Anmerkung:

Mit BMVg-Schreiben vom 9.7.1992, Gesch.Z.:
Fü S VII 4, Einstufung "VS-Vertraulich"
aufgehoben.
Köln, 21.7.1992

Mispun

KRYPTO

(Merkschrift)

Anleitung

zum

Bundeswehr-Handschlüssel (Reihenschieberverfahren)

[redacted]

ZSV 55/512

Ausgabe: März 1960

(M e r k s c h r i f t)

A n l e i t u n g
zum
Bundeswehr-Handschlüssel
(Reihenschieberverfahren)

[redacted]

Ausgabe: März 1960

Herausgegeben von der
Fernmeldedienststelle der Bundeswehr Abt. IV

Mit Ausgabe dieser Vorschrift tritt die Ausgabe Januar 1958 (ZDv 55/12) außer Kraft und ist gemäß ZDv 2/31 zu vernichten.

Inhaltsverzeichnis

K a p i t e l 1

B e s c h r e i b u n g

Abschnitt I - Allgemeines

1Ø1. Das Reihenschieberverfahren

a) Das Reihenschieberverfahren ist ein Handschlüssel.

b) Der Reihenschieber (Kurztitel: RS) wird dabei als Schlüsselherstellungsgerät benutzt. Aus ihm werden zufallsähnliche Folgen von Ziffern, die Schlüsselreihen, abgeleitet.

c) Mit den Schlüsselreihen wird Klartext in einer Umsetztabelle verschlüsselt.
Der Klartext kann aus Buchstaben und Ziffern zusammengesetzt sein. Ziffern brauchen nicht in Buchstaben umgewandelt werden.

Der Geheimtext besteht aus Buchstaben.

d) Für jeden Spruch ist eine neue Schlüsselreihe abzuleiten.

1Ø2. Verschlüsselung von eingestuftem Klartext

a) Das RS-Verfahren ist im nationalen Schlüsseldienst für Sprüche aller VS-Grade zugelassen.

b) Jeder Spruch ist mit seinem vollständigen Klartext zu verschlüsseln und darf nur verschlüsselt, also nicht in Verbindung mit Klartext übermittelt werden.

Abschnitt II - Bestandteile des Schlüsselmittels

1Ø3. Der Reihenschieber

a) Der Reihenschieber ist VS-NfD eingestuft.

b) Er besteht aus:

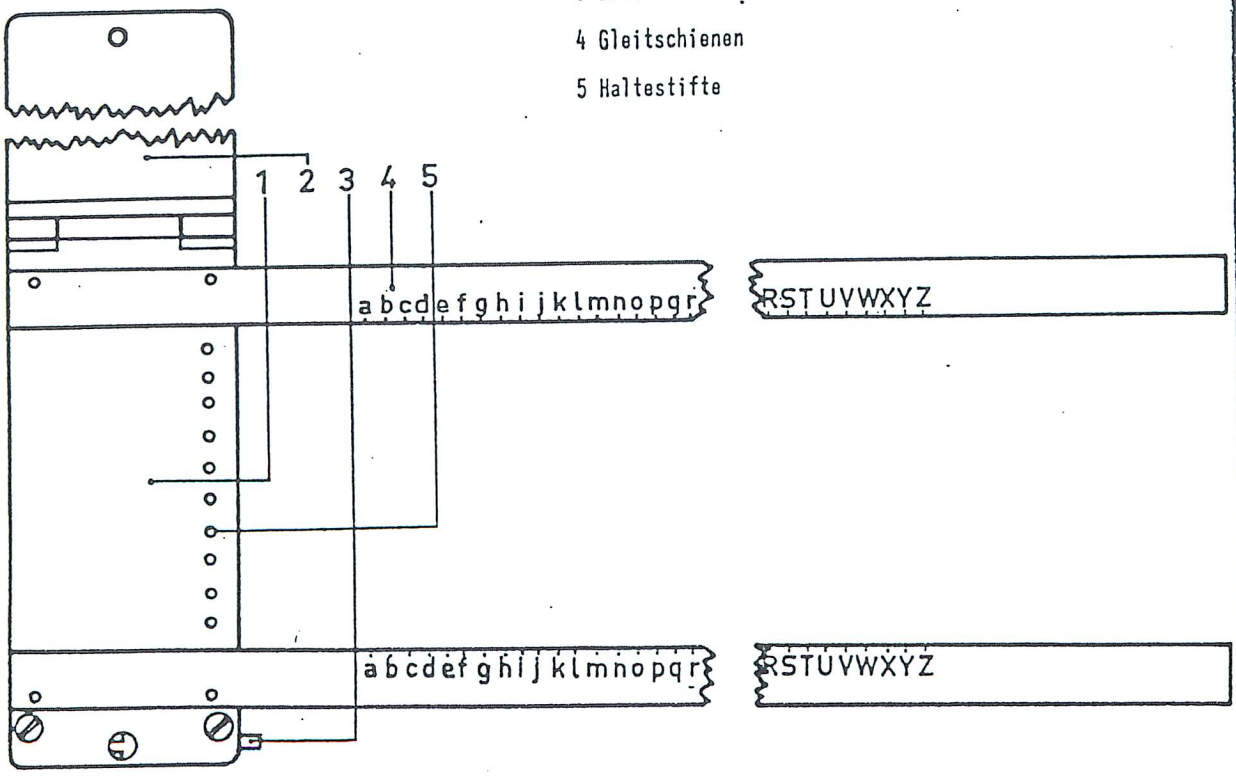
(1) einem Schloß mit zwei Gleitschienen. (Abbildung 1)

Die Vorderseite des Schlosses ist schwarz, die Rückseite weiß gefärbt.
Jede Gleitschiene trägt auf der Vorderseite ein kleines und ein großes Alphabet.

Abbildung 1

Schloß mit 2 Gleitschienen

1 Schloß
2 Schloßdeckel, geöffnet
3 Druckverschluß
4 Gleitschienen
5 Haltestifte



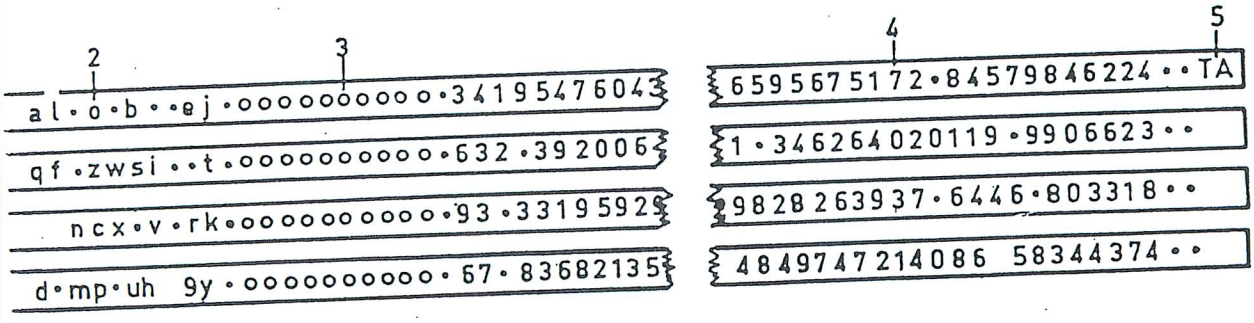
(2) 26 Stäben, von denen jeweils 1Ø in das Schloß eingelegt werden.

Jeder Stab trägt von links nach rechts folgende Zeichen:
1 großen Buchstaben (A - Z) auf 4 Seiten: Kennung der 26 Stäbe.
26 kleine Buchstaben (a - z) verwürfelt auf 4 Seiten verteilt: Kennung der Stabseiten.
Je 1Ø Durchbohrungen auf 4 Seiten: für die Haltestifte im Schloß.
Verwürfelte Zahlenreihen auf 4 Seiten: für die Ableitung von Schlüsselreihen.
2 große Buchstaben auf 1 Seite: Kennung der Stabserie.
Eine Stabserie ist für unbestimmte Zeit gültig und kann durch neue Serien ersetzt werden.

idun

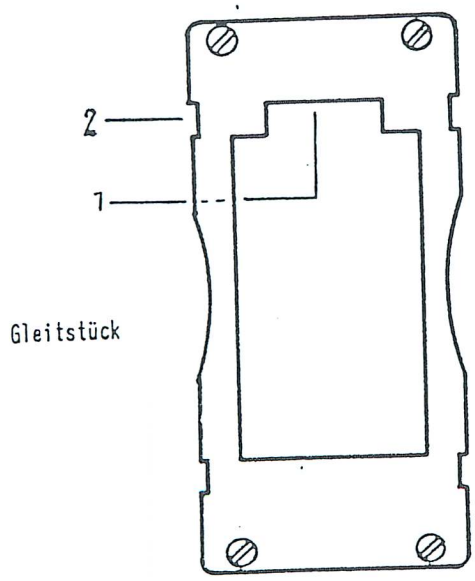
Die 4 Seiten eines abgerollten Stabes

1 Stabkennung
2 Verwürfeltes Alphabet
3 Durchbohrungen
4 Ziffernfolgen
5 Serienkennung



(3) einem Gleitstück (Abbildung 3), das auf die Gleitschienen aufgeschoben wird und in 52 Stellungen einrasten kann. Die Vorderseite des Gleitstückes ist schwarz.

ildung 3



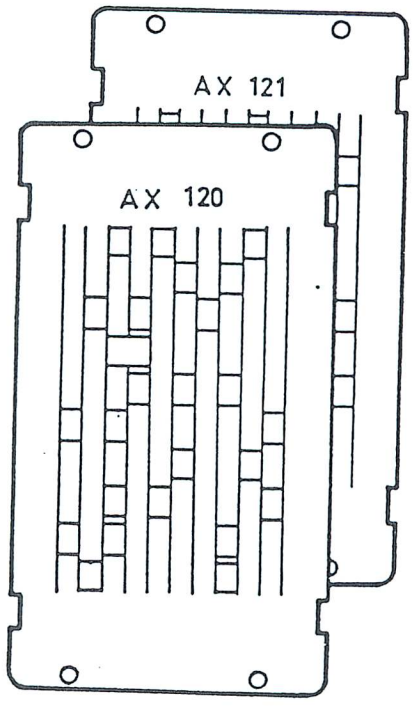
1 Ausnehmung für Schablonenkennung
2 Einstellung der Ausgangsstellung

1Ø4. Die Schlüsselunterlagen

a) Vorgeschriebene Unterlagen, die für jeden Schlüsselbereich verschieden sind. Muster einer monatlichen Ausgabe sind in den Anlagen 1, 2a und 2b dargestellt.

(1) Der Dekadenschlüssel besteht aus 2 Schablonen. Je 1 Schablone wird in die Vorder- und Rückseite des Gleitstücks eingeschoben. Die Schablonen sind mit dekadenweise wechselnden Zahlen und Buchstaben bezeichnet und enthalten etwa 25 Fenster in zufälliger Anordnung. (Abbildung 4).Sie werden als Schlüsselunterlage versandt.
Der Schlüssler darf nur die 2 für die jeweilige Dekade gültigen Schablonen erhalten.
Die Schablonen sind aus brennbarem Kunststoff hergestellt und nach Ablauf ihrer Gültigkeit zu vernichten.

Abbildung 4



Dekadenschlüssel
(2 Schablonen)

(2) Der Tagesschlüssel besteht aus 1Ø verschiedenen großen Buchstaben, die 1Ø von 26 Stäben und ihre für einen Tag gültige Reihenfolge von oben nach unten im Schloß angeben.
(= Stabfolge).

Muster eines Tagesschlüssels

W L X T B A N D O F

(3) Die Spruchschlüsselzahl besteht aus 1Ø beliebigen Ziffern. Sie ist für einen Tag gültig. Mit der Spruchschlüsselzahl wird die für jeden Spruch neu zu wählende Bereichskenngruppe in der Umsetztabelle in den Spruchschlüssel umgewandelt.

Muster einer Spruchschlüsselzahl

3 1 4 8 4 8 5 1 Ø 4

(4) Die Umsetztabelle

(a) Die Umsetztabelle ist für einen Monat gültig. Sie besteht aus dem Teil "Verschlüsseln" (dargestellt in Anlage 2 a) und dem Teil "Entschlüsseln" (dargestellt in Anlage 2 b).

(b) Die Umsetztabelle ist aus schlüsseltechnischen Gründen in zwei Hälften unterteilt, die wie folgt aufgebaut sind:
am linken Rand jeder Tabellenhälfte stehen untereinander die Buchstaben von A bis Z;
am rechten Rand jeder Tabellenhälfte die Ziffern von Ø bis 9;
am oberen Rand jeder Tabellenhälfte die Ziffernfolge von Ø bis 9
und darüber bei der linken Tabellenhälfte die Ziffern Ø - 4,
bei der rechten Tabellenhälfte die Ziffern 5 - 9.

(c) Beide Tabellenhälften "Verschlüsseln" enthalten in 26 Zeilen je 1Ø Buchstaben des Alphabets in verwürfelter Folge.

(d) Die Handhabung der Tabelle "Verschlüsseln" ist in Ziffer 3Ø7 erläutert.

(e) Die Tabelle "Entschlüsseln" ist so aufgesetzt, daß die verwürfelten Buchstaben in den Innenfeldern die Gegenwerte der Tabelle "Verschlüsseln" darstellen.

(f) Die Handhabung der Tabelle "Entschlüsseln" ist in Ziffer 3Ø8. erläutert.

b) Abzuleitende Unterlagen, die zum Schlüsseln jedes Spruches neu zu erstellen sind.

(1) Die Bereichskenngruppe ist mit dem Bereichskenngruppenschlüssel aus 5 Buchstaben zu bilden. Jeder Spruch erhält eine neue Bereichskenngruppe, die den benutzten Schlüssel angibt und zur Ableitung des Spruchschlüssels erforderlich ist.

Muster einer Bereichskenngruppe

m w l k w

(2) Der Spruchschlüssel ist beim Verschlüsseln und Entschlüsseln eines jeden Spruches neu zu bilden:

(a) Die 5 Buchstaben der Bereichskenngruppe sind zweimal hintereinander zu schreiben.

Beispiel: m w l k w m w l k w

(b) Darüber ist die Spruchschlüsselzahl zu setzen.

Beispiel: 3 1 4 8 4 8 5 1 Ø 4
m w l k w m w l k w

(c) Dann sind die 1Ø Buchstaben der doppelten Bereichskenngruppe mit der Spruchschlüsselzahl in der Umsetztabelle "Verschlüsseln" zu verschlüsseln, wie es in Nr. 3Ø7 für die Textverschlüsselung beschrieben ist.

Beispiel:

Spruchschlüsselzahl: 3 1 4 8 4 8 5 1 Ø 4

Bereichskenngruppe (doppelt): m w l k w m w l k w

Spruchschlüssel: r n c z w y u d x e

Die Schlüsselschritte im einzelnen dargestellt:

Buchstaben der doppelten Bereichskenngruppe	Schlüsselziffer	rechte Ziffer neben der Schlüsselziffer weist auf Umsetztabellenhälfte		Schlüsselergebnis (= Spruchschlüssel)
		links	rechts	
m	3	1		r
w	1	4		n
l	4		8	c
k	8	4		z
w	4		8	w
m	8		5	y
w	5	1		u
l	1	Ø		d
k	Ø	4		x
w	4	4		e

(d) Das Ergebnis ist der Spruchschlüssel. Seine 1Ø Buchstaben geben die Lage der 1Ø Stäbe im Schloß an, d.h. die 1Ø Buchstaben müssen am linken Schloßrand in der Reihenfolge von oben nach unten zu lesen sein. Siehe Abbildung 5 Ziffer 3. (= Stablage). Der letzte Buchstabe wird auf der kleinen Alphabetreihe der Gleitschiene aufgesucht und in der linken Ausnehmung des Gleitstücks eingestellt. Siehe Abbildung 5 Ziffer 4. (= Ausgangsstellung).

(e) Der Spruchschlüssel ist beim Verschlüsselungs- und beim Entschlüsselungsvorgang in der gleichen Weise zu bilden. In beiden Fällen ist nur die Umsetztabelle "Verschlüsseln" zu benutzen.

K a p i t e l 2

Allgemeine Richtlinien für das RS-Verfahren

2Ø1. Allgemeines

Eine Umschreibung des Klartextes ist zur Vorbereitung für die Verschlüsselung nicht erforderlich. Stereotype Spruchanfänge und -beendigungen beeinträchtigen die Schlüsselsicherheit des Verfahrens nicht.
An- und Unterschriften dürfen deshalb am Anfang und Ende eines Spruches stehen. Ebenso unbedenklich können Spruchwiederholungen ohne Klartextumstellungen vorgenommen werden, wenn zum wiederholten Verschlüsseln eine neu abgeleitete Schlüsselreihe benutzt wird.

2Ø2. Vorbereitende Ableitung von Schlüsselreihen

Das RS-Verfahren ermöglicht die vorbereitende Ableitung von Schlüsselreihen, so daß bei Eingang von Sprüchen die Schlüsselungszeiten wesentlich verkürzt werden können.

2Ø3. Codress

Bei dem Gebrauch des RS-Verfahrens wird die Codress-Übermittlung angewandt. Näheres siehe ZDv 55/1Ø.

2Ø4. Spruchköpfe

Für die Bildung und Kennzeichnung der Spruchköpfe verschlüsselter Sprüche gelten, soweit sie in dieser Vorschrift nicht behandelt werden, die entsprechenden Betriebsvorschriften des Funk- oder Fernschreibdienstes.

2Ø5. Einteilung in Schlüsselteile

Sprüche mit mehr als 1ØØØ Klartextzeichen sind in zwei oder mehr Schlüsselteile aufzuteilen. Näheres siehe ZDv 55/1Ø. Jeder Schlüsselteil muß eine neue Bereichskenngruppe erhalten.

2Ø6. Vorbereitung des Klartextes

a) Vor dem eigentlichen Verschlüsseln muß der Klartext so vorbereitet werden, daß in ihm nur die 26 Buchstaben des Alphabets und die Ziffern von Ø bis 9 vorkommen.

b) Die Umlaute ä werden durch ae
ö " oe
ü " ue
und das ß " ss ersetzt.

c) Interpunktionszeichen werden im allgemeinen durch den Buchstaben "x" ersetzt. Wo zum Verständnis des Textes ausführliche Interpunktionszeichen erforderlich werden, sind hierfür folgende Abkürzungen anzuwenden:

Fragezeichen:	= QUES	Komma:	= CMM
Bindestrich:	= DASH	Schrägstrich:	= SLANT
Doppelpunkt:	= CLN	Absatz:	= PARA
Klammer:	= PAREN	Anführungsstriche:	= QUOTE und UNQUOTE
Punkt:	= PD		

Diese Abkürzungen sind - entgegen Ziffer 2Ø6 f) - nicht in "y" einzuschließen.

d) Zahlen können in Ziffern oder Buchstaben ausgeschrieben werden. Werden Zahlen als Ziffer verschlüsselt, so ist jede Zahl zweifach - also einmal wiederholt - zu schreiben und die Zahl und ihre Wiederholung in "q" einzurahmen. Der Buchstabe "q" kündigt dabei Anfang und Ende einer Zahl in Ziffern an.

Beispiel: Die Zahl "1235" lautet vorbereitet: "q 1235 q 1235 q".

e) Erscheint im Klartext ein Wort mit dem Buchstaben "q", so ist anstelle des "q" ein "k" zu schreiben.

f) Dienststellen, Eigennamen und Abkürzungen sind in "y" einzuschließen. Einstellige und nicht allgemein bekannte Abkürzungen sind nicht anzuwenden, sondern auszuschreiben.
Um Irrtümer zu vermeiden, können Eigennamen und Abkürzungen wiederholt (zweimal) geschrieben werden.

Beispiel: "y Behausen y". "y STVO y STVO y".

Beispiel für die Vorbereitung eines Klartextes

Ein zu verschlüsselnder Klartext sei: "Der Feind greift seit Ø535 Uhr Behausen an."

Der zum Verschlüsseln vorbereitete Klartext lautet: "Der Feind greift seit q Ø535 q Ø535 q Uhr y Behausen y an."

K a p i t e l 3

Schlüsselvorgang

Abschnitt I - Vorbereitende Arbeitsvorgänge

3Ø1. Der Schlüsselvorgang erfordert folgende vorbereitende Arbeitsvorgänge:

a) Vorbereitung des Klartextes
b) Bildung der Bereichskenngruppe
c) Bildung des Spruchschlüssels
d) Einstellung des RS-Gerätes
e) Herauslesen der Schlüsselreihe aus dem RS-Gerät.

3Ø2. Die Vorbereitung des Klartextes ist gemäß Ziffer 2Ø6 durchzuführen, um die Länge der Schlüsselreihe zu bestimmen.

3Ø3. Die Bereichskenngruppe ist gemäß Ziffer 1Ø4. b) (1) zu bilden und als erste und letzte Gruppe in den Spruch einzusetzen.

Ø4. Spruchschlüssel
Der Spruchschlüssel ist gemäß Ziffer 1Ø4. b) (2) zu bilden und darf nicht übermittelt werden.

3Ø5. Einstellung des RS-Gerätes

a) Der Dekadenschlüssel ist gemäß Ziffer 1Ø4. a) (1) einzustellen.

b) Der Tagesschlüssel ist gemäß Ziffer 1Ø4. a) (2) einzustellen.

c) Der Spruchschlüssel ist gemäß Ziffer 1Ø4. b) (2) (d) einzustellen.

Beispiel:

Dekadenschlüssel: AX 12Ø (Vorderseite Gleitstück) (aus Schlüsselunterlage)
AX 121 (Rückseite Gleitstück)

Tagesschlüssel: W L X T B A N D O F (aus Schlüsselunterlage)

Spruchschlüssel: r n c z w y u d x e (abgeleitet)

In das Gerät einzulegen sind:

an erster Stelle Stab "W" mit der Seite, die "r" enthält,

an zweiter " " "L" " " " " "n" "

an dritter " " "X" " " " " "c" "

usw.

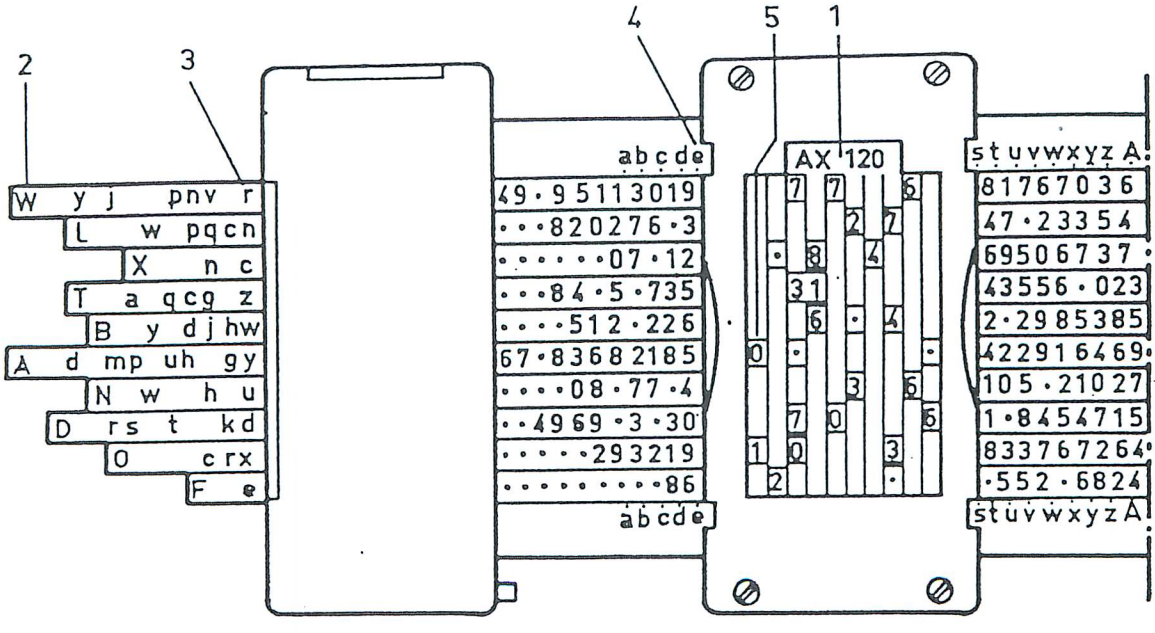
an zehnter " " "f" " " " " "e" "

a) Das gemäß vorstehendem Beispiel eingestellte RS-Gerät ist in Abbildung 5 dargestellt.

Abbildung 5

Zur Ableitung einer Schlüsselreihe eingestellter Reihenschieber

1 Dekadenschlüssel
2 Tagesschlüssel
3 Spruchschlüssel
4 Ausgangsstellung des Gleitstücks
5 Anfang der aus den Schablonenfenstern herauszulesenden Schlüsselreihe



3Ø6. Herauslesen der Schlüsselreihe aus dem RS-Gerät

a) Aus den Schablonenfenstern der Vorderseite des Gerätes am linken Rand beginnend, spaltenweise (senkrecht) die sichtbaren Ziffern herauslesen. Schablonenfenster mit einem Punkt überspringen.

Beispiel:

Der unter Ziffer 3Ø5 in Abbildung 5 dargestellte Reihenschieber zeigt folgende Schlüsselreihe:

Ø 1 2 7 3 7 Ø 8 1 6 7 Ø 2 3 4 7 4 3 6 6 6

b) Sind alle Ziffern aus der Vorderseite der Schablone herausgelesen, ohne Verschiebung des Gleitstücks die Ziffern aus der rückseitigen Schablone herauslesen.

c) Sind alle Ziffern aus der Vorder- und Rückseite herausgelesen, das Gleitstück um einen Buchstaben auf der Gleitschiene nach rechts verschieben, wobei auch das große Alphabet der Gleitschiene zu benutzen ist.

d) In dieser neuen Stellung des Gleitstücks die Ableitung der Schlüsselreihe wieder auf der Vorderseite beginnen und anschließend auf der Rückseite fortsetzen.

e) In diesem Wechsel die Ableitung der Schlüsselreihe durchführen, bis ihre Länge zur Spruchverschlüsselung ausreicht.

Beispiel:

Der gemäß dem Beispiel unter Ziffer 3Ø5 eingestellte RS liefert für den im Beispiel der Ziffer 2Ø6 angegebenen Text folgende Schlüsselreihe:

Ø 1 2 7 3 7 Ø 8 1 6 7 Ø 2 3 4 7 4 3 6 6 6 2 7 2 1 7 5 7 2 6 4 1 5 5 1 9 1 1 4 9 Ø 1 Ø 8 3

Abschnitt II - Die Ver- und Entschlüsselung

3Ø7. Die Textverschlüsselung

a) Den vorbereiteten Klartext in Fünfergruppen abteilen und, wenn erforderlich, die letzte Gruppe beliebig auffüllen.

b) Über jeden Buchstaben und über jede Ziffer der Klartextgruppen fortlaufend eine Ziffer der abgeleiteten Schlüsselreihe setzen.

Diese zugeordnete Ziffer ist jeweils die Schlüsselziffer.

c) In der Umsetztabelle die Verschlüsselung wie folgt durchführen:

(1) Den zu verschlüsselnden Buchstaben am linken Rand der Umsetztabelle "Verschlüsseln" aufsuchen.

(2) Die über dem Buchstaben stehende Schlüsselziffer am oberen Rand der Umsetztabelle aufsuchen. Die rechts neben der Schlüsselziffer stehende Ziffer weist mit einem Wert von Ø - 4 auf die linke Tabellenhälfte, von 5 - 9 auf die rechte Tabellenhälfte.
Beim Verschlüsseln des letzten Buchstabens gibt die letzte Schlüsselziffer gleichzeitig die zu benutzende Tabellenhälfte an.

(3) Im Schnittpunkt von Buchstabe und Schlüsselziffer steht der verschlüsselte Buchstabe.

(4) Sind Ziffern des Klartextes zu verschlüsseln, diese am rechten Rand der Umsetztabelle aufsuchen und in der gleichen Weise verschlüsseln wie Buchstaben.
Ziffern werden beim Verschlüsseln in Buchstaben umgewandelt.

Beispiel für eine Textverschlüsselung

1. Angenommener Klartext: "der feind greift seit Ø535 uhr behausen an"
2. Klartext vorbereitet nach Ziffer 2Ø6: "der feind greift seit q Ø535 q Ø535 q uhr y behausen y an"
3. Vorbereiteter Klartext in Fünfergruppen abgeteilt und aufgefüllt gemäß Ziffer 3Ø7. a):
"derfe indgr eifts eitqØ 535qØ 535qu hrybe hause nyanx"

4. Gemäß Ziffer 306 abgeleitete Schlüsselreihe über den Text gesetzt:

ø 1 2 7 3 7 ø 8 1 6 7 ø 2 3 4 7 4 3 6 6 6 2 7 2 1 7 5 7 2 6 4 1 5 5 1 9 1 1 4 9 ø 1 ø 8 3
d e r f e i n d g r e i f t s e i t q ø 5 3 5 q ø 5 3 5 q u h r y b e h a u s e n y a n x

5. Verschlüsselung der einzelnen Zeichen:

Zeichen des vorbereiteten Klartextes	Schlüsselziffer	rechte Ziffer neben der Schlüsselziffer weist auf Umsetztabellenhälfte		Schlüsselergebnis (= verschlüsselter Text)
		links	rechts	
d	ø	1		w
e	1	2		m
r	2		7	i
f	7	3		y
e	3		7	j
i	7	ø		l
n	ø		8	z
d	8	1		p
g	1		6	o
r	6		7	l
e	7	ø		i
i	ø	2		o
f	2	3		v
t	3	4		e
s	4		7	j
e	7	4		i
i	4	3		y
t	3		6	n
q	6		6	z
ø	6		6	y
5	6	2		a
3	2		7	g
5	7	2		y
q	2	1		e
ø	1		7	p
5	7		5	d
3	5		7	i
5	7	2		y
q	2		6	v
u	6	4		w
h	4	1		r
r	1		5	d
y	5		5	r
b	5	1		t
e	1		9	a
h	9	1		z
a	1	1		g
u	1	4		c
s	4		9	j
e	9	ø		t
n	ø	1		r
y	1	ø		t
a	ø		8	e
n	8	3		v
x	3	3		y

6. Verschlüsselter Text mit eingesetzter Bereichskenngruppe:

mwlkw wmiyj lzpol iovej iynzy agyep diyvw rdrta zgcjt rtevy mwlkw

3Ø8. Die Entschlüsselung

a) Die erste und letzte Gruppe des Spruches zeigen als Bereichskenngruppe die Schlüsselbereichszahl (= benutzten Schlüssel) an und bleiben bei der Entschlüsselung der Textgruppen unberücksichtigt.

b) Aus der Bereichskenngruppe und der Spruchschlüsselzahl den Spruchschlüssel bilden, wie in Ziffer 1Ø4. b) (2) beschrieben.

Da der Spruchschlüssel beim Verschlüsseln und Entschlüsseln in der gleichen Weise gebildet wird, darf in beiden Fällen nur die Umsetztabelle "Verschlüsseln" (im Gegensatz zur Textentschlüsselung) angewandt werden.

c) Das RS-Gerät einstellen, wie in Ziffer 3Ø5 beschrieben.

d) Die Schlüsselreihe aus dem RS-Gerät herauslesen, wie in Ziffer 3Ø6 beschrieben.

e) Die aus dem RS-Gerät herausgelesene Schlüsselreihe fortlaufend über die Buchstaben des verschlüsselten Textes schreiben.

f) Anhand der Umsetztabelle "Entschlüsseln" die Entschlüsselung vornehmen.

(1) Den Buchstaben des verschlüsselten Textes am linken Tabellenrand aufsuchen.

(2) Die über dem Buchstaben stehende Schlüsselziffer am oberen Tabellenrand aufsuchen. Die rechts neben der Schlüsselziffer stehende Ziffer weist mit einem Wert von Ø - 4 auf die linke Tabellenhälfte, von 5 - 9 auf die rechte Tabellenhälfte. Beim Entschlüsseln des letzten Buchstabens gibt die letzte Schlüsselziffer gleichzeitig an, welche Tabellenhälfte zu benutzen ist.

(3) Im Schnittpunkt von Buchstabe und Schlüsselziffer steht der Klarbuchstabe.

(4) Erscheint bei der Entschlüsselung der Buchstabe "q" im Klartext, so folgen dahinter Zahlen in Ziffern, bis ein nochmaliges "q" das Ende der Zahl und folgend die Wiederholung der Zahl anzeigt. Der Übergang von Ziffern auf Buchstaben wird am Schluß der wiederholten Zahl durch "q" angezeigt.

(5) Bei der Entschlüsselung einer Ziffer gibt die Tabelle zunächst einen Buchstaben an, der dann am linken Tabellenrand aufgesucht, auf der gleichen Zeile am rechten Tabellenrand die Ziffer angibt.

(6) In dem entschlüsselten Spruchtext die nach Ziffer 2Ø6 zur Verschlüsselung erforderlich gewesenen Hilfszeichen streichen und die Worttrennungen vornehmen. Damit ist der ursprüngliche Klartext wiedergegeben.

Beispiel für die Entschlüsselung eines Spruches

a) Vorbereitung: (1) Ableitung des Spruchschlüssels gemäß Ziffer 1Ø4. b) (2)

(2) Einstellung des RS-Gerätes " " 3Ø5

(3) Ableitung der Schlüsselreihe " " 3Ø6

(4) Über die Buchstaben der Textgruppen (außer erster und letzter Gruppe = Bereichskenngruppe) die Ziffern der Schlüsselreihe fortlaufend schreiben:

Schlüsselreihe:	Ø1273	7Ø816	7Ø234	74366	62721	75726	41551	91149	Ø1Ø83
Textgruppen:	wmiyj	lzpol	iovej	iynzy	agyep	diyvw	rdrta	zgcjt	rtevy

b) Entschlüsselung in der Umsetztabelle "Entschlüsseln" durchführen.

(1) Entschlüsselung der einzelnen Buchstaben:

Buchstaben des verschlüsselten Textes	Schlüsselziffer	rechte Ziffer neben der Schlüsselziffer weist auf Umsetztabellenhälfte		Ergebnis der Entschlüsselung (= Klartext)
		links	rechts	
w	Ø	1		d
m	1	2		e
i	2		7	r
y	7	3		f
j	3		7	e
l	7	Ø		i
z	Ø		8	n
p	8	1		d
o	1		6	g
l	6		7	r
i	7	Ø		e
o	Ø	2		i
v	2	3		f
e	3	4		t
j	4		7	s
i	7	4		e
y	4	3		i
n	3		6	t
z	6		6	q
y	6		6	Ø
a	6	2		5
g	2		7	3
y	7	2		5
e	2	1		q
p	1		7	Ø
d	7		5	5
i	5		7	3
y	7	2		5
v	2		6	q
w	6	4		u
r	4	1		h
d	1		5	r
r	5		5	y
t	5	1		b
a	1		9	e
z	9	1		h
g	1	1		a
c	1	4		u
j	4		9	s
t	9	Ø		e
r	Ø	1		n
t	1	Ø		y
e	Ø		8	a
v	8	3		n
y	3	3		x

(2) Entschlüsselter Text: derfeindgreiftseitqØ535qØ535quhrybehausenyanx

(3) Entschlüsselten Text in ursprünglichen Klartext umwandeln, d.h. alle Hilfszeichen streichen und Worttrennungen vornehmen.

Klartext: "Der Feind greift seit Ø535 Uhr Behausen an."

Anlage 1

Schlüsselbereich: ...

Muster der Schlüsselunterlagen

Tag	Dekade	Dekadenschlüssel xx)	Tagesschlüssel	Spruchschlüsselzahl
31	III.	AX 12Ø / AX 121	P C T R O M F A H Q	2 3 9 5 6 4 7 1 8 Ø
3Ø	III.	AX 12Ø / AX 121	J G Z K B I E W L Y	4 1 5 7 9 2 Ø 3 8 6
29	III.	AX 12Ø / AX 121	C D U P G J X W R I	9 1 3 4 7 5 2 6 8 Ø
28	III.	AX 12Ø / AX 121	O Y N K F B S H A V	8 7 9 3 5 Ø 1 6 2 5
27	III.	AX 12Ø / AX 121	A R W G E I J Y V N	7 5 1 3 Ø 8 4 2 6 9
26	III.	AX 12Ø / AX 121	U S Q Z D L O X K C	3 2 5 8 4 9 6 1 7 Ø
x) 25	III.	AX 12Ø / AX 121	W L X T B A N D O F	3 1 4 8 4 8 5 1 Ø 4
24	III.	AX 12Ø / AX 121	L C Z A D B N Y P R	4 6 8 2 3 7 9 5 Ø 1
23	III.	AX 12Ø / AX 121	W K L O N P E B T R	Ø 7 8 9 1 4 2 6 5 3
22	III.	AX 12Ø / AX 121	U G Q I Y M F C A D	1 3 2 4 6 9 8 Ø 7 5
21	III.	AX 12Ø / AX 121	W H G V U E D A Q F	6 9 5 3 7 2 4 8 1 Ø
2Ø	II.	AX 122 / AX 123	J O T S I X Y R L N	9 3 4 7 Ø 5 6 2 1 8
19	II.	AX 122 / AX 123	J W K E A V X T D Z	6 7 8 2 9 1 5 3 Ø 4
18	II.	AX 122 / AX 123	S L H M U Y C R F O	9 3 4 Ø 2 8 5 6 1 7
17	II.	AX 122 / AX 123	O Y Q K R V J P N B	4 1 Ø 3 5 7 6 2 9 8
16	II.	AX 122 / AX 123	E U H S D G M T L W	8 7 5 Ø 3 4 6 2 1 9
15	II.	AX 122 / AX 123	K X T R H U J Z I B	8 3 7 9 3 4 1 5 Ø 6
14	II.	AX 122 / AX 123	C W E G Q S M L N D	7 8 2 1 4 3 Ø 5 6 9
13	II.	AX 122 / AX 123	L R S F K O T C Y B	3 8 2 5 6 Ø 9 4 1 7
12	II.	AX 122 / AX 123	G J U H A I E X M Z	9 8 1 2 Ø 7 5 6 4 3
11	II.	AX 122 / AX 123	V Q E U Y L Z M I S	9 7 3 Ø 8 4 1 5 2 6
1Ø	I.	AX 124 / AX 125	X N F B W K T C O R	4 8 3 2 6 7 Ø 1 5 9
9	I.	AX 124 / AX 125	C X G I K P O H N S	4 5 1 9 Ø 2 3 6 8 7
8	I.	AX 124 / AX 125	M B W Q U T F E V Z	6 Ø 1 4 3 9 2 8 5 7
7	I.	AX 124 / AX 125	V T E Q B A O N F J	7 6 Ø 1 9 2 5 3 4 1
6	I.	AX 124 / AX 125	M C I L H Z G S U Y	2 7 6 4 9 3 1 8 5 Ø
5	I.	AX 124 / AX 125	B D W L K T R S Y G	2 Ø 1 6 8 5 3 4 9 7
4	I.	AX 124 / AX 125	M F U A H P O V N X	1 7 Ø 8 4 5 3 9 6 2
3	I.	AX 124 / AX 125	H W Y D V F C P N K	Ø 4 5 8 9 3 7 2 1 6
2	I.	AX 124 / AX 125	T M U L B G I Y A Z	9 8 6 7 1 Ø 2 5 3 4
1	I.	AX 124 / AX 125	C G V Q L Z S A U P	9 5 2 7 4 3 Ø 8 1 6

x) Anmerkung: Für alle Beispiele in dieser Vorschrift sind die für den 25. Tag vorgeschriebenen Schlüsselangaben benutzt.

xx) Erste Schablone AX 12Ø für Vorderseite des Gleitstücks
Zweite " AX 121 " Rückseite " "

Anlage 2 a

Muster der Umsetztabelle

Schlüsselbereich ...

Ø - 4

	Ø	1	2	3	4	5	6	7	8	9	
a	i	g	o	l	n	q	x	a	s	u	Ø
b	e	j	u	c	s	t	i	k	x	f	1
c	s	k	a	v	f	d	h	q	e	l	2
d	w	y	l	z	m	x	t	s	p	c	3
e	c	m	g	p	z	b	v	i	r	t	4
f	n	r	v	i	q	w	a	y	h	b	5
g	b	q	h	k	d	n	j	r	f	g	6
h	g	l	j	u	r	f	o	e	q	z	7
i	o	e	c	h	y	z	m	l	w	i	8
j	h	p	i	s	o	v	e	w	d	y	9
k	x	s	t	d	a	p	q	b	z	e	Ø
l	l	d	k	g	j	r	n	m	t	q	1
m	a	f	m	r	u	g	k	p	c	h	2
n	r	x	p	w	b	j	f	h	v	m	3
o	y	w	z	x	i	s	r	u	a	p	4
p	u	b	q	j	l	e	z	o	n	d	5
q	d	o	e	n	x	i	b	t	l	w	6
r	q	a	w	m	t	h	s	c	g	n	7
s	f	h	x	q	g	k	l	v	y	r	8
t	p	z	s	e	h	y	u	f	m	o	9
u	z	c	b	o	p	a	w	d	j	s	Ø
v	j	u	n	t	v	l	g	z	k	x	1
w	t	n	y	a	e	u	c	j	o	v	2
x	m	v	r	y	c	o	d	n	b	k	3
y	k	t	d	f	w	m	y	x	i	a	4
z	v	i	f	b	k	c	p	g	u	j	5

5 - 9

	Ø	1	2	3	4	5	6	7	8	9	
a	e	p	m	c	v	h	y	r	w	b	Ø
b	h	b	z	o	d	q	p	a	l	w	1
c	n	r	j	w	y	m	g	z	u	x	2
d	u	v	g	d	f	i	e	k	b	j	3
e	y	a	n	j	x	s	q	o	h	l	4
f	j	k	p	g	o	l	f	d	t	e	5
g	l	o	e	t	s	a	u	m	v	e	6
h	d	m	c	s	k	n	b	w	p	y	7
i	s	g	u	v	p	f	r	j	d	a	8
j	x	n	b	a	q	u	t	g	z	f	9
k	o	h	r	y	m	j	k	l	c	n	Ø
l	a	x	f	z	c	v	o	u	s	p	1
m	i	l	s	e	n	b	j	q	y	d	2
n	z	u	k	l	g	o	a	i	e	t	3
o	v	e	o	b	h	t	d	f	n	m	4
p	r	c	x	m	t	w	i	p	g	v	5
q	m	s	v	k	u	c	z	y	f	h	6
r	k	d	i	f	b	x	l	v	o	r	7
s	t	w	a	u	j	p	s	n	m	o	8
t	c	j	q	n	r	d	w	b	k	i	9
u	q	y	h	i	e	k	v	t	x	u	Ø
v	p	i	w	q	a	y	h	c	r	s	1
w	g	f	d	x	w	z	m	h	i	k	2
x	f	z	t	h	i	g	x	s	a	q	3
y	b	q	l	p	z	r	c	e	j	g	4
z	w	t	y	r	l	e	n	x	q	z	5

Verschlüsseln

Anlage 2 b

Ø - 4

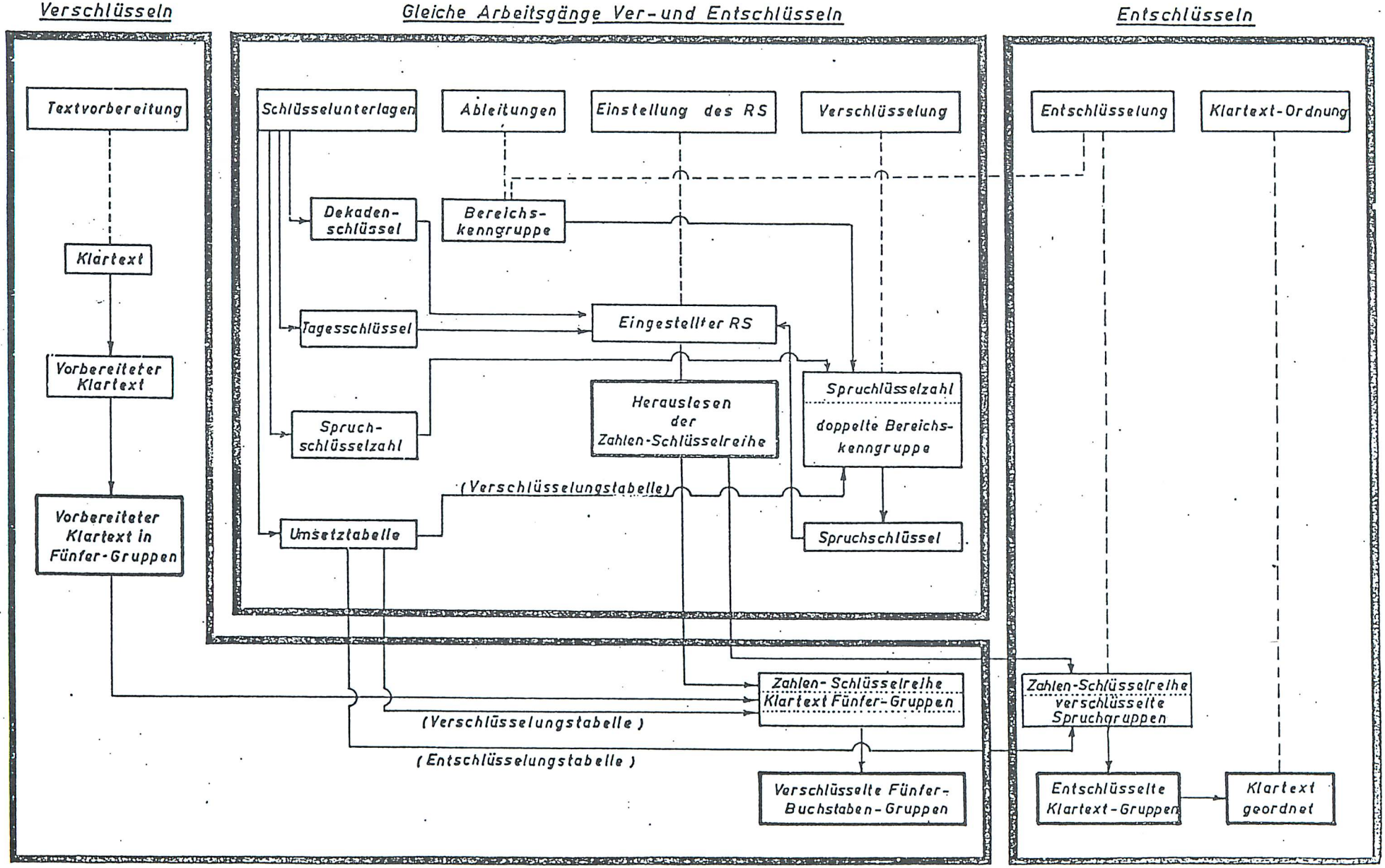
	Ø	1	2	3	4	5	6	7	8	9	
a	m	r	c	w	k	u	f	a	o	y	Ø
b	g	p	u	z	n	e	q	k	x	f	1
c	e	u	i	b	x	z	w	r	m	d	2
d	q	l	y	k	g	c	x	u	j	p	3
e	b	i	q	t	w	p	j	h	c	k	4
f	s	m	z	y	c	h	n	t	g	b	5
g	h	a	e	l	s	m	v	z	r	g	6
h	j	s	g	i	t	r	c	n	f	m	7
i	a	z	j	f	o	q	b	e	y	i	8
j	v	b	h	p	l	n	g	w	u	z	9
k	y	c	l	g	z	s	m	b	v	x	Ø
l	l	h	d	a	p	v	s	i	q	c	1
m	x	e	m	r	d	y	i	l	t	n	2
n	f	w	v	q	a	g	l	x	p	r	3
o	i	q	a	u	j	x	h	p	w	t	4
p	t	j	n	e	u	k	z	m	d	o	5
q	r	g	p	s	f	a	k	c	h	l	6
r	n	f	x	m	h	l	o	g	e	s	7
s	c	k	t	j	b	o	r	d	a	u	8
t	w	y	k	v	r	b	d	q	l	e	9
u	p	v	b	h	m	w	t	o	z	a	Ø
v	z	x	f	c	v	j	e	s	n	w	1
w	d	o	r	n	y	f	u	j	i	q	2
x	k	n	s	o	q	d	a	y	b	v	3
y	o	d	w	x	i	t	y	f	s	j	4
z	u	t	o	d	e	i	p	v	k	h	5

5 - 9

	Ø	1	2	3	4	5	6	7	8	9	
a	l	e	s	j	v	g	n	b	x	i	Ø
b	y	b	j	o	r	m	h	t	d	a	1
c	t	p	h	a	l	q	y	v	k	g	2
d	h	r	w	d	b	t	o	f	i	m	3
e	a	o	g	m	u	z	d	y	n	f	4
f	x	w	l	r	d	i	f	o	q	j	5
g	w	i	d	f	n	x	c	j	p	y	6
h	b	k	u	x	o	a	v	w	e	q	7
i	m	v	r	u	x	d	p	n	w	t	8
j	f	t	c	e	s	k	m	i	y	d	9
k	r	f	n	q	h	u	k	d	t	w	Ø
l	g	m	y	n	z	f	r	k	b	e	1
m	q	h	a	p	k	c	w	g	s	o	2
n	c	j	e	t	m	h	z	s	o	k	3
o	k	g	o	b	f	n	l	e	r	s	4
p	v	a	f	y	i	s	b	p	h	l	5
q	u	y	t	v	j	b	e	m	z	x	6
r	p	c	k	z	t	y	i	a	v	r	7
s	i	q	m	h	g	e	s	x	l	v	8
t	s	z	x	g	p	o	j	u	f	n	9
u	d	n	i	s	q	j	g	l	c	u	Ø
v	o	d	q	i	a	l	u	r	g	p	1
w	z	s	v	c	w	p	t	h	a	b	2
x	j	l	p	w	e	r	x	z	u	c	3
y	e	u	z	k	c	v	a	q	m	h	4
z	n	x	b	l	y	w	q	c	j	z	5

Entschlüsseln

Schematische Darstellung der Schlüsselvorgänge



Anlage 3