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

Prüf = Nr

Geheim!

Schlüsselangleitung zur Chiffriermaschine Enigma

Vom 8.6.37

Berlin 1937
Gedruckt in der Reichsdruckerei

Editor's note: I was unable to read the original text. However, the general meaning should be as follows.

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.

Inhaltsverzeichnis.

			Seite
I.		Erklärung von Begriffen und Bezeichnungen..	3
II.	1.-2.	Allgemeines	3
III.	3.-5.	Schlüsselunterlagen	3
IV.	6-9.	Verschlüsseln	5
V.	10.-12.	Kennzeichnung des Schlüssels	6
VI.	13.-15.	Entschlüsseln	7
VII.	16.	Notschlüssel	7
VIII.	17.-26.	Beispiel.	8

I. Erklärung von Begriffen und Bezeichnungen.

Klartext ist ein in offener Sprache geschriebener Text.

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

Verschlüsseln heißt Umwandeln eines Klartextes in Geheimtext.

Entschlüsseln heißt Umwandeln eines Geheimtextes in Klartext.

Schlüsseln kann sowohl Ver- als auch Entschlüsseln sein.

Schlüssel ist die wechselnde Ausführungsform für das Schlüsselverfahren (z.B. die Angaben zur Einstellung der Schiffriermaschine).

Schlüsselmittel ist der zum Schlüssel erforderliche Behelf, z.B. Chiffrier-Maschine.

II. Allgemeines

1. Die Verwendung der Schiffriermaschine Enigma wird vom Reichskriegsministerium gesondert befohlen.

2. Die allgemeinen Schlüsselregeln sind in der Vorschrift "Die Heeres-Schlüssel (H. Dv g. 7)", Abschnitt IX, die Anweisung für die Bedienung der Schiffriermaschine Enigma ist in der "Gebrauchsanleitung für die Schiffier-Maschine Enigma (H. Dv. g. 13)" enthalten.

III. Schlüsselunterlagen.

3. Der Schlüssel wechselt täglich (Tagesschlüssel). Die Schlüssel und ihre Kennzeichnungen (vgl. IV.) werden unter Zusammenfassung der einzelnen Tagesschlüssel und Kennzeichnungen in einer "Schlüsseltafel" mit aufgedruckter Kerngruppentafel und Kenngruppenweiser in der Regel für einen Monat ausgegeben

Zur Einstellung der Schiffriermaschine enthält Schlüssel folgende Angaben, die täglich wechfein:

a) Walzenlage (in römifchen zablen),

b) Ringstellung,

c) Grundstellung,

d) Steckerverbindungen.

Mit Aushahme von a webden die Schlüsselangaben durch Buchstaben oder durch Zahlen ausgedruckt, wobei die Zablen an Stelle der Buchstaben gemäßz ihrer Reihenfolge im Alphabet treten.

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 befonderer Buchstabe bei der Chiffirermaschine vorhander ist, fo dass das Alphabet aus 26 Buchstaben be-fteht!) Die Schlüsselangaben find in den folgenden Beifpielen in Buchstaben eingefetzt und die entfprechenden Zahlen in Klammern darunter beigefügt.

5. Beifpiel zu:

4a) Die Walzenlage begichnet die Aechenfolge, in der die einzelnen schiffrierwalzen vonlinks nach rechts in die Schiffriermaschine ein-zufessen find (vgl. H. Dv. g. 13, Ziff. 10a und 12)

e.g. II I III;

4b) Die Ringstellung zeigt die Einstellung der Buchstaben oder Zahlen-ringe jeder einzelnen Walze an (vgl. H. Dv. g. 13, Ziff. 10b un 13)

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

4c) Die Grundstellung schreibt die Zahlen oder Buchstaben vor, die in den 3 Fenften der Chiffiermaschine von links nach rechtz einzustellen find (vgl. H. Dv. g. 13, Ziff. 10c und 11)

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

4d) Durch die Angabe der Steckerverbindungen werten die Buchfenpaare gekennzeichnet, welche durch die Dopperlsteckerfehnure miteinander zu verbinden find (vgl. H. Dv. g. 13, Ziff. 10d und 15). Jeder Buchstabe bzw. jede Zahl bezeichnet ein beftimmtes Buchfenpaar und zwei zufammnenftehende Buchstaben oder zwei durch Schrägftrich ver-bundene Zahlen diejenigen Buchfenpaare, die miteinander verbunden werden follen alfo

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

IV. Berschlüsseln.

6. Die Schiffriermaschine wird auf Grund der Schlüsselangaben eingeftellt. Diefe Einstellung ift für alle mit demfelben Schlüssel (z. B. Wehrlacht-Mafchinenfchlüssel) arbeitenden Stellen die gleiche.

7. Jeder Spruch ift fodann nach einem befonderen Spruchfchlüssel zu verfchlüsseln, den fich der Schlüssler felbft aus den Buchftaben bzw. Zahlen für die 3 Ringe AAA bis ZZZ (01 01 01 bis 26 26 26) wählt. Bei der Wahl der einzelnen Spruchschlüssel ift es ausbdrücklich verboten, gleiche Buch-staben (AAA), Wörten (ift), Abfürzungen (Rgt), Rufzeichen des eigenen Ber-kehrsbereiches, Berkehrszeichen (QRM), Buchstaben in Taftaturreihenfolgeder Schiffiermaschine (ERT) oder in alphabetifcher Reihenfolge (vornvärts oder rückwärts : (ABC-CBA) zu verdenden.

Für jeden Spruch und für jeden taiel eines mehrteiligen Spruches ift am gleichen Tage ftes ein neuer Spruchschlüssel zu benussen.

8. Der von dem Schlüssler gewählte Spruchschlüssel, z. B. XFR (24 06 18), Wird nach Einstellung der Chiffiermaschine auf Grund des vorgefchriebenen Tagesfchlüssels (vgl. Ziff. 6) zweimal nacheinander auf der Chiffreiermaschine getftet. Die fich dabei ergebenden 6 Buchstaben werden dein mit dem Spruchschlüssel zu verfchlüsselnden Spruch vorangefeszt.

9. Der Schlüszler ftellt nunmehr in den Fenften die als Spruchchlüssel gewählten Buchftaben, z. B. XFR (24 06 18), ein und taftet den Kartext. Die hierbei aufleuchtenden Buchftaben werden hinter die durch Taften des Spruchfchlüssels gewonenen Buchftaben gefchrieben und gemeinfam zu gruppe (vgl. Ziff. 10, die "Einfassftelle") ift dabei auszufparen.

V. Kennzeichnung des Schlüssels.

10. Die Kennzeichnung des in einem Spruch angewendeten Schlüssels erfolgt durch eine fünfftellige Buchftaben-Kenngruppe. Die beiden erften Buch-ſtaben (Füllbuchftaben) diefer Gruppe find beliebig zu wählen und zur Tar-nung der Kenngruppe für jeden Spruch zu wechfeln. Die 3 letzten Buch-ſtaben (Kenngruppenbuchſtaben) werden der jedem Schlüſſel aufgedruchten oder beigefügten „Kenngrupptafel" entnommen. Je Schlüſſelbereich und Tag fthen mehrere Kenngruppen zu je 3 Buchtaben zur Verfügung. Diefe einzelnen Buchftabengruppen find abwechfelnd zu vewenden; babei ift die Reihenfolge der einzelnen Buchftaben innerhalb diefer Buchftabengruppen bei jedem Spruch zu ändern.

Bei mehrteiligen Sprüchen erfolgt die Kennzeichnung eines jeden Teiles für fich unter Verwendung verfchiedener Kenngruppenbuchftaben und ver-fchiedener Füllbuchftaben.

Die Kengruppe (2 Füllbuchftaben und 3 kenngruppenbuchftaben) wird in den in Gruppen zup 5 Buchftaben eingeteilten Text des verfchlüllselten Spruches an einer vorher feftgelegten und dafür ausgefparten Stelle (vgl. Ziff. 9) nachträglich eingefügt. Die 5 Buchftaben der Kenngruppe find in die im Spruchkopf enthaltene Buchftabenzahl miteinzurechnen. Die täglich wechfelnde „Einfatzftelle" der kernngruppe ift aus dem mit dem Tages-fchlüſſel gemeinfam ausgegebenen „Kenngruppenweifer" zu entnebmen. Die kenngruppen werden alfo nicht mitverfchlüſſelt, fondern in den bereitz verfchlüſſelten Spruch eingefilgt und vor dem Entfchlüſſeln nach Feſt-ftellung des Schlüſſelbereiches geftrichen (vgl. Ziff. 13).

Ift als kenngruppen-Einfatzftelle die 1. Gruppe vorgefchrieben, fo wird die kenngruppe on den Anfang des Spruches vor den verfchlüſſelten Spruch-fchlüſſel gefetzt.

Die kenngruppe ift dem verfchlüſſelten Spruch als tetzte Gruppe dann an-zufügen, wenn infolge der geringen Buchftabenzahl des Spruches die vor-gefchriebene Einfatzftelle nicht eingehalten werden fann. Enthält bierbei die letzte Textgruppe des verfchlüſſelten Spruches weniger als 5 Buchftaben, fo muss fie vor Anfügen der kernngruppe durch Füllbuchftaben, die den Cinn bes Spruches nicht flören dürfen und untereinander verfchieden fein müffen, auf eine volle Gruppe ergänzt werden.

11. Die Minderftlänge eines mit der Chiffriermafchine gefchlüsselten Spru-ches ift nicht begrenzt. Die Höchftlänge des zur üdermittlung fertigen Spruches darf 180 Buchftaben nich überfchreiten.

12. Der Spruchkopf enthält keine Kennzeichnung des Schlüsselverfahrens, fondern nur

a) Datum vierftellig z. B. 0405 (4.5)

b) Uhrzeit vierftellig z. B. 1755,

c) Buchfteabenzahl eifchl. der 6 Buchftaben des Spruchfchlüssels und der 5 Buchftaben der Kenngruppe.

VI. Entfchüseeln.

13. Aus dem aufgenommenen Schlüsseltext ift auf Grund der den einzelnen Schlüsseltafeln beigedruckten kenngruppentafeln und kenngruppen-weifer der verivendete Schlüssel feftzuftellen und die kenngruppe zu ftreichen (vgl. Ziff. 10).

14. Zum entfchlüsseln muss der Schlüssler zuerft den verwendeten Spruch-fchlüssel fetftellen. Nach Einftellung der Schiffiermaschine gemäss dem gültigen Tagesfchlüssel (fiehe Datum im Spruchkopf) werden die erften 6 buchftaben getaftet; fie ergeben zweimal den dreiftelligen Spruchfchlüssel.

15. Vunnrehr ftellt der Schlüssler die Walzen nach dem fo gemonnenen Spruchfchlüssel in den Fenftern der Mafchine ein und taftet vom 7. Buch-ftaben ab den Schlüsseltext. Die hierbei aufleuchtenden Buchftaben werden aufgefchrieben und ergeben den Klartext.

VII. Notfchlüssel.

16. Zu jedem Mafchinenfchlüssel wird ein Erfatzchlüssel ausgegeben, der nach dem Wehrmacht "Handfchlüsselverfahren (H. Dv. g. 15a und 15b) zu benutzen ift. Beif Blossftellung oder Berluft des Mafchinenfchlüssels tritt er bei allen Dienftellen, die mid der gleichen Schlüsseltafel arbeiten (vgl. H. Dv. g. 7, Ziff. 10), an die Stelle des Mafchinenfchlüssels.

Bei Störungen an der Chiffreiermafchine dient er als Erfassfchlüssel.

VIII. Beifpiel.

17. Gültiger Tagesfchlüſſel:
(Ausfchnitt aus der für die Befchlüsselung des Klartextes in Betracht kommenden Schlüsseltafel, z. B. "....."
Mafchinenfchlüſſel für Monat Mai.)

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. Befchlüsseln.

18. Zu verfchlüselnder Spruch:
Tazg 4. 5.,
Abbgangzeit 17,55 Uhr
Korpskommande VI
angreift 5. Mai 0345 Uhr mit 3. und 10. Div. Feind bei Maifach.
Gef. Stanb. Milbertshofen Vordausgang.

19. Für die Berfchlüsselung ift der Klartext des Spruches gem. H. Dv. g. 7, Ziff. 40 wie fofgt niederzufchreiben:

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. Auf bem Spruchformular bezeichnet der Schlüssler die im Tages-fchlüſſel vorgefchriebene Einfatzftelle (im Beifpiel 2. Gruppe) für die Kenn-gruppe und fpart diefe Gruppe beim Einstragen ddes Spruchfchlüssels bzw. bes Schlüsseltextes aus.

21. Der Schlüssler wählt den Spruchfchlüssel, z. B. XFR (24 06 18), und taftet diefe 3 Buchftaben zweimal nacheinander, wobei fich die Buch-ſtaben hfi klb ergeben, die unter Berückfichtigung der nachtrÄglich ein-zufetzenden Kenngruppe (vgl. Ziff. 20) als erfte Buchftaben des zu be födenden Spruches nieberzufchreiben find.

22. Vunmehr ftellt der Schlüssler bei fonft gleichbleibender Einsftellung der Chiffriermaſchine in den Frenftern die als Spruchfchlüssel gewäblten Buch-ftaben XFR (24 06 18) ein und taftet den klartext. Die fich ergebenden Buchftaben werden im Anfchluss and die 6 buchftaben, die beim Taften des Spruchfchlüssels entftanden find, niedergefchrieben. Dabei werden gleich-zeitig Gruppen zu je 5 buchftaben gebilbet.

Es ergibt fich folgender Schlüsseltext:

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

23. Zur Bezeichnung der für die Schlüsselung des Spruches verwendeten Schlüsseltafel ift aus dem Tagesfchlüssel eine der 4 kenngruppen, z. B. ″nuz″, zu entnhmen, die z. B. in znu umgeftellt wird und unter Voranftellen zweier Füllbuchftaben, z. B. ″ul″, als Kenngruppe an der ausfefparten Stelle einzufeſſen.

Unter gleichzeitiger Voranfetzung des Spruchkopfes (vgl. Ziff. 12à lautet der zur übermittlung fertige Spruch:

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. Entfchlüsseln.

24. Der zu entfchlüsselnde Spruch laute wie vorftehend (Ziff. 23).

25. Aus den Schlüsseltafeln für den Monat Mai ergibt fich für den 4. des Monats als Einfatzftelle die 2. Gruppe, mithin nach Strichung der beiden Füllbuchftaben und nach alphabetifcher Ordnung der reftlichen 3 Buchftaben die kenngruppe nuz.

Mit hilfe diefer kenngruppe wird der verivendete Schlüssel ermittelt und die Schiffriermafchine nach dern Tagesfchlüssel eigeftellt.

Nach Streichung der kenngruppe find die erften 6 buchftaben hfiklb zu taften und gleichfalls im spruch zu fteichen. Der entfchlüsselte spruch-fchlüssel lautet: ″xfr xfr″.

26. Rumehr ftellt der Schlüssler in den Fenftern der Schiffiermaschine die Buchftaben des spruchfchlüssels XFR (24 06 18) ein und tafted den Geheimtext. Dabei ergeben fich die Buchftaben:

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

Der endgültige klartext des spruches lautet:

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

Berlin, den 8. Juni 1937

Der Reichskriegsminifter
und Oberbefehlshaber der Wehrmacht.

J. A.
Fellgiebel.