Vorläufige Schlüsselanleitung zum Doppelkastenschlüssel

Ausgabe Dezember 1941

Source: NSA Historic Cryptographic Collection,
RG 457, Box 7, NR. 57, CBBA17,
PRELIMINARY INSTRUCTIONS FOR DOUBLE ENCIPHERMENT,
US National Archive (NARA), College Park, MD.

URL: https://cryptocellar.org/wmc/schluesselanleitung-dk-1941.pdf

Editor: Frode Weierud, Crypto Cellar Research

Frode Weierud, Crypto Cellar Research
13 February 2021

Oberkommando der Wehrmacht
Chef Wehrmacht-Nachrichtenverbindungen

Stab WNV/Fu I 89a 11 Nr. 1800/41 geh.

Ausfertigungs-Nr. 2663 OKW

Geheim!

Vorläufige Schlüsselanleitung zum Doppelkastenschlüssel

Ausgabe Dezember 1941

A. 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 Geheimtext.

Entschlüsseln heißt Umwandeln eines Geheimtextes 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.

Schlüsselmittel ist der zum Schlüsseln erforderliche Behelf, z. B. Schlüsselblock, Schlüsselmaschine usw.

Schlüsseltafel ist die Zusammenstellung einzelner Schlüssel für einen längeren Zeitraum.

Kenngruppe dient zur Kennzeichnung des für einen Spruch angewendeten Schlüssels.

B. Allgemeines

1. Die für alle Schlüsselverfahren gemeinsam gültigen Bestimmungen der H. Dv. g. 7, M. Dv. 534, L. Dv. g. 7 »Allgemeine Schlüsselregeln für die Wehrmacht« sind auch beim Schlüsseln mit dem Doppelkastenschlüssel zu beachten.

   Für die Luftwaffe gelten außerdem die Bestimmungen der L. Dv. g. 60 »Die Luftwaffenschlüssel«.

2. In Ergänzung der Bestimmungen der »Allgemeinen Schlüsselregeln für die Wehrmacht« Ziffer 11 wird für die Benutzung des Doppelkastenschlüssels folgendes **befohlen:**

   a) Empfangende und absendende Dienststelle sind **nur dann** zu verschlüsseln, wenn sie nicht mit den Kommandostellen übereinstimmen, zu denen die Funkstellen gehören.

   b) Wenn die Verschlüsselung dieser Angaben notwendig ist, so sind sie **stets**, ohne daß Mißverständnisse möglich werden, an **wechselnden** Stellen in den Text des zu verschlüsselnden Spruches aufzunehmen.

   c) Empfangende und absendende Dienststelle (einschl. Unterschrift) dürfen **niemals** am **Anfang** oder **Ende** des Spruches oder Spruchteiles stehen.

3. Der Doppelkastenschlüssel ist ein Handverfahren, bei dem die Klartextbuchstaben durch Ersatzbuchstaben ausgedrückt werden.

4. Die Schlüssel (s. Ziffer 6) wechseln täglich um **0** Uhr. Sie bestehen aus den Kästen A und B zu je 25 Feldern, in die das Alphabet (ohne den Buchstaben »j«) verwürfelt eingetragen ist, und den Kenngruppen.

   Der Buchstabe »j« ist gegebenenfalls durch »ii« zu ersetzen.

   Die Zeilenlänge ist feststehend und beträgt 17 Buchstaben.

5. Die **Mindestlänge** eines mit dem Doppelkastenschlüssel verschlüsselten Spruches oder Spruchteiles ist **nicht begrenzt.**

   Die **Höchstlänge** eines zur Übermittlung fertigen Spruches oder Spruchteiles darf **500 Buchstaben** nicht überschreiten.

6. Vorbereiten der Schlüsselmittel und Schlüssel.

a) **Schlüsselblock:** An Stelle eines Schlüsselblocks kann jedes karierte Papier (z. B. Spruchvordruck) verwendet werden.

Zur Vereinfachung und Beschleunigung des Schlüsselns können die beiden Kästen A und B, wie in Ziffer 6c angegeben, aufgeschrieben werden.

Zur weiteren Vereinfachung des Schlüsselns können Schlüsseltafeln auf Grund der Tagesschlüssel aufgestellt werden, wie es im Abschnitt F dieser Schlüsselanleitung beschrieben ist.

b) **Schlüssel:** Muster eines Tagesschlüssels.

15.

A						B					Kenngr.
h	i	l	q	e	h	z	n	o	c	h	r e t
t	u	a	r	s	t	b	x	a	v	i	l a w
b	k	x	f	g	b	u	d	t	g	w	i w e
p	w	c	o	z	p	m	y	e	l	s	s o g
d	v	y	m	n	d	k	p	q	r	f	

c) Zum Schlüsseln vorbereiteter Tagesschlüssel:

A — Zum Verschlüsseln							B									
h	i	l	q	e	h	h	z	n	o	c	h	z	e	h	i	l	q	e
t	u	a	r	s	t	i	b	x	a	v	i	b	s	t	u	a	r	s
b	k	x	f	g	b	w	u	d	t	g	w	u	g	b	k	x	f	g
p	w	c	o	z	p	s	m	y	e	l	s	m	z	p	w	c	o	z
d	v	y	m	n	d	f	k	p	q	r	f	k	n	d	v	y	m	n
							B — Zum Entschlüsseln									A

C. Kenngruppen

7. Der für einen Spruch angewendete Schlüssel wird durch dreistellige Buchstabenkenngruppen gekennzeichnet, die mit dem täglich wechselnden Schlüssel ausgegeben werden.

Je Schlüssel stehen täglich vier Kenngruppen zur Verfügung, die abwechselnd zu verwenden sind. Die Reihenfolge der Buchstaben innerhalb dieser Kenngruppen wechselt **nicht.** Bei **mehrteiligen** Sprüchen ist bei jedem Teil die **gleiche** Kenngruppe zu verwenden.

8. Die Kenngruppen werden nicht mit verschlüsselt, sondern in den Spruchkopf hinter die Buchstabenzahl eingefügt.

Beispiel:

Kenngruppen: r e t l a w i w e s o g

Spruchkopf: — 1512 — 54 — i w e —

D. Verschlüsseln

9. Klartext:

1512 — Feindlicher Angriff auf Straße Adorf–Behausen abgewehrt.

Der Klartext wird grundsätzlich in Zeilen zu je 17 **Buchstaben** nach den »Allgemeinen Schlüsselregeln« so niedergeschrieben, daß zwischen je zwei Zeilen ein Abstand bleibt.

Die keine Doppelzeile ausfüllenden Restbuchstaben werden so in zwei Zeilen eingetragen, daß je zwei Buchstaben untereinander stehen.

Ist die Anzahl der Buchstaben ungerade, so wird dem letzten Buchstaben des Klartextes ein frei gewählter **(außer »x«)**, bei den einzelnen Sprüchen **wechselnder** Buchstabe als Blender angehängt.

Beispiel:

f	e	i	n	d	l	i	q	e	r	a	n	g	r	i	f	f		
a	u	f	s	t	r	a	s	z	e	a	d	o	r	f	s	t		
r	i	q	b	e	h	a	u	s	e									
n	a	b	g	e	w	e	h	r	t									

10. Die untereinanderstehenden Buchstaben werden zu Paaren zusammengefaßt und gemeinsam verschlüsselt. Die Buchstaben der oberen Zeile bilden bei den Paaren immer den »1. Klarbuchstaben« und die Buchstaben der unteren Zeile immer den »2. Klarbuchstaben«.

11. Der 1. Klarbuchstabe eines jeden Buchstabenpaares wird im Kasten A, der 2. Klarbuchstabe eines jeden Buchstabenpaares im Kasten B aufgesucht und nach den folgenden Vorschriften ersetzt.

12. Stehen die beiden Klarbuchstaben **in derselben Zeile,** so wird der

    1. Klarbuchstabe durch den Buchstaben ersetzt, der rechts vom 2. Klarbuchstaben im Kasten B steht; der
    2. Klarbuchstabe durch den Buchstaben ersetzt, der rechts vom 1. Klarbuchstaben im Kasten A steht.

Z. B.: »a a« (klar) wird »v r« (geheim).
(Zwischentext).

13. Stehen die beiden Klarbuchstaben in beiden Kästen **in verschiedenen Zeilen,** so werden sie durch das Buchstabenpaar ersetzt, das mit dem Klarbuchstabenpaar die Ecken eines Rechteckes oder eines Quadrates bildet. Dabei wird der Geheimbuchstabe aus Kasten B als erster und der Geheimbuchstabe aus Kasten A als zweiter gelesen.

Z. B.: »f a« (klar) wird »t r« (geheim)
(Zwischentext).

14. Die so gefundenen Buchstabenpaare (Zwischentext) werden nach ihrem Auffinden sofort **noch einmal** nach den gleichen Vorschriften verschlüsselt und als Geheimbuchstaben von links nach rechts in Gruppen zu je fünf Buchstaben auf einen Spruchvordruck geschrieben.

Beispiel: Es werden also

aus dem Klarbuchstabenpaar »aa« über »vr« das endgültige Geheimbuchstabenpaar »fy« und aus dem Klarbuchstabenpaar »fa« über »tr« das endgültige Geheimbuchstabenpaar »vd«.

15. Der Spruchkopf enthält Zeitgruppe, Buchstabenzahl und Kenngruppe. Zur Beschleunigung kann die Buchstabenzahl statt im Spruchkopf auch am Ende der Gruppen (zwischen Trennungszeichen gesetzt) angefügt werden. Sie bleibt dennoch ein Teil des Spruchkopfes.

16. Der zur Übermittlung fertige Spruch lautet:

1512 — 54 — iwe —

v d l g c t u q z r e o m f c i f e a l
f y l b a p k w c t e i w b t y m f l n
m v m q z t y l h u p i l f

E. Entschlüsseln

17. **Geheimtext:**

1512 — 54 — iwe —

v d l g c t u q z r e o m f c i f e a l
f y l b a p k w c t e i w b t y m f l n
m v m q z t v l h u p i l f

Der Geheimtext wird von links nach rechts in Paare abgeteilt.

1512 — 54 — iwe —

v d/l g/c t/u q/z r/ e o/m f/c i/f e/a l/
f y/l b/a p/k w/c t/ e i/w b/t y/m f/l n/
m v/m q/z t/v l/h u/ p i/l f

18. Der 1. Geheimbuchstabe eines jeden Buchstabenpaares wird im Kasten B, der 2. Geheimbuchstabe eines jeden Buchstabenpaares im Kasten A aufgesucht und nach den folgenden Vorschriften ersetzt.

19. Stehen die beiden Geheimbuchstaben in beiden Kästen **in derselben Zeile**, so wird

der 1. Geheimbuchstabe durch den Buchstaben ersetzt, der links von dem 2. Geheimbuchstaben im Kasten A steht, und

der 2. Geheimbuchstabe durch den Buchstaben ersetzt, der links von dem 1. Geheimbuchstaben im Kasten B steht.

Z. B.: »f y« (geheim) wird »v r« (Zwischentext).

20. Stehen die beiden Geheimbuchstaben in beiden Kästen **in verschiedenen** Zeilen, so werden sie durch das Buchstabenpaar ersetzt, das mit dem Geheimbuchstabenpaar die Ecken eines Rechteckes oder eines Quadrates bildet. Dabei wird der Klarbuchstabe (bzw. Zwischenbuchstabe) aus dem Kasten A als erster und der Klarbuchstabe (bzw. Zwischenbuchstabe) aus dem Kasten B als zweiter gelesen.

Z. B.: »v d« (geheim) wird »t r« (Zwischentext).

21. Die so gefundenen Buchstaben (Zwischentext) werden nach ihrem Auffinden sofort **noch einmal** nach den gleichen Vorschriften ersetzt und (der Zeilenlänge 17 entsprechend) als Klartext paarweise untereinander von links nach rechts niedergeschrieben.

Beispiel: Es werden also

aus dem Geheimbuchstabenpaar »fy« über »vr«
das endgültige Klarbuchstabenpaar »aa« und
aus dem Geheimbuchstabenpaar »vd« über »tr«
das endgültige Klarbuchstabenpaar »fa«.

22. Der in Doppelzeilen von je 17 Buchstaben niedergeschriebene Klartext lautet dann:

f	e	i	n	d	l	i	q	e	r	a	n	g	r	i	f	f		
a	u	f	s	t	r	a	s	z	e	a	d	o	r	f	s	t		
r	i	q	b	e	h	a	u	s	e									
n	a	b	g	e	w	e	h	r	t									

23. Der Klartext wird sodann auf einen Spruchvordruck niedergeschrieben

1512 — Feindlicher Angriff auf Straße Adorf—Behausen abgewehrt.

F. Schlüsseltafeln für Tagesschlüssel

(Vordrucke siehe Anlagen 1 und 2.)

24. Zum Vereinfachen der Schlüsselarbeit **können** für einzelne Tagesschlüssel Schlüsseltafeln aufgestellt werden, bei denen alle Klarbuchstabenpaare von aa, ab usw. bis zz gleich mit den entsprechenden Geheimbuchstabenpaaren zusammengeschrieben werden (siehe Anlage 3). Die Zwischenbuchstabenpaare erscheinen in dieser Tafel **nicht** mehr.

Zum Entschlüsseln ist eine zweite besondere Tafel entsprechend aufzustellen (siehe Anlage 4).

Die in den Anlagen 3 und 4 aufgestellten Muster für Schlüsseltafeln entsprechen dem in Ziffer 6 dargestellten Schlüsselmuster und können daher auch zum Schlüsseln der in dieser Schlüsselanleitung wiedergegebenen Beispiele benutzt werden.

25. Das Aufstellen dieser Schlüsseltafeln erfordert bei zwei sehr gewandt und sorgfältig arbeitenden Schlüsslern etwa vier Stunden. Diese Arbeit ist daher nur dann lohnend, wenn voraussichtlich eine größere Anzahl von Sprüchen zum Schlüsseln zu erwarten sein wird.

G. Ersatz- und Notschlüssel

26. Zur Sicherstellung von schlüsselsicheren Nachrichtenverbindungen im Falle der Bloßstellung von Schlüsselunterlagen werden zum Doppelkastenschlüssel entweder Ersatzschlüssel oder Notschlüssel ausgegeben.

27. **Ersatzschlüssel** sind in Schlüsseltafeln für einen ganzen Monat (31 Tage) zusammengefaßt, aber meistens nicht mit einer bestimmten Monatsangabe versehen. Sie sind **getrennt** von den übrigen Schlüsseln zu befördern und aufzubewahren, so daß ein gleichzeitiger Verlust mit den Gebrauchsschlüsseln unmöglich ist. Eine Ausgabe der Ersatzschlüssel an Dienststellen, bei denen Feindberührung zu erwarten ist, erfolgt erst im Bedarfsfall, d. h. wenn der Gebrauchsschlüssel bloßgestellt und die Inkraftsetzung des Ersatzschlüssels befohlen ist.

28. **Notschlüssel** entsprechen in ihrem Aufbau einem einzelnen Tagesschlüssel mit besonderen Kenngruppen. Die Notschlüssel werden an solche Dienststellen ausgegeben, bei denen infolge unmittelbarer Feindeinwirkung die Möglichkeit einer Schlüsselbloßstellung besteht und das rechtzeitige Heranbringen von Ersatzschlüsseln nicht sichergestellt werden kann. Notschlüssel (einschl. Kenngruppen) sind **sofort** nach Eingang der Schlüsselunterlagen **unverfänglich** (z. B. als Teil eines Funkspruches) aufzuschreiben; der Schlüssel selbst ist dann **sofort** durch **Feuer** zu vernichten.