

Schlüsselanleitung zum Doppelkastenschlüssel

Entwurf vom 2.12.1940

Source: TICOM Document T-16, Box 14,
Bestand Rückgabe TICOM, S8,
Politisches Archiv des Auswärtigen Amts, Berlin.

URL: <https://cryptocellar.org/wmc/schluesselanleitung-dk-1940.pdf>

Editor: Frode Weierud, Crypto Cellar Research

Oberkommando des Heeres
Gen St & H /Chef HNW IV
47 p 12 (M) S Nr. 7030/40 geh.

Prüf-Nr. 1727

Geheim!

12

Schlüsselanleitung

zum

Doppelkastenschlüssel.

Entwurf vom 2.12.1940.

Dies ist ein geheimer Gegenstand im Sinne des § 88 Reichs-Straf-Gesetzbuch (Fassung vom 24. April 1934). Mißbrauch wird nach den Bestimmungen dieses Gesetzes bestraft, sofern nicht andere Strafbestimmungen in Frage kommen.

Inhaltsverzeichnis.
=====

I.		Erklärung von Begriffen und Bezeichnungen
II.	1. - 6.	Allgemeines
III.	7. - 8.	Verschlüsseln
IV.	9. - 11.	Entschlüsseln.

I. 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 ein 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.

II. Allgemeines.

- 1.) Die für alle Schlüsselverfahren gemeinsam gültigen "Allgemeinen Vorschriften für das Schlüsseln" sind auch beim Doppelkastenschlüssel zu beachten.
- 2.) Der Doppelkastenschlüssel ist ein Handverfahren, bei dem die Klartextbuchstaben durch Ersatzbuchstaben ausgedrückt werden.
- 3.) Die Schlüsselunterlagen (vgl. Ziff. 6) wechseln täglich um 00,00 Uhr. Sie bestehen aus zwei Kästen (Buchstabentauschtafel A und B) zu je 25 Feldern, in die das Alphabet ohne den Buchstaben "j" verwürfelt eingetragen ist. Der Buchstabe "j" ist gegebenenfalls durch die Buchstaben "ii" zu ersetzen. Die Zeilenlänge ist feststehend und beträgt 17 Buchstaben.
- 4.) Vorbereiten der Schlüsselmittel:
Schlüsselblock: Anstelle des Schlüsselblockes kann jedes karierte Papier (z.B. Spruchformular) verwendet werden. Zur Vereinfachung und Beschleunigung des Schlüssels können die 2 Kästen, wie in Ziff. 6b angegeben, aufgeschrieben werden.
- 5.) Ein Notschlüssel zum Doppelkastenschlüssel ist nicht vorgesehen.

6.) Schlüsselunterlagen.

a) Muster eines Tagesschlüssels:

Tag: 15.

A

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

B

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

b) Zum Schlüsseln vorbereiteter Tagesschlüssel:

Zum Verschlüsseln

A

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

A

Zum Entschlüsseln

III. Verschlüsseln.

7.) a) Klartext:

1512 - Feindlicher Angriff auf Strasse Adorf-Behausen
abgewehrt.

b) Der Klartext wird grundsätzlich in Zeilen zu 17 Buchstaben
nach den allgemeinen Schlüsselvorschriften so niedergeschrie-
ben, daß zwischen je 2 Zeilen ein Zwischenraum bleibt. Die

d) 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 5 Buchstaben auf das Spruchformular geschrieben.

Es werden also z.B.

aus dem Klarbuchstabenpaar "fg" über "wg" das endgültige Geheimbuchstabenpaar "lk",

und aus dem Klarbuchstabenpaar "er" über "cn" das endgültige Geheimbuchstabenpaar "yl".

Der Spruchkopf enthält Zeitgruppe und Buchstabenzahl. Zur Beschleunigung kann die Buchstabenzahl anstatt im Spruchkopf auch am Ende der Gruppen - zwischen Trennungszeichen gesetzt - angefügt werden. Sie bleibt dennoch ein Teil des Spruchkopfes.

Der zur Übermittlung fertige Spruch lautet:

1512 - 54 -

v d l g c	t u q z r	e o m f c	i n i 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	

IV. Entschlüsseln.

9.) a) Geheimtext:

1512 - 54 -

v d l g c	t u q z r	e o m f c	i n i 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	

b) Der Geheimtext wird von links nach rechts in Paare abgeteilt.

10.) a) Der 1. Geheimbuchstabe eines jeden Buchstabenpaares wird im Kasten B, der 2. Geheimbuchstabe eines jeden Buchstabenpaares im Kasten A aufgesucht und nach folgenden Vorschriften ersetzt:

Der Klartext wird sodann auf ein Spruchformular geschrieben:

1512

Feindlicher Angriff auf Strasse Adorf-Behausen
abgewehrt.