Schlüsselmaschine nach dem entsprechenden Tagesschlüssel eingestellt.

Die verwendete Grundstellung wird dem “Spruchkopf” entnommen, z.B. wep (23 05 16) und in den Fenstern der Schlüsselmaschine Enigma eingestellt.

Sodann werden die im Spruchkopf den 3 Buchstaben der Grundstellung (wep) nachgestellten 3 Geheimbuchstaben (hfi) des Spruchschlüssels getastet. Die aufleuchtenden Buchstaben xfr stellen den Spruchschlüssel dar.

26.Nunmehr stellt der Schlüssler in den Fenstern der Schlüsselmaschine die Buchstaben der Spruchschlüssels X F R (24 06 18) ein und tastet den Schlüsseltext. Dabei ergeben sich die Buchstaben:

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.

Der endgültige Klartext des Spruches lautet:
Gen. Kdo. VI angreift 5. mai 0345 Uhr mit 3. und 10. Div. Feind bei Maisach.
Gef. Stand Milbertshofen Nordausgang.

X.Merkblatt für das Aufstellen von Übungs-Maschinenschlüsseln.

Bei dem Aufstellen von Übungsschlüsseln ist folgendes zu beachten:
27.Walzenlage muß täglich wechseln. Es sind die Walzen I – V zu verwenden.

28.Zum Aufstellen der Ringstellung ist es zweckmäßig, sich 26 Pappblättchen (wie beim Lottospiel) herzustellen und sie mit den Nummern 1 bis 26 zu versehen. Auf diese Weise können im Sinne des Lottospiels 8 Zeilen (also 8 Tage) in der Spalte Ringstellung ermittelt werden (2 Zahlen fallen naturgemäß jedesmal aus), z.B.:

Tag	Ringstellung	Tag	Ringstellung
31.	24 14 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

Hiermit sind all Zahlen außer 04 und 20 zur Verwendung gelangt. In gleicher Weise wird die Ringstellung für die übrigen Monatstage festgelegt.

29.Zum Festlegen der 10 Steckerverbindungen werden 26 mit je einem Buchstaben des Alphabetes beschriftete Pappblättchen hergestellt, von denen wahllos 20 herausgegriffen und zu zweien als Steckerverbindungen zusammengelegt werden. Sie werden so aufgeschrieben, daß innerhalb eines Buchstabenpaars die Buchstaben alphabetisch ansteigen, z.B.:

KV IT BY FG CO EJ DP MR QS LX

30.Zum Kennzeichnen der Schlüsselart sind dem Tagesschlüssel 4 Kenngruppen zu je 3 Buchstaben anzufügen. Während die Kenngruppen der Schlüssel für den geheimen Nachrichtenverkehr (vgl. H. Dv. g. 7, M. Dv. 534, L. Dv. g. 7 Ziff. 27) durch die Oberbefehlshaber der Wehrmachtteile festgelegt werden, sind sie für Übungsschlüssel frei zu wählen, indem 4mal 3 Buchstaben wahllos zusammengestellt werden. Z.B.

B L V K U X R T Z S W Y.

Den Oberbefehlshabern der Wehrmachtteile ist es freigestellt, auch für Übungs- und Sonderschlüssel Kenngruppen zuzuweisen.

April 1940 Nr. 5 734

Geheim

Berichtigt: Doppelfeld, Ogefr.
20. 7. 42

Deckblätter Nr. 1-8

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

"Schlüsselanleitung zur Schlüsselmaschine Enigma vom 13. 1. 40"