



Top Secret –Top Secret



Arbeitshilfe

Codierung/Dekodierung mittels

U L T R A – C o d e

Dieses Dokument darf nicht in fremde Hände fallen!

A 1 Verteilen von Kryptomitteln gemäß Weisung der Kryptobereichsleitstelle.

A 2 Durchführen der Authentisierung mit NATO Schlüsselunterlagen.

Top Secret –Top Secret

- **1. Manuelles Verfahren**

1. Die Beschreibung stellt nur prinzipiell dar, wie manuell chiffriert wurde. Es ist in englischer Sprache und mit Codebüchern gearbeitet worden.
2. Das Verfahren beruht auf folgenden System:
 - Wandlung des Klartextes durch Substitution in Zahlenkolonnen
 - chiffrieren dieser mit Chiffriertabellen die aus dem Handbuch "Statistisches Jahrbuch des Deutschen Reiches" gebildet wurden

1a. Die Substitutionstabelle:

Kennwort	S	U	B	W	A	Y
Substitut	0	82	87	91	5	97
Klartext	C	D	E	F	G	H
Substitut	80	83	3	92	95	98
Klartext	I	J	K	L	M	N
Substitut	1	84	88	93	96	7
Klartext	O	P	Q	R	T	V
Substitut	2	85	89	4	6	99
Klartext	X	Z	•	/		
Substitut	81	86	90	94		

	0	1	2	3	4	5	6	7	8	9
	s	i	o	e	r	a	t	n		
8	c	x	u	d	j	p	z	b	k	q
9	•	w	f	l	/	g	m	y	h	v

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	•	/
5	87	80	83	3	92	95	98	1	84	88	93	96	7	2	85	89	4	0	6	82	99	91	81	97	86	90	94

1b. Die Klartextbearbeitung

DAL ("Dalny Wostok" = Ferner Osten Absender-Ort)

DER SOWJETISCHE FERNE OSTEN KANN ALS SICHER VOR EINEM ANGRIFF JAPANS ERACHTET WERDEN

(die Information)

RAMSAY

1c. ausgeführte Substitution:

DAL .DE R/SO WJE TISC HE/ FERN E/OS TEN/ KANN /AL S/SI CHE R/V OR/E INEM /ANG RIF F/J APA NS/E RACH TET/ WER DEN. RAM SAY •
83593 90833 49402 91843 61080 98394 92347 39420 63794 88577 94593 09401 80983 49499 24943 17396 94579 54192 92948 45855 70943 45809 86369 49134 83379 04596 05979 0

zu beachten: bei Überstand der 5er Gruppen wurden diese weggelassen oder aufgefüllt!

Hier wurde die 0 weggelassen!

1d. aussuchen der Schlüsselgruppen aus dem Handbuch:

Seite 193 Zeile 7 Spalte 5 ist der Beginn (19375)

1.e Addition OHNE übertrag des Substitut mit dem Schlüssel:

8359	9083	4940	91843	6108	9839	9234	3942	6379	8857	9459	0940	8098	4949	2494	1739	9457	5419	9294	4585	7094	4580	8636	4913	83379	0459	0597
3	3	2		0	4	7	0	4	7	3	1	3	9	3	6	9	2	8	5	3	9	9	4	6	9	
3563	5130	2493	10010	7819	1210	2116	4186	7614	1058	6698	8524	5039	0147	0333	9192	5662	0180	1511	8411	1386	8631	0915	6521	43724	4383	9272
5	3	2		1	6	9	1	7	9	4	9	7	1	0	9	2	6	2	2	5	8	0	3	9	7	
1812	4113	6333	01853	3917	0049	1340	7028	3983	9805	5347	8464	3027	4086	2727	0821	4019	5599	0705	2996	8370	2111	8541	0434	26093	2609	9769
8	6	4		1	0	6	1	1	6	7	0	0	0	3	5	1	8	0	7	8	7	9	7	3	6	

4.
Grupp

3
letzte

1f. Übermittlung der Angaben zum Schlüssel (1d.)

4. Gruppe:	01853
3. letzte Gruppe:	+ 26093
Seite/Zeile/Spalte:	<u>+ 19375</u>
Schlüsselgruppe =	36111

Die Schlüsselgruppe wird immer am Anfang des Spruches gesetzt!

2. Die manuelle Chiffrierverfahren z. B. der chemischen Aufklärung, Politabteilung, (KOBRA, PYTHON)

Die Verwendung von KOBRA ist in der [DV A 040/1/312](#) geregelt.

Allgemeine Grundsätze der Ziffernadditionsverfahren sind in der vom ZCO festgelegten Normen und weiteren Varianten wie KOBRA, PYTHON oder Code 50010 festgelegt.

Grundsätze der Codier- und Verschleierungsverfahren in der [DV 040/0/010](#) und in der [DV 040/0/014](#).

Vorlagen ([Formblatt 44444](#)) sind zur Vereinfachung und extremen Verkürzung von Meldungen der Kern-, chemischen und bakteriologischen Aufklärung (KCB-Aufklärung).

Bereits 1980 wurde es als [einheitliches Verfahren](#) für alle Einrichtungen die KCB Aufklärung verwendet, wie NVA, MfS, Zivilverteidigung, MdI und Kampftruppen.

Details sind zu finden in den Kurz- und Dienstvorschrift [KOBRA](#), den [Additionsverfahren](#) und [PYTHON](#).

Die Dienstvorschrift des [MfS](#) entspricht der Dienstvorschrift der [NVA](#) sowie der [DV A 040/1/312](#).

Die [Abbildungen](#) entstammen den der Handbüchern KOBRA der NVA. Sammler*16

In den zahlreichen manuellen Chiffrierverfahren gibt es Unterschiede in der Bildung der Kenngruppen.

3. Die Substitutionstabellen

3.1. TAPIR

Die Substitutionstabelle TAPIR wird genutzt bei der manuellen Chiffrierung im [Ziffernadditionsverfahren](#).

Z. B. bei den Chiffrierverfahren [KOBRA](#) und [PYTHON](#).

TAPIR wurde in fast allen Chiffrierstellen genutzt, außer bei den [Grenztruppen](#).

Programm: TAPIR Umsetzung für Windows per [Download](#)

[Original](#) TAPIR Dokument^{Sammler*15}Rückseite [TAPIR](#)

Abb.: TAPIR, Verwendung z.B in der NVA

A 0	E 1	I 2	N 3	R 4	TAPIR VVS-Ex. 03086				
B 50	BE 51	C 52	CH 53	D 54	DE 55	F 56	G 57	GE 58	H 59
J 60	K 61	L 62	M 63	O 64	65	66	P 67	Q 68	S 69
T 70	TE 71	U 72	UN 73	V 74	75	76	W 77	X 78	Y 79
WR 80	Bu 81	Zi 82	ZwR 83	Code 84	RPT 85	86	87	88	• 89
: 90	, 91	- 92	/ 93	(94) 95	+ 96	= 97	" 98	99
0 00	1 11	2 22	3 33	4 44	5 55	6 66	7 77	8 88	9 99

Abb.: TAPIR, Verwendung in der HA VII/3, ^{BStU*286}

A 0	E 1	I 2	N 3	R 4	TAPIR VVS-Ex. xxxxx				
B 50	BE 51	C 52	CH 53	D 54	DE 55	F 56	G 57	GE 58	H 59
J 60	K 61	L 62	M 63	O 64	ß 65	Ä 66	P 67	Q 68	S 69

T 70	TE 71	U 72	UN 73	V 74	unv. 75	W 76	X 77	Y 78	Z 79
wiedh. 80	Bu 81	Zi 82	ZwR 83	Code 84	DDR 85	BRD 86	WB 87	Ö 88	• 89
: 90	, 91	- 92	/ 93	(94) 95	+ 96	= 97	" 98	Ü 99
0 00	1 11	2 22	3 33	4 44	5 55	6 66	7 77	8 88	9 99

Als erstes erfolgt die Umwandlung des Klartextes in den Zifferntext:

[\(Formular NVA 40 652 Ag 117/I/2 3411-6\)](#)

Vereinfachung langer Texte erfolgt mittels eines [Codebuches](#) Sammler*16

UEB SNV

WOSTOK 944

UEBUNGSSPRUCH 12

DAS WETTER UM.

SOROKA 944

UEB	SNV	WO-	STO	Kzi-	944	buU E	BU N	GSS	PRU -	CHzi -	12-	buD A-	SWE -	TTE R	UM-	SOR -	OK A-	zi94	4__
7215 0	6937 4	7664 6	9706 4	6182 9	9444 4	8172 1	5073 5	7696 9	6747 2	5382 1	1122 8	1540 6	9761 7	0701 4	7263 6	9644 6	4610 8	2994 4	4483 8

Die letzte 5er Gruppe muß aufgefüllt werden. Das Verwendete Auffüllzeichen ist gesondert festgelegt. In diesem Beispiel 83.

Jetzt werden die 5er Gruppen mit dem Schlüssel aus dem Schlüsselheft der jeweiligen Verbindung verschlüsselt.

50482 84817 13460 72551 31005 37283 93086 67829 74134 88460
 26821 75102 15599 43236 85304 04150 91357 21028 99218 88375
 15100 19916 53492 59234 47600 40268 84615 16975 62516 79852
 53367 29076 97504 08467 31270 30476 63139 66483 38534 41724
 33465 19406 19442 89014 20932 42923 61808 02250 44866 27503
 06099 46262 86741 56555 92085 43097 25198 98430 73370 30412
 70847 70490 32795 12041 61227 26896 11794 40937 13766 47818
 70757 06030 52177 84711 62108 68330 75852 93244 29499 82430
 73924 05193 72608 93583 83220 26608 80436 32210 94755 73740
 16385 0 0

Die Zifferngruppen werden ohne Übertrag addiert.

UEB	SNV	WO-	STO	Kzi-	944	buU E	BU N	GSS	PRU -	CHzi -	12-	buD A-	SWE -	TTE R	UM-	SOR -	OK A-	zi94	4_
7215 0	6937 4	7664 6	9706 4	6182 9	9444 4	8172 1	5073 5	7696 9	6747 2	5382 1	1122 8	1540 6	9761 7	0701 4	7263 6	9644 6	4610 8	2994 4	4483 8
5048 2	8481 7	1346 0	7255 1	3100 5	3728 3	9308 6	6782 9	7413 4	8846 0	2682 1	7510 2	1559 9	4323 6	8530 4	0415 0	9135 7	2102 8	9921 8	8837 5

2253	4318	8900	6921	9282	2162	7470	1745	4009	4583	7964	8632	2099	3084	8231	7678	8779	6712	1815	2210
2	1	6	5	4	7	7	4	3	2	2	0	5	3	8	6	3	6	2	3

Jetzt wird dem Spruch nur noch die Verbindungsnummer/Schlüsselheftnummer und die gültige Schlüsselgruppe angehängt.

Bsp.: Verbindungsnummer 50001-39082

Schlüsselheftnummer 18732

der Verwendete Schlüssel aus dem Schlüsselheft mit dem Code: 16385

Da die Schlüssel immer Verbindungsorientiert sind, muß trotzdem das Heft und die Seite aus dem Heft angeben da sonst nicht erkennbar ist ob der Teilnehmer nicht schon 2 Seiten weiter ist, oder ein neues Schlüsselheft benutzt (Kompromittierung etc.). Dafür kann die Verbindungsnummer entfallen (Bsp-2).

Der Spruch der gesendet wird könnte so aussehen:

Bsp1.: 39082 18732 16385 22532 43181 16385 00022

Bsp2.: 18732 16385 22532 43181 16385 00021

Die letzten zwei Gruppen ergeben sich aus Schlüsselheft Nr. und der Gruppenanzahl des Spruches

Bsp1.: 00022

Bsp2.: 00021

Oder auch aus dem Datum und der Gruppenanzahl des Spruches

Bsp1.: 29025

Bsp2.: 29024

Ein vereinfachtes Verfahren wurde in der HA VII benutzt: BStU^{[*286](#)}
Wurmtabellenheft Typ 350:

34534 74078 49774 28162 95091 74305 51814 43321

37765 76588 51395 18093 80550 59005 37922 03501

71249 83986 31363 54842 03475 06022 49936 44305

55724 43830 00130 83462 84775 00823 42479 56844

44021 51838 16947 45921 69525 29310 63334 72887

25149 46123 52011 02660 66528 43837 40181 48031

65652 91631 16309 03423 01467 10484 75054 81790

Abb.: Type 350, Wurmtabellenheft BStU^{*286}

Die erste und letzte Gruppe der Wurmtabellenzeile ist die Kenngruppe:

34534 33037 12219 50627 59205 28518 10613 52265 36751 34534

gefolgt vom chiffrierten Text. Ohne weitere Angaben wie Datum, Länge, Empfänger, Absender oder Verbindung bzw. Teilnehmer. Es handelt sich um eine reine individuelle Chiffrierverbindung.

3.2.Aufbau der Tarntafel ASTRA/ASTER. BStU ^{*215}

ASTRA

Tajne 480/57

ASTER

Instrukcja

Egz. pojedynczy 1

posługiwania się tablicą sygnałową "DP - 1"

I. Przeznaczenie tablicy sygnałowej i jej budowa

Niniejsza tablica sygnałowa przeznaczona jest dla sieci współdziałania i służy do kodowania danych przekazywanych między morską Policją Graniczną Niemieckiej Republiki Demokratycznej a jednostkami morskimi Wojsk Chrony Pogranicza Polskiej Rzeczypospolitej Ludowej. Terminologia tablicy, po wyrażeniu obustronnej zgody, wydrukowana została w językach polskim i niemieckim. Poszczególne wielkości są jednakowej treści w obydwu językach.

Całość dokumentu składa się z dwóch tablic. Pierwsza tablica, posiadająca część specjalną i alfabetyczny układ terminologii służy do kodowania, natomiast druga tablica z wpisanym w kolejności oznaczeniem przeznaczona jest do rozkadowania.

Część specjalna zawiera cyfry, znaki pisarskie, sygnały, alfabet polsko-niemiecki i alfabet roszyjski.

W części alfabetycznej znajdują się pojedyncze wyrazy i zdania najczęściej używane w wspomnianej wyżej sieci.

Terminologia ułożona jest w porządku alfabetycznym umożliwiającym szybkie wyszukanie potrzebnej wielkości.

Zarówno w części specjalnej jak i w części alfabetycznej znajduje się odpowiednia ilość wolnych miejsc przeznaczonych dla wpisania brakującej terminologii. Wpisanie do tablicy brakujących wielkości może nastąpić po otrzymaniu w tej sprawie zgody drugiej strony. Przy występowaniu z tego rodzaju propozycjami należy każdorazowo dokładnie określić miejsce, w którym ma być wpisana proponowana wielkość z jednoczesnym podaniem daty i godziny wprowadzenia w życie

dodatkowo ustalonej terminologii.

Każda wielkość kodowa znajdująca się zarówno w części specjalnej jak i alfabetycznej posiada trzycyfrowe oznaczenie. Również miejsca wolne posiadają odpowiednie oznaczenie, nie powtarzające się w całości tablicy.

II. Kodowanie

Tekst przeznaczony do kodowania winien zawierać wyrazy i zdania zawarte w tablicy, mając jednak na uwadze, by kodowany tekst nie uległ zniekształceniu.

Każda wielkość kodowana jest przy użyciu całego trzycyfrowego oznaczenia znajdującego się po lewej stronie danej wielkości. Wpisując oznaczenia na blankiet radigramu należy tworzyć grupy trzycyfrowe umożliwiające - w razie potrzeby - szybkie sprawdzenie zakodowanego tekstu.

Podczas kodowania obowiązują następujące zasady:

1. kodowanie wyrazów i zdań nieznajdujących się w tablicy dozwolone jest jedynie w wyjątkowych wypadkach. Wówczas należy użyć zarówno przed jak i po podaniu brakującego tekstu sygnału "sylabozwany tekst niemiecki początek/koniec" lub "sylabizowany tekst polski/początek/koniec". Jeden lub drugi sygnał przekazujemy w zależności od języka, w jakim przekazujemy brakujące wyrazy lub zdania.
Przekanie tekstu nieznajdującego się w tablicy może mieć miejsce pod warunkiem, że osoba nadająca tego rodzaju tekst zna w dostatecznym stopniu język adresta, lub jeśli osoba ta jest w stanie wspomniany tekst przetłumaczyć przy użyciu słownika.
2. Tekst winien być zakodowany całkowicie. Stosowanie tekstu mieszanego, to znaczy częściowo zakodowanego a częściowo odkrytego jest niedozwolone.
Wielkości, których nie ma w tablicy, nie wolno do tekstu dodawać.
3. Znajdujące się w tablicy wielkości dot. rzeczowników użytych w liczbie pojedynczej odnoszą się również do odpowiednich rzeczowników liczby mnogiej. W przypadku, gdy z tekstu nie wynika czy dana wielkość oznacza liczbę mnogą, wówczas należy podać

sygnał "poprzednia prupa liczba mnoga".

Przykład:

T e k s t o d k r y t y : Idziemy w kierunku

T e k s t z a k r y t y : Ide w kierunku, sygnał: "poprzedina prupa
liczba mnoga"
(142 700)

4. Przy kodowaniu wielkości wymagających uzupełnienia odpowiednimi dynamami, należy przestrzegać taką kolejność uzupełnienia, jaka wynika z odnośnej wielkości tablicy.

Przykład:

T e k s t o d k r y t y : Pozycja i kurs naszej jednostki: szer.geogr.
54 stopni, 17 minut, dlug.geogr.15 stopni,
6 minut kurs 180 stopni.

T e k s t z a k r y t y : Pozycja i kurs naszej jednostki: szer.geogr.
. dlug.geogr.
kurs 54 17 15 6 180
(733 524 703 263 582 095 656)

Przy podawaniu współrzędnych z mapy należy posługiwać się właściwymi oznaczeniami określającymi szerokość i długość geograficzną (w stopniach i minutach).

5. Wszystkie dane cyfrowe koduje się przy użyciu tablicy, wielkości cyfrowe o różnym znaczeniu należy kodować oddzielnie np: godziny podaje się w jednej grupie, minuty w drugiej grupie itd.

Przykład: 1

T e k s t o d k r y t y : Dnia 27.03.1957 r.

T e k s t z a k r y t y : Dnia 27 03 57 (605 629 656 416 989)

Przykład: 2

T e k s t o d k r y t y : Godzina 3.30

T e k s t z a k r y t y : Godzina 03 30 (511 656 416 839)

Każdy kodowany tekst musi być powtórnie zaopatrzony kluczem.

Kodowany teks nie zaopatrzony kluczen posyłać jest niedozwolone.

Uwagi:

- Wszelkie uwagi i propozycje odnosace się do tablicy sygnałowej winny być zgłaszane do vetralnego organu szyfrowego włącznie,
- jeden egzemplarz nieniejszeji instrukcj, winien znadować się w każdym punkcie kodowym i prechowywany w opieczętowanej kopercie pod zamknięciem,
- czasokres używalności danej tablicy sygnałowej, wszelkie wnioski i uwagi dotyczacej zarowno samej tablicy jak i spraw odnoszacych się do sieci współdziałania w ogole, winny być uzgadniane w trybie roboczym miedzy obu stronami za pośrednictwem centralnych organów szyfrowych NRD i PRL.

CZĘŚĆ DLA KODOWANIA

CODIERTEIL

CZĘŚĆ SPECJALNA

SONDERTEIL

**Cyfry
Ziffern**

**Alfabet polsko-niemiecki
Deutsch-polnische Buchstabiertafel**

**Alfabet rosyjski
Rusisches Alphabet**

Znaki pisarske
Satzzeichen

Sygnaly
Indikatoren

Cyfry: **Zahlen**

080	1	1
397	2	2
416	3	3
790	4	4
852	5	5
582	6	6
917	7	7
161	8	8
657	9	9
952	10	10
212	11	11

...

656	0	0
989	00	00
466	000	000

Alfabet polsko-niemiecki **Deutsch-polnische Buchstabiertafel**

199	A	A
453	ä	ä
613	a	a
823	B	B

...

Alfabet rosyjski - Russisches Alphabet

310	A	882	K	658	X
830	Б	469	Л	577	Ц
707	В	641	М	757	Ч

...

Znaki pisarskie

Satzzeichen

349	.	(Kropka)	.	(Punkt)
919	;	(Przecinek)	,	(Komma)
673	:	(Dwukropek)	:	(Doppelpunkt)
164	?	(Znak zapytania)	?	(Fragezeichen)
076	()	(Nawias)	()	(Klammern)

Sygnaly

Indikatoren

342	Cyfry	początek / koniec	Zahl	Anfang / Ende
452	Sylabizowany tekst niemiecki	początek / koniec	Deutscher Text	buchstabiert Anfang / Ende

...

CZĘŚĆ ALFABETYCZNA

ALPHABETISCHER TEIL

280	Ahlbeck	Ahlbeck
545	Alarm	Alarm
492	Alarm zakonczony	Alarm beendet
935	Altwar	Altwar
990	A municja	Munition

...

018

STRENG GEHEIM

GVS Nr, 1244
Exempl. Nr. 202

Benutzungsanweisung

1. In die Codeunterlagen dürfen nur Personen Einblick erhalten, die ausdrücklich dazu bestimmt sind. Verlust oder Dekonspiration der Codeunterlagen ist sofort der vorgesetzten Dienststelle zu melden.

Wörter, Endungen und Satzzeichen, deren Weglassung den Sinn des Textes nicht verändern oder unverständlich machen, werden nicht mit codiert.

Als dekonspiriert gelten die Codeunterlagen, wenn irgendein Unbefugter Einblick in sie erhält oder begründeter Verdacht dafür besteht. Die Codeunterlagen werden außerhalb des Einsatzes unter Verschluss aufbewahrt.

2. Beim Codieren werden die einzelnen Phrasen durch die dreistelligen Zahlen ersetzt, die aus der zweistelligen Ziffer gebildet werden.
3. Nicht vorhandene Wörter werden aus vorhandenen Wortteilen und Buchstaben zusammengesetzt oder, wenn dadurch der Sinn nicht entstellt wird, durch andere, vorhandene Wörter ersetzt.
4. Der Nachrichtentext ist so zu formulieren, daß er den vorhandenen Phrasen so weit wie möglich angepaßt ist.

5. Das Codiersignal Mehrzahl ist nur dann zu setzen, wenn aus dem Satzzusammenhang nicht erkennbar ist, daß die Mehrzahl gesetzt werden muß.
6. Die Anschriften befinden sich auf einer Sondertafel. Beim Codieren muß vor die Anschrift immer ein Codiersignal Anschrift, welches sich in jeder Tafel im rechten unteren Eckfeld befindet, gesetzt werden. auf, muß die folgende Gruppe in der Anschriftentafel aufgesucht werden.
7. Die Anschrift muß an einer willkürlich gewählten Stelle im Telegramm versteckt werden. Die Anschrift ständig an die gleiche Stelle zu setzen, ist verboten!
8. Die Phrasentafeln werden zu bestimmten Zeitpunkten, die von der vorgesetzten Dienststelle angegeben werden ausgewechselt.

	6	5	0	1	7	9	4	3	2	8
85	Adlershof BP	Ditrichshütte GP	Fürstenberg BP	Halle TP	Löcknitz GP	Perleberg GP	Schwerin BP	Wolgast BP		
67	Alt-Reese BP	Dresden BP	Gardelegen GP		
32	AZKW	Dresden TP	Gera BP	Johannesthal TP			

Aster
Astra

GVS-Nr. 479/57
Exemplar-Nr. 1

Streng geheim!

1. In die Codeunterlagen dürfen nur die Personen Einblick erhalten, die ausdrücklich dazu bestimmt sind. **Verlust oder Dekonspiration der Codeunterlagen ist sofort der zuständigen Dienststelle zu melden.** Als dekonspiriert gelten die Codeunterlagen, wenn irgendein Unbefugter Einblick in sie erhält oder begründeter Ver-

dacht dafür besteht. Vor und nach dem unmittelbaren Gebrauch müssen die Codeunterlagen im Stahlschrank oder in der Stahlkassette unter Verschuß gehalten werden.

2. Beim **Codieren** werden die einzelnen Phrasen durch die dreistelligen Zifferngruppen (Codegruppen) ersetzt, die links von den Phrasen stehen.
3. Der Klartext ist so herzurichten, daß er den im Code enthaltenen Phrasen angepaßt ist.
4. Wörter, die im Code nicht enthalten sind, können nur in besonderen Fällen gesendet werden. Solche Wörter müssen in der Sprache des Empfängers buchstabiert werden, d. h. von deutscher Seite müßte der polnische Ausdruck für das entsprechende deutsche Wort buchstabiert und jeder Buchstabe durch die entsprechende Codegruppe ersetzt werden, von polnische Seite müßte das entsprechende deutsche Wort buchstabiert werden. Wer die Sprache des Empfängers nicht beherrscht, kann ein Wörterbuch benutzen. Vor und nach dem buchstabierten Wort ist das Codiersignal „Polnischer Text buchstabiert Anfang/Ende“ bzw. „Deutscher Text buchstabiert Anfang/Ende“ zu setzen.
5. Das Codiersignal „Mehrzahl vorige Gruppe“ ist nur dann zu verwenden, wenn aus dem Textzusammenhang nicht ersichtlich ist, daß die Mehrzahl gemeint ist.
6. Positionsangaben müssen immer in 4 Codegruppen gegeben werden: 1.Grad/Breite 2.Minuten/Breite 3.Grad/Länge 4.Minuten/Länge.
7. Jeder Klartext muß **vollständig** codiert werden. Einen Mischtext, d. h. teilweise codierten und teilweise nicht codierten Text, zu senden ist unzulässig.
8. Jeder Codetext muß überschlüsselt werden. einen nicht überschlüsselten Codetext zu senden ist unzulässig.

CODIERTEIL

CZĘŚĆ DLA KODOWANIA

...

SONDERTEIL

CZĘŚĆ SPECJALNA

Ziffern

Cyfry

Deutsch-polnische Buchstabiertafel
Alfabet polka-niemiecki

Russisches Alphabet
Alfabet rosyjski

Satzzeichen
Znaki pisarskie

Indikatoren
Sygnaly

...

ALPHABETISCHER TEIL

CZĘŚĆ ALFABETYCZNA

738	Abbrechen	Przerwać
833	Abgeschlossen	Zestrzelony
981	Ablösung/Veränderung	Zmiana

...

3.3. Substitutionstabelle ZEBRA-1 BSU [*173](#)

Die Substitutionstabelle ZEBRA-1 wurde bis ca. 1964 verwendet.
Sie dient der Umwandlung von Mischtexten in Zifferntexte.
Die Zifferntexte werden mit dem Verfahren 001 chiffriert.

A 0	E 1	I 2	N 3	ZEBRA-1 VVS-Ex. 00001					CODE 9
Ä 40	AU 41	B 42	BE 43	C 44	CH 45	D 46	DE 47	DER 48	ER 49
F 50	G 51	GE 52	H 53	J 54	K 55	L 56	M 57	O 58	Ö 59
P 60	Q 61	R 62	RE 63	S 64	SCH 65	SE 66	ST 67	SU 68	T 69

TE 70	U 71	Ü 72	UNG 73	V 74	W 75	X 76	Y 77	Z 78	ZE 79
• 80	: 81	, 82	- 83	/ 84	(85	86) 87	" 88	Zi/Bu 89
0 000	1 111	2 222	3 333	4 444	5 555	6 666	7 777	8 888	9 999

Abb.: Substitutionstafel ZEBRA-1

3.4. Substitutionstabelle 535 und manuelles Chiffrierverfahren "50010 der Grenztruppen der DDR" ^{BStU *118}

Das manuelle Chiffrierverfahren wurde 1980 in den Grenztruppen der DDR eingeführt. Es besteht aus einem Codebuch sowie einer Substitutionstafel Typ 535.

A 0	E 1	I 2	N 3	R 4	S 5	Code 535		VVS-Ex. 00944		CODE 9
B 60	C 61	D 62	F 63	G 64	H 65	J 66	K 67	L 68	M 69	
O 70	P 71	Q 72	T 73	U 74	V 75	W 76	X 77	Y 78	Z 79	
Ä 80	Ö 81	Ü 82	ß 83	() 84	: 85	/ 86	• 87	, 88	- 89	

Abb.: Substitutionstafel 535

Die Klartexte sind mittels des Codebuches in Zifferntexte umzuwandeln. Nicht im Codebuch enthaltene Wörter sind mit der Substitutionstafel 535 umzuwandeln.

Die so erhaltenen Zifferngruppen sind mit dem Verfahren 001 zu chiffrieren. Es dürfen nur chiffrierte Texte gesendet werden.

3.5. Substitutionstabelle JUNO der T-305 ^{BStU*1 *76}

Realisiert wurde der Komplex T-305 durch das VEB Kombinat Zentronik, Büromaschinenwerk Sömmerda.

Das Pflichtenheft für die [T-305](#) wurde am 11. Mai 1972 festgeschrieben. Die T-305 ist eine maschinelle Buchstabensubstitution - JUNO - und der anschließenden Chiffrierung mit der [T-304](#). Die Substitution JUNO T-305, im zusammenwirken mit dem Chiffriergerät T-304, wurde für die automatisierte Chiffrierung des agenturischen Chiffrierverkehr genutzt. Das Nachfolgerät [T-307/3](#) wird nachfolgend beschrieben und verwendet das gleiche Chiffrierverfahren.

Substitutionstabelle JUNO

	0	1	2	3	4	5	6	7	8	9
7	a	e	i	n	r	s	+cs			
8	ä	b	c	d	f	g	h	j	k	l
9	m	o	ö	p	q	ß	t	u	ü	zs
9	.	,	-	:	/	v	w	x	y	z

Besonderheiten:

6 = + = CS (Codesignal)

89 = ZS (Ziffernsignal)

Die Zahlen von 0 bis 9 werden als Trigramme abgebildet.

0 = 000, 1 = 111, ... 9 = 999

3.6. Substitutionstabelle JUPITER der HV A ab 1960.

Zur automatischen Chiffrierung im Chiffriergerät [T-307/3](#) implementierte Substitution JUPITER erleichterte die Bearbeitung der agenturischen Funkprüche der HV A/C. ^{BStU} [*210](#)

Software JUPITER für Windows auf der [Freeware](#) Seite.

A	E	I	N	R	S	Code			
0	1	2	3	4	5	6			
Ä	B	C	D	F	G	H	J	K	L
70	71	72	73	74	75	76	77	78	79
M	O	Ö	P	Q	ß	T	U	Ü	Zahl
80	81	82	83	84	85	86	87	88	89
•	≠	—	:	()	V	W	X	Y	Z
90	91	92	93	94	95	96	97	98	99

3.7. Das dazugehörige Codebuch TITAN-Z

000 abgesandt	253 Deckadresse	505 laufend	758 Stimmung
019 Adresse	262 Dokument	514 Legende	767 TBK
028 Änderung	271 dringend	523 lesbar	776 Termin
037 Anleg-en/ung	280 Einsatz, einsetzen	532 Maßnahme	785 Treff
046 Antwort-en	299 Einschätz-en/ung	541 Material	794 Treff wie vereinbart
055 Anweis-en/ung	307 einverstanden (mit)	550 Mikrat	802 Treffart
064 Arbeit-en	316 Empfang-en	569 Militär-isch	811 Trefftermin
073 Arbeitsstelle	325 Entleer-en/ung	578 mitbringen	820 über
082 Aufenthalt	334 entleert	587 Mittel-en/ung	839 Übergabe, übergeben
091 Aufgabe, aufgeben	343 Ergebnis	596 Nachricht	848 Überprüf-en/ung
109 Aufklär-en/ung	352 Erhalt-en/ung	604 nächst	857 unbedingt
118 Aufnahme, aufgeben	361 Ermittel-n/ung	613 negativ	866 Unterstütz-en/ung
127 Auftrag	370 Erwart-n/ung	622 normal	875 Verbind-en/ung
136 ausführlich	389 Feststell-en/ung	631 notwendig	884 Vereinbar-en/ung
145 Bahnhof	398 Frequenz	640 Objekt	893 Vernicht-en/ung
154 Beginn-en	406 Funk	659 operativ	901 voraussichtlich
163 Beleg-en/ung	415 Geheimschreibmittel	668 Päckchen	910 Vorbereit-en/ung
172 belegt	424 Grenzübergang	677 Politik, politisch	929 vorläufig
181 benötigen	433 Information, informieren	686 Post	938 Vorschlag-en
190 Beobacht-en/ung	442 Instrukteur	695 Post noch nicht erhalten	947 Westberlin
208 Bericht-en	451 Interesse, interessieren	703 Reaktion (auf)	956 Westdeutschland
217 Berlin	460 Karte	712 Send-en/ung	965 Wiederholung-en/ung
226 Bestätig-en/ung	479 Kontakt	721 Sicherheit	974 Wirtschaft-lich
235 Brief	488 Kontroll-en/ieren	730 sofort	983 Zeichen
244 Chiffre	497 Kurier	749 Spruch	992 Zentrale

Chiffrieranweisung:

Der Text wird mit der Substitutionstabelle und dem Codebuch umgesetzt.

Vor Zahlen und Codes sind die Signale, 6 bzw. 89, zu setzen.
Die Zahlen werden durch Verdreifachung codiert. Bsp.: 5 wird zu 555.
Die letzte Fünfergruppe wird mit Punkt "." aufgefüllt.
Siehe auch [Spruch an Kurras](#) und [Chiffrierunterlagen](#) für IM,
sowie der [Spruch](#) eines entdeckten Agenten der HV A.

3.8. TAIFUN, Tarntafel der Funkaufklärung ^{BSU*206} Gebrauchsanweisung

1. Die Tarntafel „TAIFUN“ dient der schnellen Übermittlung getarnter Kommandos zur Peilung schnell-automatisch arbeitender Agentenfunkstationen.
2. Die Kommandos werden nach dem deutschen Buchstabieralphabet gesprochen und einmal wiederholt.
3. **Tarnung**
 - 3.1 Jedes Kommando besteht aus einer Tarngruppe mit 4 Buchstaben, die folgende Bedeutung haben:
 1. Buchstabe: Netzangabe und Tausender der Frequenz (Nach Zeile 1)
 2. Buchstabe: Hunderter der Frequenz (Nach Zeile 2)
 3. Buchstabe: Zehner der Frequenz (Nach Zeile 3)
 4. Buchstabe: Einer der Frequenz (Nach Zeile 4)
 - 3.2 Jedes Blindkommando besteht aus 4 Buchstaben. Der Tarnbuchstabe für die Phrase „Blind“ wird an die Stelle des Kommandos gesetzt, deren Nummer mit der Zeile, aus der die Phrase „Blind“ genommen wurde, identisch ist. An die übrigen 3 Stellen werden beliebige 3 Buchstaben gesetzt. Während der Geltungsdauer eines Schlüssels darf die Phrase "Blind" einer Zeile bis zu dreimal, aber nicht nacheinander, benutzt werden.
 - 3.3 Nach der unter 3.1 und 3.2 und angegebenen Folge wird jede Phrase durch einen der zugeordneten Buchstaben aus dem unmittelbar darunterstehenden Tarnstreifen ersetzt. Die den einzelnen Phrasen zugeordneten Buchstaben sind in unregelmäßigen Wechsel zu benutzen.

4. **Enttarnung**

Die Enttarnung erfolgt im Enttarnenteil.

- 4.1 Die beiden ersten Buchstaben der Tarngruppe werden im oberen Alphabet aufgesucht, und zwar
- nach dem 1. Buchstaben die Netzangabe und den Tausender der Frequenz im oberen Teil der Schlüsselsteine:
 - nach dem 2. Buchstaben den Hunderter der Frequenz im unteren Teil der Schlüsselsteine.

Die beiden letzten Buchstaben der Tarngruppe werden im unteren Alphabet aufgesucht, und zwar

- nach dem 3. Buchstaben den Zehner der Frequenz im oberen Teil der Schlüsselsteine;
- nach dem 4. Buchstaben den einer der Frequenz im unteren Teil der Schlüsselsteine.

- 4.2 Steht an einer Stelle die Phrase „Blind“, so sind die anderen 3 Phrasen ungültig.

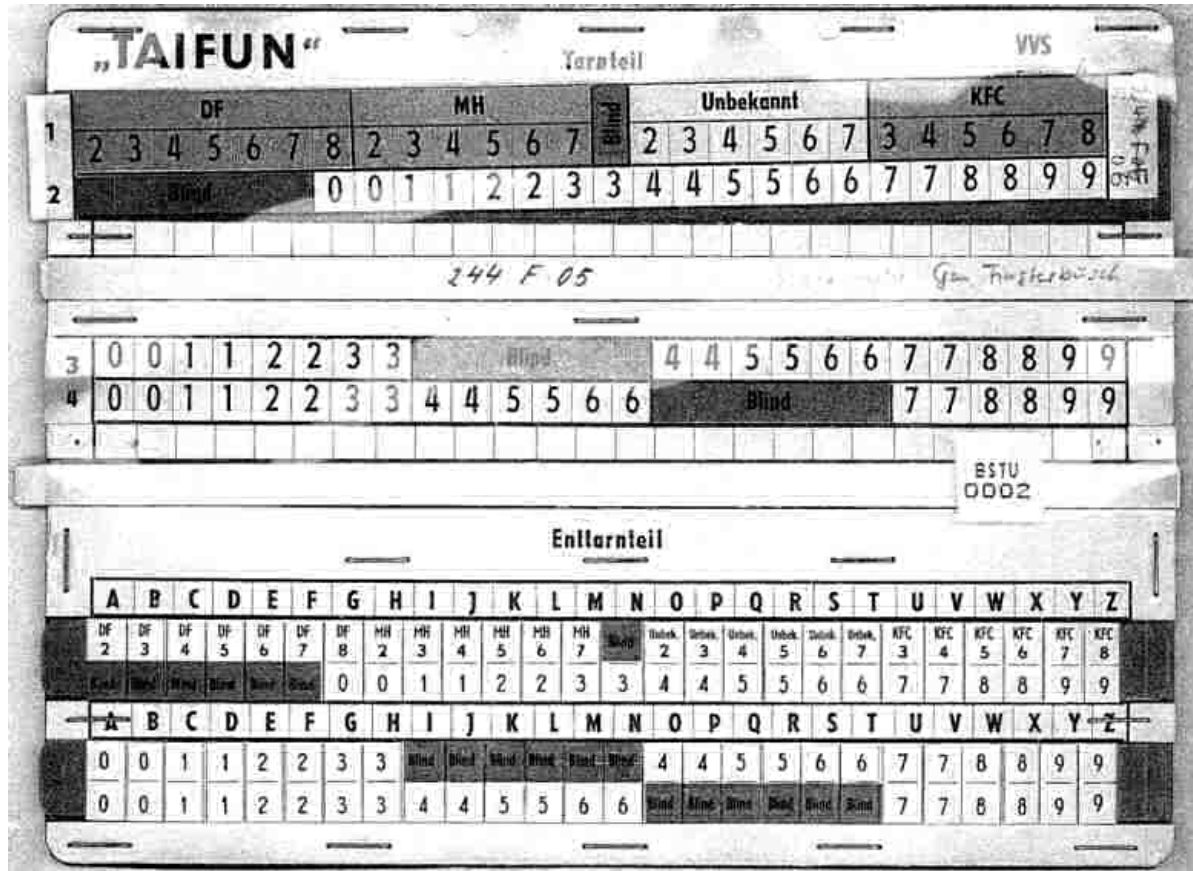


Abb.: TAIFUN Schlüsselschieber

1. oben	N	I	P	W	V	E	Y	M	F	K	B	C	H	R	S	Q	T	G	X	Z	D	L	O	A	U	J	TAIFUN 000 1. Tag / 1. oben
1. unten	N	H	Z	Y	A	D	S	R	F	M	V	W	C	L	P	K	O	T	G	J	X	Q	E	I	U	B	TAIFUN 000 1. Tag / 1. unten
2. oben	U	V	O	F	X	L	G	B	S	Y	T	N	J	K	P	Q	A	H	W	R	M	I	C	Z	D	E	TAIFUN 000 1: Tag / 2. oben

2. unten	W	K	Y	E	J	P	M	L	A	V	H	Z	X	Q	C	B	U	T	G	R	F	N	I	O	D	S	TAIFUN 000
1. Tag / 2. unten																											

Abb.: Tarnstreifen

3.9. ТАБЛИЦА I, ТАБЛИЦА II ^{BStU*195}

А 0				ТАБЛИЦА I				СОВ. СЕКРЕТНО 1 Экс.: №	
АВ 40	АН 41	Б 42	В 43	ВЫ 44	Г 45	Д 46	Ж 47	З 48	Сигн. кода 9
ЗА 50	Й 51	ИЗ 52	К 53	Л 54	М 55	НА 56	О 57	ОБ 58	Сигн. лат. т. 59
ОТ 60	П 61	ПО 62	Р 63	С 64	Т 65	У 66	Ф 67	Х 68	Сигн. арабск. цифр 69
Ц 70	Ч 71	Ш 72	Щ 73	Ъ 74	Ы 75	Ь 76	Э 77	Ю 78	Сигн. римск. цифр 79
Я 80	. ТЧК 81	, ЗПТ 82	- ТИРЕ 83	() СКОБА 84	/ДРОБЬ 85	:ДВТЧК 86	№ 87	Сигн. адрес 88	Сигн. повтор. 89

A 0	E 1	ТАБЛИЦА II							СОВ. СЕКРЕТНО Экс.: № 1	
Ä 20	Ǻ 21	á 22	a 23	B 24	C 25	é 26	ě 27	CH 28	cz 29	
D 30	ǻ 31	drz 32	ě 33	e 34	F 35	G 36	H 37	I 38	Î 39	
и (союз) 40	í 41	J 42	K 43	L 44	ł 45	M 46	N 47	ń 48	Сигн. русск. т. 49	
ň 50	O 51	Ö 52	P 53	Q 54	R 55	ř 56	rz 57	S 58	Сигн. кода 9	
S 60	ś 61	śc 62	š 63	sz 64	T 65	T 66	t 67	trz 68	Сигн. арабск. цифр 69	
U 70	Û 71	V 72	W 73	X 74	Y 75	Z 76	ž 77	ž 78	Сигн. римск. цифр 79	
ž 80	. ТЧК 81	, ЗПТ 82	- ТИРЕ 83	() СКОБА 84	/ ДРОБЬ 85	: ДВТЧК 86	№ 87	Сигн. адрес 88	Сигн. повтор. 89	

3.10. Substitutionstabellen der HV A Agenten, eingesetzt ab den 50ern bis 1990 [Sammler*12](#)
 Erste Substitutionstabellen ab den 50ern bis Ende der 60er.

	1	0	2	6	5	8	4	9	7	3
	R	I	N	S	T	E				
9	A	Ä	Bericht	B	C	D	F	Information	G	N ^o
4	H	J	K	L	bestätigen	M	Stimmung	O	Ö	P
7	benötigen	Ablage	Q	ß	U	Û	V	Telegramm	W	Post erhalten
3	X	Y	Z	Treff	ZS	•	,	-	:	()

	7	9	8	2	5	4	1	6	3	0
	S	E	A	I	T	N				
6	Ä	B	C	erhalten	be- nötigen	D	mitteilen, -ung	F	Tele- gramm	G

0	H	J	K	L	In-formation	M	O	Ö	P	Q
1	R	Stimmung	ß	U	Ü	Bericht	V	W	be-stätigen	X
3	Y	Z	zs	•	,	-	:	()	TBK	/

Eines der beiden Tabellen wurde auch von [G. Guillaume](#) für den [Doppelwürfel](#) später mit Wurmtabellen verwendet.

3.11. Substitutionstabellen der BND Agenten Sammler*12

	0	1	2	3	4	5	6	7	8	9
	D	E	I	N			S	T	A	R
4	B	C	F	G	H	J	K	L	M	O
5	P	Q	U	V	W	X	Y	Z	•	,

Abb.: Umsetztabelle eines BND Schweigefunkers in der DDR. Weitere Fundstellen der Umsetzungstabelle DEIN STAR ist in den Archiven der [polnischen](#) und [tschechischen](#) Sicherheitsdienste zu finden. Weitere Beschreibung des Chiffrierens und der Funkunterlagen sind in [Punkt 19](#) beschrieben.

Die BND Agenten in der VR Polen ohne Deutschkenntnisse hatten ein anderes Merkwort für die Bildung der Substitutionstabelle. Nachzulesen bei Jan Bury in der Cryptologia 31/2007 S. 343 - 357 Sammler*87.

Das Merkwort wurde ab 1960 verwendet. Das Merkwort lautete: ZA OWIES. Übersetzt ins deutsche "FÜR HA FER".

	0	1	2	3	4	5	6	7	8	9
	Z	A				O	W	I	E	S
2	R	B	C	C	D	E	F	G	H	J
3	K	L	Ł	M	N	Ń	O	P	R	S
4	T	W	Y	Z	Ż	•	,	?	-/	-//

3.12. Substitutionstabellen der U.S. Agenten Sammler*87

3.12.1. In der VR Polen

In der Cryptologia 32/2008 S. 343 - 357, vom Autor Jan Bury unter dem Titel: "The U.S. and West German Agent Radio Ciphers" beschreibt er die Verschlüsselung der Nachrichten des BND und des U.S. Geheimdienstes.

Die des BND ist bei Punkt [3.6](#) und [19](#) zu finden.

Diese entsprechen auch denen der in der BStU gefundenen Dokumenten.

Jan Bury beschreibt das U.S. Verfahren wie folgt:

Ähnlich wie bei der BND Substitutionstabelle "DEIN STAR" gab es bei dem U.S.-Verfahren zwei Merkwörter und eine Ziffernfolge zur Bildung der Substitution. Die Merkwörter und die Ziffernfolge wurde individuell für den Agenten erzeugt, das erhöhte die Sicherheit anderer Agenten in der VR Polen. Das erste Merkwort lautete: "KARTEN" und das zweite: "KOSAK". Die Ziffernfolge wurde gebildet aus Geburtsdatum der Ehefrau des Agenten. Das Geburtsdatum lautete 14.8.1930. Da dieses zweimal die "1" beinhaltete wurde die zweite "1" gestrichen. Somit lautete die Ziffernfolge 148930. Die Ziffernfolge und Merkwörter wurden nun in die Substitutionstabelle eingetragen:

	1	4	8	9	3	0	2	5	6	7
	K	A	R	T	E	N				
7	O	P	Q	R	S	T	U	V	W	X
6	S	T	U	V	W	X	Y	Z	A	B
5	A	B	C	D	E	F	G	H	I	J
2	K	L	M	N	O	P	Q	R	S	T

Der Chiffriervorgang ist in [Punkt 9.2.](#) beschrieben. Bei den Agenten im Jahr 1962 gefundenen Substitutionstabelle:

3.12.2. Substitutionstabellen der U.S. Agenten in der UdSSR ^{Link*104}

	0	1	2	3	4	5	6	7	8	9
	A	E	И	Н	О	С	Т			
7	Б	В	Г	Д	Ж	З	Й	К	Л	М
8	П	Р	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
9	Ы	Ь	Э	Ю	Я	•	Lat	RPT	,	Zi.

Zahlen: 1 * 1 2 * 2, etc.

Englisch ersetzt: A - 01 B - 02 C - 03, etc.

Bei den Agenten im Jahr 1972 gefundenen kyrillisch-lateinische Substitutionstabelle:

	0	1	2	3	4	5	6	7	8	9
	A/A	E/E	И/N	Н/R	O/O	C/I	T/T			
7	Б/В	В/С	Г/Г	Д/Д	Ж/Ф	З/Н	Й/Ј	К/К	Л/Л	М/М
8	П/Р	Р/Р	У/С	Ф/У	Х/У	Ц/У	Ч/Х	Ш/У	Щ/З	Ы

9	Ь	Э	Ю	Я	START	•	,	?	-	ENDE
---	---	---	---	---	-------	---	---	---	---	------

94 - Beginn und 99 - Ende
des Signals Kyr.- Lat.- Ziffernregister.

Ziffern:

11 - 1, 66 - 6
22 - 2, 77 - 7
33 - 3, 88 - 8
44 - 4, 99 - 9
55 - 5, 00 - 0

3.12.3. Substitutionstabellen der U.S. Agenten in der DDR^{BSU*25}

	1	2	3	4	5	6	7	8	9	0
	A	N	R	E	I	S				
7	Ä	B	C	D	F	G	H	J	K	L
8	M	O	Ö	P	Q	T	U	Ü	V	W
9	X	Y	Z	,	•	?	!	()	,	-

Ziffern:

01 - 1, 02 - 2
03 - 3, 04 - 4
05 - 5, 06 - 6
07 - 7, 08 - 8
09 - 9, 00 - 0

4. OTP Unterlagen für Agenten ^{Sammler*12}



Abb.: OTP Unterlagen der HVA. [Sammler*12](#)
 Dargestellt sind die Schlüsselunterlagen zum Chiffrieren, im Bild rechts (siehe auch die Abbildung eines [OTP der HVA](#)), und zum Dechiffrieren, im Bild obenliegend, sowie die [Substitutionstabelle und Codetabellen](#) im braunen Umschlag.

BStU
000003

33/0254 01

08178	36878	72241	91936	63141
30725	69085	62311	58046	24539
06147	80503	62168	62635	89613
70378	76894	87414	75304	44323
82540	71985	10842	78504	61729
22208	50537	27255	57983	92088
02102	20553	56910	23159	97867
34289	76398	60782	91398	93774
78172	81658	13670	94835	98453
73235	78465	83962	13128	43090
43898	70174	90114	60730	50370
65570	65667	60164	96472	71630
15484	14845	98729	75873	37020
21183	17689	18406	25783	80744
39885	33543	08117	94211	93420
54027	77932	45781	49475	31674
75878	27410	38260	23221	00313
78340	49555	26188	92201	83725
66463	44242	73783	58105	35290
41163	50834	88500	90326	47153
45021	71527	35628	20347	97355
50022	51416	28821	63835	00082
38014	54041	48657	20679	33704
06332	03455	85212	95381	91808
58812	38144	95124	74068	31300

Abb.: OTP Unterlagen eines CIA Agenten [BStU*25](#)

Handwritten:
4. KSD → ER-4

GVS 350 / 018732
Tabellen 00-99

350

Ex. 021

Abb.: OTP Unterlagen aller DDR Chiffriereinrichtungen [Sammler*16](#)

СИГНАЛЬНАЯ ТАБЛИЦА „1050 А“

Совершенно секретно
Экз. № 90

BSTU
0003

H

												С К П			СКП ВД	См. стр. 5													1 ВРЕМЯ КЛЮЧ №								
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	К2	
00	03	06	09	12	15	18	21	24	27	30	33	36	39	42	45	47	49	51	53	55	57	60	63	66	69	72	75	78	81	84	87	90	93	96	98	3	
D	DFA	DMA		F		I		K		KF	KFA 4	KK	KM		M		MK	ML	MLF	MO		SM														НЕИЗВЕСТН.	4
																																				5	

BSTU 0005	y	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	2 Tag (2. Fassung) ARCHIV E 467
		4 ₂	43	44	45	46	47	48	Blend	Pause	5 ₁	52	53	54	55	56	57	58	59	Ende	QTA	6 ₂	63	64	65	66	67	68	69	7 ₃	74	75	76	77	78	zkk	zbb	
BSTU 0004	y	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	2 Nacht E 46. ARCHIV
		2 ₅	26	27	28	29	Pause	3 ₀	31	32	33	34	35	36	Ende	37	38	39	QTA	4 ₀	41	42	43	44	45	46	zkk	zbb	47	48	49	Blend						

Abb.: Signaltabelle 1050 A. [BSTU*222](#)

5.3. Bipartite Bigramm Chiffrierung [Sammler*13](#)
der NVA, die durch den Funker benutzt wurden.

Ausschnitt:
MRP Rufzeichentabelle
MRP RT

Nr. 5004 Dienstsache . Ausfertigung **K-447**

01 02 03 04 05 06 07 08 09 10
!-----!-----!-----!-----!-----!-----!-----!-----!-----!-----!

```

!-----!
01! !+6 572!JY754 !+8 771!U9 712!I3 728!RE 814!MR 889!EW 298!I2 358!
! !BARK !ZAGREB!STIEGE!SALETT!TEMPO 1KINZIK!DELITA!PESETA!FEMINA!
!-----!
02! !4H 337!KA 916!JN 985!3I 150!9H 217!RM 169!V+ 593!HJ 585!
! !PELLE !ENDAU !JUNGE !SENIOR!RALLEY!ISLAND!ESPAND!DEFROL!
!-----!
03! !8D 688!MS 872!LW 422!+W 123!PK 880!CH 961!L+ 665!
! !LEIHE !KULTUS!ADULA !HOPLIT!LADOGA!DAJAK !DUBLIN!
!-----!
04! !X1 148!AY 366!XE 596!4G 795!VT 187!JJ 622!
! !KALIKO!FLOEZ !PAMIR !FUGE !ALASKA!GRAVIS!
!-----!
05! !8S 847!PX 261!8E 544!DE 864!RN 454!
! !AZETON!IGLAU !MUNDA !OELBAD!HUBERT!
!-----!
06! !4Y 384!3W 927!H1 696!7W 939!
! !DUENE !GLUCKE!PLANUM!MIRAT !
!-----!
07! !D5 438!GU 654!HM 142!
! !RAMBUR!DANTE !EIMAL !
!-----!
08! !6S 591!GW 576!
! !BLICK !FESSEL!
!-----!
09! !KG 657
! !GUTTA

```

Hier ist die vollständige [Abbildung](#) einer MRP Rufzeichentabelle

5.4. Auszug aus der Parolen und Gesprächstabelle des diensthabenden Funkers Ausgabejahr 1969

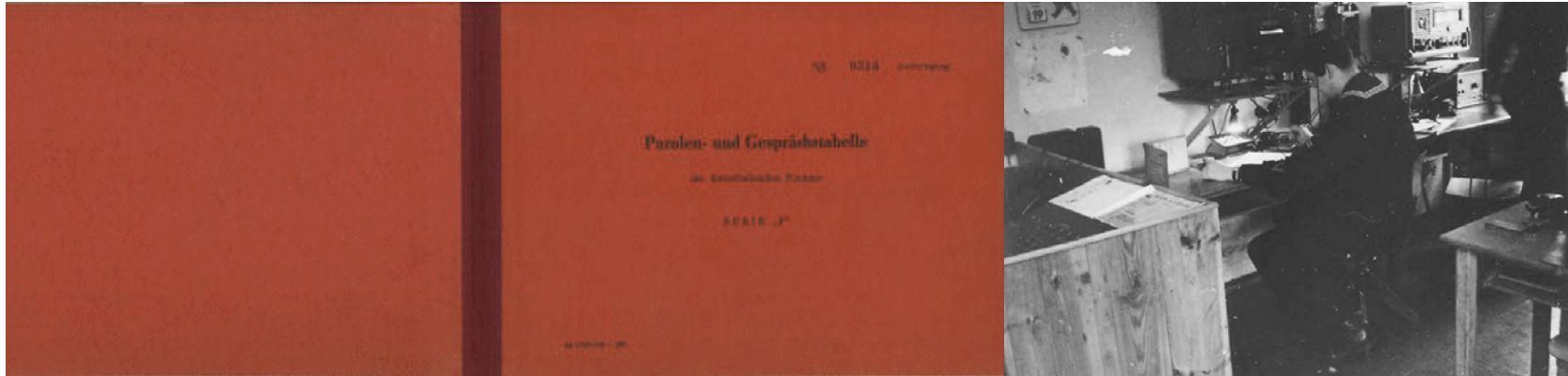


Abb.: Parolen und Gesprächstabelle [Sammler*14](#)

Foto: Funker mit Parolen- und Gesprächstabelle [Sammler*78](#)

Nº 0314 Ausfertigung

Parolen- und Gesprächstabelle

des diensthabenden Funkers

SERIE "F"

Ag 117/II-1/69 - 1203

Arbeiten Sie mit Gerät T (Nr) 1	Senden Sie Spruch (Sprüche) über ... (Rfz.) 2 LUFT	Gehen Sie über auf Zahlen 3 A	Arbeiten Sie ohne Rufzeichen 4 FLUGZEUG
Gehen Sie auf Arbeitsfrequenz kHz (vereinb. Nr.) 11	Arbeiten Sie mit Gerät R (Nr) 12 W	Sie arbeiten mit falschen Ruf- zeichen, über- prüfen Sie 13 FLUGZEUG	Arbeiten Sie (ich arbeite) mit STA-2M (ST-2M) Drehzahl 102U/min 14 DRINGEND

Wechsel der	Gehen Sie auf	
Tag- (Nacht-)	Ersatzfrequenz	
frequenz um kHz	LUFT (L)
.... Uhr	(vereinb. Nr.)	
21 D	22	23

Entschlüsseln Sie	Arbeiten Sie mit	
mit den Begriffen	Amplituden-	
der Gesprächs-	modulation	
tabelle		
31 LUFT	32	

Gehen Sie auf	
Parallelsender auf	
d. Frequenz kHz	
(vereinb. Nr.)	
41	

Serie ,E'

1 9 5 7 2
0 6 2 6
3 2 9
9 7
5

Serie ,F'

Hier ist die vollständige [Abbildung](#) einer Tabelle des diensthabenden Funkers.

5.5. Auszug aus der TDR-78 Sammler*14

						Nr. ...
AB	LUFT	BB	12	BB	B(W)	ГВ 37
AG	Gehen Sie auf Ersatzfrequenz Nr. ...	БГ	13	БГ	teilen Sie Fu.-St. ... Rfz) mit, daß ich sie auf ... kHz rufe	ГГ Г(G)
AD	01	БД		ВД	AUSNAHME	ГД 38
AE	02	BE	Senden Sie (ich sende) Parole	BE	26	ГЕ Starke atmosphärische Störungen
AЖ	Senden Sie auf ... kHz	БЖ	14	ВЖ	Empfangen Sie (ich empfangen) auf Frequenz Nr. ...	ГЖ DRINGEND
A3		Б3	15	В3		Г3 39
AI	03	БИ	Senden Sie (ich sende) auf Frequenz Nr. ...	БИ	27	ГИ
AЙ	FLUGZEUG	БЙ	FLUGZEUG	ВЙ	28	ГЙ Empfangen Sie auf ... kHz
AK	04	БК	Maßnahme gegen Funkstörung Nr. ...	БК	29	ГК Übergang in (Betriebsaufnahme in) FuN Nr. ...

Hier ist die vollständige [Abbildung](#) einer Tabelle des diensthabenden Funkers.

5.6. Auszug aus der TDR-84 Sammler*14

013728 *

Tabelle
des diensthabenden Funkers
TDR-84

Ausgabe 1987

\ / F	0	1	2	3
B \	Reservefrequenz Nr.	FLUGZEUG -F-	(Habe) Antenne f. Arbeit mit Flugzeug - Azi- mutwinkel ... (Grad) ausrich- ten (ausgerich- tet) 02	MONUMENT -M- PLATIN -P- 03
0	00	A(A)	01	
1	Gehen Sie auf Reservefrequenz (Nr. ...)	Eröffnen Sie Arbeit in FuR Nr. ...		
	Γ(G) 10		11	
2	Senden Sie (ich sende) Parole			
	20			

Hier ist die vollständige [Abbildung](#) einer Tabelle des diensthabenden Funkers

5.7. Auszug aus der TDR HA I [Sammler*14](#)

1. Periode

01.03. - 05.05.

08.00/18.00

Vertrauliche Verschlusssache

2. Periode

06.05. - 31.08.

06.00/21.00

VVS-o130

3. Periode

01.09. - 31.10.

08.00/18.00

MfS-Nr. E 17/89

4. Periode

01.11. - 28./29.02.

09.00/17.00

1.Ausf. Bl. 1 bis -

Funknetz-38-111/1	Frequenzen Funknetz				Programmzeiten:
	Tag	Res.	Nacht	Res.	
Variante 03					08.30 - 11.30 Uhr
1. Periode	5372	5750	3352	3198	

2. Periode	4574	5906	3524	3543							
3. Periode	3369	3374	2685	2040							
4. Periode	3640	5191	1766	2063							
					Frequenz nach Kernwaffeneinsatz 1903 KHz						
lfd. Nr.	Teilnehmer	Rufzeichen Funknetz				Havarie RZ	ständ. Frequ.	Reservefrequenz FR		Reservefrequ. HFst.	
		1	2	3	4			Frequenz	Nr.	Frequenz	Nr.
1	2	3				4	5	6		7	
1	Rundspruch	WFMD	9S5N	8C1H	KUEW	PKC4		2392	50	2664*	56
2	Kdo. GT	PKT9	8AFT	MW+Q	SLY2	TUDM	4640	3293	51	3269	57
3	Abt. GKN	F4N9	H27N	9NIQ	BP41	BENP	5013	4544	52	4741#	58
4	UA GAR 5	4JPQ	1UPY	H19N	U5JQ	AHCU	5483#	4933	53	5086#	59
5	UA GR 6	ZI9G	9VIK	HZ5R	NTMN	UIQP	3892	5171	54	5664#	60

Hier ist die vollständige [Abbildung](#) einer Tabelle des diensthabenden Funkers

GVS MfS o008 - 17 / 88^{BStU*43}

5.8. Auszüge aus der Anweisung 2/88

Die Anweisung regelt den Kurzwellenfunkbetriebsdienst des MfS, und es basiert auf der DV 040/0/004 Funkbetriebsdienst des MfNV.

Organisatorische Voraussetzung:

- Funkauftrag mit Nummer des Funknetzes, Nummer der Variante, Funkteilnehmer, Indexzuweisung für Rufzeichen, Havarierufzeichen, Frequenzen.
- Tabelle des diensthabenden Funkers TDR
- Rufzeichentabelle RT
- Unterlagen für den Parolenaustausch

- Schlüsselwechsel in den Funknetzen ist 22.01 Uhr MEZ/MESZ
- Zuweisung der Frequenzen des Funknetzes erfolgt in 4 Gültigkeitsperioden:

- 1. Periode 01.03. - 05.05. 08.00 Uhr 18.00 Uhr
- 2. Periode 06.05. - 31.08. 06.00 Uhr 21.00 Uhr
- 3. Periode 01.09. - 31.10. 08.00 Uhr 18.00 Uhr
- 4. Periode 01.11. - 28./29.02. 09.00 Uhr 17.00 Uhr

Ab dem 25. April 1988 ist die TDR 78-M sowie deren Schlüsselmittel ungültig und zu vernichten.

Anlage 1: Regeln für die Anwendung der Rufzeichentabelle

Anlage 2: Regeln für die Durchführung des Parolenaustausches - Methode SVSk 84

Anlage 3: Regeln für die Anwendung der Tabelle des diensthabenden Funkers (TDR-84)

Anlage 1

Regeln für die Anwendung der Rufzeichentabelle (RT)

1. Die Rufzeichentabelle enthält Felder mit zweistelligen Kombinationen zur Bildung von Tastfunk-/Funkfernsehreibrufzeichen und Substantive mit dreistelligen Zahlen zur Bildung von Sprechfunkrufzeichen.
2. Am linken vertikalen Rand (von oben nach unten) und am oberen horizontalen Rand (von links nach rechts) ist der jeweilige Tagesschlüssel einzutragen.
3. Auf der Grundlage der Indexzuweisung werden die täglich wechselnden Rufzeichen erarbeitet.
Für die im Funkauftrag ausgedruckten Rufzeichenindexe gilt, daß die Null und das Zeichen "+" dem Buchstaben "O" (Otto) entsprechen.
4. Erarbeitung der Tastfunkrufzeichen/Rufzeichen Funkfernsehreiben
 - 1. Zeichen des Indexes in der vertikalen Schlüsselleiste aufsuchen
 - 2. Zeichen des Indexes in der horizontalen Schlüsselleiste aufsuchen
 - Feld im Schnittpunkt beider gedachter Linien aufsuchen und daraus zweistellige Kombination als 1. Teil des Rufzeichens entnehmen
 - 3. Zeichen des Indexes in der vertikalen Schlüsselleiste aufsuchen
 - 4. Zeichen des Indexes in der horizontalen Schlüsselleiste

aufsuchen

- Feld im Schnittpunkt beider gedachter Linien aufsuchen und daraus zweistellige Kombination als 2. Teil des Rufzeichens entnehmen.

Das vollständige Rufzeichen wird durch das Zusammenfügen des 1. und 2. Teiles gebildet.

5. Erarbeitung des Sprechfunkzeichens

- 1. und 2. Zeichen des Indexes dient zur Festlegung der Substantivs
- 3. und 4. Zeichen des Indexes dient zur Bildung der 2-stelligen Zahl
(die 2-stellige Zahl besteht aus dem ersten zwei Ziffern der aufgefundenen 3-stelligen Ziffernkombination).

R S T RSDF6 VERTRAULICHE VFRSCHLUSSACHE
 S T 3 -----
 P G T VVS-NR.: A 758 674
 . AUSF., BLATT 0015

 RSDF6 01, JANUAR
 RST V: Л1М9АБКУ+6Т*3Ц2ЫИ4ГПЬАЗФ85СЕАРХВИ7Н
 H: +ХС5МН2Щ3К4Л3ЦЫФГ8АЕБИЖ6А1РТМЯВ7У9Ь

 ST3 V: АЕФ ХК УГР ЩС ЛЫ АБ+ МЗ ТПЬ ВЖИ ИЯ:1
 H: ЩА ТЖ ГИМ ЗУЫ +Е ПЦ ХВЬ АКФ БРН АСЛ

 PGT 04 05 14 24 26 34 36 37 41 43

RSDF6 02, JANUAR
 RST V: Б8ЫКФЕРППУААЖИЦ1В7+А3РТС4У539ЛЪМН62Х
 H: С46РУ+Ц*8ПНА9Т2ЕРЩАБХЗМ5КЫЛ1ББ7АМЗФ

 ST3 V: ПУ ЗБИ ШЛР ФЬ ГА СХЯ БУД МЕЖ КЦ +ВН
 H: ПЛК ТИВ ЯИ УЕ ХЦД ШЖЫ СА Е+Б ГФР МЗ

 PGT 02 04 11 18 21 23 32 37 45 47

RSDF6 03, JANUAR
 RST V: ЫХУ*4ФС9МПАЛШ+3КАУЕЦР1Т7Р63Б5БНА2А8
 H: 5ЕСФ2Щ9ГИН7АЯР1+Б63МЛЦЫЗВАЖ4УТ7ВХКБ

 ST3 V: Ъ+ ДРК ФЕР Ш*Х ЫВП АН МСА ЯТ ЛЦБ ЗУ
 H: РЦУ АРС ЖХ ШГ Ф+ МЕК ПББ ЯА3 ТЛБ НУ

 PGT 03 08 09 12 19 26 34 36 37 41

Abb.: Schlüsselblatt aus dem MRP-Schlüsselheft.

Funkunterlagen

Gültig ab 8.5.83 für FN/FR ØØA mit R118

Hd. Nr.	Tarnname	Sprechfunkrufzeichen	Telegrafierufzeichen				Sendefrequenzen			
			Tag	Nacht	1. Ers.	2. Ers.	3. Ers.	4. Ers.	Tag	Nacht
1	Objekt		2zbl	2ino	u51m	v8mu		jzxj	1997	2328
2	B 131		7yb4	fkar	h5ev	c3ca		n5ln	4522	1739
3	B151		hjtj	fela	nitx	x1yo		xgje	5240	1909
4	RR		esfk	ibt5	huaø	wfwy			4942	2525
5									5178	2470
6	Einsatz der freiwählbaren Ziffer in die fünfstelligen								5616	2128
7	Farole <u>AM A N F A N G !</u>								1615	2764
8										
9										
10										

Schlüssel senkrecht: 7561049832
 waagrecht: 4765913028
 Schlüsselgruppen: 076 13 429 85
 Strukturgruppe: _____

Persönliche _____
 Rufzeichen/ _____
 Signale/ _____
 Bemerkung: _____

Ersatz-Nr.

1. _____
2. _____
3. _____
4. _____

Erhalten _____
(Datum, Uhrzeit) (Name) (Dienstgrad)

NVA 40 703 Ag 117/1/2 1562-8

Abb.: Auszug für den Dh. Funker.

Anlage 2

5.10. Regeln für die Durchführung des Parolenaustausches

- Methode SVSK-84

1. Für den Parolenaustausch werden benötigt:
 - die Tabelle des diensthabenden Funkers TDR-84 mit eingetragenen Tagesschlüsseln
 - gültige Parolengruppen.

2. Für jeden Tag sind 10 Parolengruppen (Zahlen zwischen 01 und 49) festgelegt.
Der tägliche Wechsel der Parolengruppen erfolgt
22.01 Uhr MEZ/MESZ.
Alle Phrasen des Parolenaustausches sind mit der TDR-84 zu verschleiern.

3. Ordnung des Parolenaustausches
Bei der Parolenanforderung ruft die Funkstelle A die Funkstelle B und übermittelt die Phrasen:
 - "Senden Sie (ich sende) Parole"
 - eine frei gewählte Zahl zwischen 01 und 99.

Die Funkstelle B addiert zu dieser frei gewählten Zahl, wenn diese gleich oder kleiner 50 ist, bzw. subtrahiert von der frei gewählten Zahl, wenn diese größer als 50 ist, eine beliebige Parolengruppe. Die erhaltene Summe bzw. Differenz wird als Parolenantwort zusammen mit einer gleichfalls frei gewählten Zahl und der Phrase "Senden Sie (ich sende) Parole" an die Funkstelle A übermittelt.

Die Funkstelle A überprüft die Richtigkeit der Parolenantwort, indem sie von der als Parolenantwort erhaltenen Zahl die frei gewählte Ausgangszahl subtrahiert, wenn letztere gleich 50 bzw. kleiner als 50 ist, bzw. subtrahiert die Parolenantwort von der frei gewählten Ausgangszahl, wenn letztere größer als 50 ist.

Die Identität der Funkstelle B ist dann gegeben, wenn als Ergebnis eine für den laufenden Tag festgelegte Parolengruppe ermittelt wird.

Danach ermittelt die Funkstelle A die Gegenparole und

sendet diese mittels Phrase "Senden Sie (ich sende) Parole"
an die Funkstelle B.

Die Funkstelle B beendet nach Überprüfung der Identität der
Funkstelle A den Parolenaustausch mit der Verkehrsabkürzung
"OK".

4. Beispiel für den Parolenaustausch

8hnl de c6lk zaw zlt k

8hnl zlp zfm zbw k

c6lk zlt zno k

8hnl ok k

Parolengruppen: 04 08 09 14 19 25 31 38 44 47

c6lk	-	Rufzeichen der Funkstelle A
8hnl	-	Rufzeichen der Funkstelle B
zaw	-	Phrase "Senden Sie (ich sende) Parole"
zlt	-	frei gewählte Zahl (37)
zlp	-	Phrase "Senden Sie (ich sende) Parole"
zfm	-	Parolenantwort (51)
zbw	-	frei gewählte Zahl (67)
zlk	-	Phrase "Senden Sie (ich sende) Parole"
zno	-	Parolenantwort (36)

Anlage 3

Regeln für die Anwendung der Tabelle des diensthabenden
Funktlers (TDR-84)

1. Die Tabelle des diensthabenden Funktlers ist für die Abwicklung
des Dienstfunkverkehrs bestimmt.
2. Die in der Tabelle enthaltenen Felder enthalten Phrasen, Buch-
staben und Zahlen, die mit Hilfe des Tagesschlüssels vor dem
Senden zu verschleiern und nach dem Empfang zu entschleiern sind.

3. Der TDR-Tagesschlüssel besteht aus einem "senkrechten" und einem "waagerechten" Teil mit jeweils zehn 2- bzw. 3-stelligen Buchstabengruppen.

Der jeweilige Tagesschlüssel ist wie folgt einzutragen:

- die erste Schlüsselreihe in die vertikale Schlüsselleiste der TDR-84 von oben nach unten
- die zweite Schlüsselreihe in die vertikale Schlüsselleiste von links nach rechts.

Der Tagesschlüssel ist täglich 22.01 Uhr MEZ/MESZ zu wechseln.

4. Vorgehensweise bei der Verschleierung einer Phrase, eines Buchstabens bzw. Zahl:

- in der betreffenden Zeile aus der vertikalen Schlüsselleiste einen zugeordneten Buchstaben auswählen (1. Zeichen).
- in der betreffenden Spalte aus der horizontalen Schlüsselleiste einen Buchstaben auswählen (2. Zeichen).

Die Entschleierung ist in umgekehrter Reihenfolge durchzuführen.

5. Den ermittelten Zeichen ist beim Senden in den Betriebsarten Tastfunk und Funkfern schreiben der Buchstabe "Z" voranzustellen. Bei Sprechfunk entfällt das Voranstellen des Buchstaben "Z".
6. Die Anwendung der Phrasen "Lesen Sie Zahlen" und "lesen Sie Buchstaben" ist nur gestattet, wenn aus der vorher gesendeten Phrase nicht eindeutig hervorgeht, daß ein Buchstabe bzw. eine Zahl folgt.
7. Vor dem Verschleiern von Zahlen mit ungerader Zifferanzahl ist eine Null voranzustellen und anschließend eine paarweise Verschleierung vorzunehmen.
8. Es ist verboten:
 - ganze Wörter bzw. Texte mit Hilfe der TDR-84 zu verschleiern

- eine Phrase stets mit der gleichen Buchstabenkombination zu verschleiern.

9. Werden Q-Gruppen zusammen mit Uhrzeiten, Spruchnummern, Rufzeichen u.a. gesendet, sind diese Zeichen nicht zu verschleiern.

Werden Q-Gruppen zusammen mit einem Index gesendet, ist im Falle der Verneinung die Zahl 5 anzufügen.

Die in der TDR-84 aufgeführten Verkehrsabkürzungen und Q-Gruppen sind gleichfalls für den Dienstfunkverkehr anzuwenden.

5.9. PTRTS-73 Parolen und Gesprächstabelle des diensthabenden Richtfunkers ^{BStU*185}

Richtfunkbetriebsunterlagen

1. Schlüssel für die Parolen und Gesprächstabelle des diensthabenden Richtfunkers (PTRTS-73)

<u>Datum</u>	<u>senkrecht</u>	<u>waagrecht</u>
01., 11., 21., 31.	24895 06713	68931 52470
02., 12., 22.	39572 81064	78654 32190
03., 13., 23.	03657 94182	41835 02976
..		
..		

2. Tarnzahlen für den Dienstkanalverkehr

<u>Dienststellung</u>	<u>1.Monats- dekade</u>	<u>2.Monats- dekade</u>	<u>3.Monats- dekade</u>
Chef/Leiter Nachrichten	13	42	85
Vertreter CN/LN	72	03	11
Kommandeur	55	71	67
Stabschef	47	39	41
Stv.Kom.für PA	56	81	01
Stv.Kom.für TA	31	46	96
Stv.Kom.für NT	63	29	98
Ltr.RFuZ/RFuSt	04	59	43
Chef Richtfunkverb.	17	99	20
Ltr.RFuA/RFuR	44	10	17
Truppführer	76	49	31

3. Bezeichnung der Trupps und Richtfunkstrecken

Bereich	Truppsnummer	Nr. der RFuA/RFuR
MfS	.1-2. bis .1-4.	80. bis 84.
MdI	.1-5. bis .1-59.	85.
MfNV	.5-0. bis .5-7.	

4. Zuweisung der Nummern der Richtfunkrichtungen und der Sende-/Empfangskanäle für FM 24/400

1. Bezirksverwaltung (Stationäre Führungsstelle -AFüSt)

BV	Nr.-RR	Sende-/Empfangskanal
Rostock	831	880/960
Schwerin	832	716/796

..
..

2. Wachregiment "F. Dzierzynski"

..
..

3. Zentrale Dienstseinheiten des MfS

..
..

5. Regeln für die Anwendung der Tabelle PTRTS-73

- (1) Die Tabelle PTRTS-73 ist für den Parolenaustausch bei Aufnahme der Verbindung und das Führen von Dienstgesprächen zwischen Diensthabenden der Richtfunkstellen/-zentralen beim Herstellen, Halten und Betreiben von Richtfunkverbindungen bestimmt. Sie ist gleichermaßen auf Richtfunkverbindungen zu Funkfernbedienung anzuwenden.
- (2) Die Tabelle hat insgesamt 388 Felder, die durch 100 Großfelder und deren Unterteilung in 4 Kleinfelder gebildet werden. Die Großfelder sind stark, die Kleinfelder schwach umrandet. Felder, deren Ecken schwarz markiert sind, dürfen nur innerhalb der bewaffneten Organe und anderen Organe der DDR genutzt werden.
- (3) In den Feldern der Tabelle sind Phrasen, Buchstaben und Zahlen enthalten, die mit Hilfe der täglich wechselnden

Schlüssel vor dem Senden zu verschleiern sind.

A	B
D	C

Zuordnung: A - obere Phrase
B - kyrillische und lateinische Buchstaben
C - ein- und zweistellige Zahlen
D - untere Phrase

(4) In die Tabelle sind zwei Schlüssel einzutragen.

Senkrechter Schlüssel: in die vertikalen Schlüsselleisten
von oben nach unten

Waagerechter Schlüssel: in die horizontalen Schlüsselleisten
von links nach rechts

Diese beiden Schlüsselzahlen geben die Koordinaten des Großfeldes an.

Das Kleinfeld wird durch die Schlüsselzahl der betreffenden Phrase

- lesen Sie die obere Phrase
- lesen Sie die untere Phrase
- lesen Sie Ziffern
- lesen Sie Buchstaben

bestimmt.

(5) Reihenfolge der Tätigkeit zur Verschleierung der in den Feldern aufgeführten Phrasen, Buchstaben und Zahlen.

Jede beliebig in den Feldern enthaltene Phrase/Buchstabe/Zahl wird mit vier Zahlen des jeweils gültigen Schlüssels verschleiert. Die ersten beiden Zahlen ergeben in der Reihenfolge senkrecht waagrecht die Koordinaten des Großfeldes. Die dritte und vierte Zeile bestimmen das Kleinfeld.

(6) Das Entschleiern wird in umgekehrter Reihenfolge durchgeführt.

Die erste Zahl der empfangenen vierstelligen Zahlengruppe wird in der senkrechten, die zweite Zahl in der waagerechten Schlüssel-
leiste aufgesucht. Die dritte Zahl ist wiederum in der senkrechten, die
vierte Zahl in der waagerechten Schlüsselleiste aufzusuchen.
Im Schnittpunkt befinden sich das Großfeld, welches festgelegt,
welchem der 4 Kleinfelder der Begriff zu entnehmen ist.

(7) Parolenaustausch ist in folgender Ordnung durchzuführen:

- a) Zur Parolenanforderung ist die Phrase "Geben Sie Parole"
und eine zweistellige Zahl aus dem Kleinfeld (C) zu ver-
schleiern. Die Parolenanforderung besteht also aus
2 vierstelligen Zahlengruppen.
- b) Zur Ermittlung der Parole sind durch den Empfänger die
beiden Zahlengruppen zu entschleiern. Die aus der zweiten
Zahlengruppe ermittelte Zahl ist in der Reihenfolge
erste Ziffer senkrecht, zweite Ziffer waagrecht im
Schlüselfeld aufzusuchen. Im Schnittpunkt wird im
Kleinfeld C die Parolenzahl gefunden.
- c) Als Parolenantwort ist die Phrase "Ich gebe Parole" zu
verschleiern. Als zweite Zahlengruppe ist die unter b)
ermittelte Parolenzahl und die Verschleierung der Phrase
"Lesen Sie Ziffern" zu übermitteln.
- d) Zur Überprüfung der Parolenantwort ist die erste Zahlen-
gruppe zu entschleiern. Sie muß die Phrase "Ich gebe
Parole" enthalten. Die erste zweistellige Zahl der zweiten
Zahlengruppe ist im Kleinfeld C aufzusuchen. Ihre Ver-
schleierung muß die unter a) ausgewählte Zahl ergeben.

(8) Beispiel für den Parolenaustausch

1.) Schlüssel für die PTRTS-73

Senkrecht: 75 09 32 14 86
waagrecht: 38 64 92 01 45

2.) Parolenanforderung

"Geben Sie Parole" = 0275
Zahl 52 = 2605
übermitteln werden die Zahlengruppen: 0275 2605

3.) Ermitteln der Parolenzahl

0275 = "Geben Sie Parole"
2605 = Zahl 52
Ziffer 5 im senkrechten, Ziffer 2 im waagerechten
Schlüsselstreifen, es ergibt sich die Parolenzahl 14.

4.) Parolenantwort

"Ich gebe Parole" = 9575
Zahl 14 und Phrase "Lesen Sie Ziffern" = 1405
übermittelt werden die Zahlengruppen: 9575 1405

5.) Überprüfen der Parolenantwort

9575 = "Ich gebe Parole"
Zahl 14 im Kleinfeld C aufsuchen, im senkrechten Schlüssel-
streifen ergibt sich 5, im waagerechten 2, also die der
Parolenaufforderung zu Grunde gelegte Zahl 52.

5.11. Meldung über die Verwendung operativer Sendetechnik

Um Kollisionen mit der Funküberwachung zu vermeiden mußten die Nutzer der operativen Sendetechnik, UFT-Funkgeräte, diese dem Funkdispatcher melden.

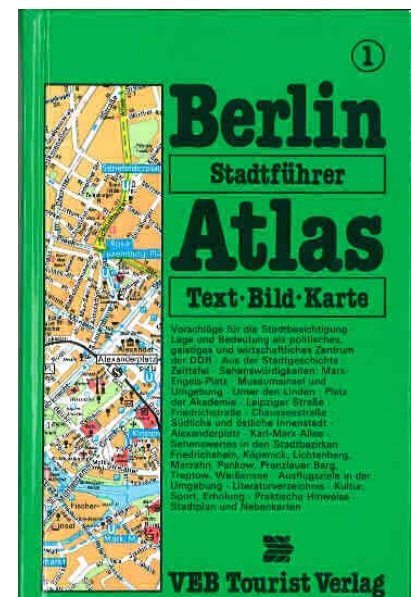
Dies erfolgte per Telefon kodiert in derart:

Als Basis für die Ortsbestimmung in dem Raum in der die Funktechnik genutzt wurde, legte man fest für Berlin das der Stadtplan von Berlin mit folgenden Daten zu nutzen ist:

"Stadtplan - Berlin 1 : 25 000 Buchplan VEB Tourist Verlag 2. Auflage / 151.- 200 Tausend 1980"

Die kodierte Meldung: **9B3 Anmeldung 0105 1130 960 Konrad Krause XVIII/8 44353**

setzte sich zusammen aus:



9 Seite des Buchplanes
B3 Planquadrat, es wurden keine Unterquadrate gebildet.
Anmeldung 0105 1130 An-, Abmeldung Tag Uhrzeit
960 Frequenz
Konrad Konrad = Kurzbetrieb, Dora = Dauerbetrieb. Wobei die Sendetechnik max. 30 min betrieben wird.
 Oder es handelt sich um ferngesteuerte operative Sendetechnik. (Wanzen ?)
Krause Name des Meldenden
XVIII/8 HA oder Abteilung No.
44353 Telefonnummer

5.12. Stärkemeldung des Wachregimentes mittels Bigramme Codes

Wachregiment Berlin
 "Feliks Dzierzynski"
 Chiffrierdienst

Kennwort für KBM: A m s e l
Kennwort für KTE: N e l k e

Vertrauliche Verschlusssache
 o007 MfS WR-Nr. 240/81

Gültig ab: 01.Dez. 1981

Z A H L E N T A F E L

C O D I E R T E I L

0	1	2	3	4	5	6	7	8	9	<u>KBM</u>	
XN YM	WN TY	WC SX	RM SN	OR RH	OI RC	VJ OL	TK ZI	NS PH	WK OB		.52 Ausfertigung 1 Blatt
YV XK	VI OH	UR PO	TA XG	WP XI	US OC	YU NZ	YR UD	SO RB	VM OM		
RG PS	VB PD	YS SV	YQ VH	ZR VA	YT WF	XD XE	XH SM	WQ SZ	NE UY		
UQ WM	XA TB	SQ SW	UP RA	VD OP	YN YL	PU NF	ZB OF	WR PJ	NK YW		
PT TH	NH WA	ZS TQ	NQ NA	UC RL	NL UN	ZC ZD	ZH ZK	PK XB	TZ XR		
PQ WL	OQ TC	SR RE	ZP UK	SP TR	VE ZM	PR RN	ND RD	VL UB	VO TO		
										13 Ural mit TrVR	1 = ^A ist
										14 SPW 60 PB	2 = ^A e
										15 Ural m.chem.Mitteln	
										16 D -30	3 = KTE
										17 SPG - 9	
										18 R 142	<u>Kfz.</u>
										19 P 240 T	Einsatztechnik = rot

DECODIERTEIL

N	O	P	R	S	T	U	V	W	X	Y	Z
A 3	B 9	D 1	A 3	M 7	A 3	B 8	A 4	A 1	A 1	L 5	B 7
D 7	C 5	H 8	B 8	N 3	B 1	C 4	B 1	C 2	B 8	M 0	C 6
E 9	F 7	J 8	C 5	O 8	C 1	D 7	D 4	F 5	D 6	N 5	D 6
F 6	H 1	K 8	D 7	P 4	H 0	K 3	E 5	K 9	E 6	Q 3	H 7
H 1	I 5	O 2	E 2	Q 2	K 7	N 5	H 3	L 0	G 3	R 7	I 7
K 9	L 6	Q 0	G 0	R 2	O 9	P 3	I 1	M 0	H 7	S 2	K 7
L 5	M 9	R 6	H 4	V 2	Q 2	Q 0	J 6	N 1	I 4	T 5	M 5
Q 3	P 4	S 0	L 4	W 2	R 4	R 2	L 8	P 4	K 0	U 6	P 3
S 8	Q 1	T 0	M 3	X 2	Y 1	S 5	M 9	Q 8	N 0	V 0	R 4
Z 6	R 4	U 6	N 6	Z 8	Z 9	Y 9	O 9	R 8	R 9	W 9	S 2

Anwendung:

1. Mit dem CODIERTEIL werden Zahlen codiert. 12-fach Belegung.
Buchstabenpolygramme unsystematisch benutzen.
2. Mit dem DECODIERTEIL werden die codiert übermittelten Zahlen in Klareinheiten umgesetzt, z. B.: TB UC VO = 149
3. Einheitsbezeichnungen sind grundsätzlich mit Tarnnamen durchzugeben.
4. Einheiten mit Kp.-Stärkebuch (NVA 37301) melden nach Hoch- und Rechtswert.
5. Einheiten mit Batl.Stärkebuch (NVA 37302) melden nach den in der Kopfleiste angegebenen Ziffern.

20 FS-Chiff.-Trupp	
21 LBW	Transporttechnik = blau
22 Stabsbautrupp	
23 TZ - 74	<u>Panzer</u>
24 Ladetrupp	Kampftechnik = schwarz
25 R - 140	
26 R - 405 xN-1	<u>Artilleriebewaffnung</u>
27 NF Schaltstelle	
28 ARS - 14/12 U	Haubitze D-30 = grün
29 PSH K-O PiAT	SPG - 9 = braun
30 Kran	
31 DA - 66	<u>Fla-Raketenbewaffnung</u>
32 TS - 8	Strela-2 Kampftechn. = gelb
33 LO - Ch	
34 RCH / Lab	
35 Ponton	
36 Pugsierboot	
37 PiKW	
38 DOK	<u>Beispiel der Anwendung</u>
39 WFS - 3	
40 WFS - 2	<u>rot</u> 1 VB WC = 12
41 Sägegatter	2 TB UK = 13
42 EKS	3 YW UN = 95
43 Raupe	
44 Bagger	<u>blau</u> 1 WA RA = 13
45 UAS - 469	2 OQ ZM = 15
46 BLS 0,5 WR	3 XR WL = 90
47 AGW	
48 StW / Ch	usw.
49	

6. Bildung von Rufzeichen, durch Schweigefunker des CIA in der DDR. Literatur*[Zwischen den Fronten](#)*

Im Buch "Zwischen den Fronten" von Heinz Günther, wird auf Seite 67f an dem konkreten Beispiel eines CIA Schweigefunker beschrieben wie der Funker seine Rufzeichentabelle bildet.

Zitat:

Es wird ein Merkspruch vereinbart, in diesem Beispiel:

(Theodor Fontane, "Der Stechlin", Spruch des alten Dubslav)

"DAS IST EINE DAME UND EIN FRAUENZIMMER ZUGLEICH"

Dieser wird in eine Tabelle geschrieben, im Kopf stehen die Tage des Monats beginnen mit dem Ersten und endet mit dem Einunddreißigsten.

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.	29.	30.	31.		
D	A	S	I	S	T	E	I	N	E	D	A	M	E	U	N	D	E	I	N	F	R	A	U	E	N	Z	I	M	M	E	R	Z	U	G	L	E	I	C	H	
5	1	3	1	3	3	8	1	2	9	6	2	24	10	36	28	7	11	20	29	15	31	3	37	12	30	39	21	25	26	13	3	4	3	1	2	1	2	4	1	
			8	4	5		8	9	7																					2	0	8	6	3	4	2	4	7		
4	4	7	5	7	7	4	5	6	49	46	42	64	50	76	68	47	51	60	69	55	71	43	77	52	70	79	61	65	66	53	7	8	7	5	6	5	6	4	5	
			8	4	5	8	8	9	7																					2	0	8	6	3	4	2	4	7		

Die Buchstaben werden "durchgezählt". D. h. "A" = 1, 2, 3; "C" = 4; "D" = 5, 6, usw. usf. Als nächstes wird "geschüttelt", in dem beginnend mit dem ersten Buchstaben folgend die Spalten nebeneinander geschrieben werden. Sowie neu beginnen um die untere Zeile ab dem 21. aufzufüllen.

D	5	4	A	1	4	S	3	7	I	1	58	S	34	74	T	35	7	E	8	48	I	19	59	N	2	67	E	9	49	D	6	46	A	2	42	M	2	6	E	1	5	U	3	7	N	2
		5		1	1	3	3	3	8				74			5		8		48		19	59	N	2	67	E	9	49	D	6	46	A	2	42	M	2	6	E	1	5	U	3	7	N	2
6	D	7	4	E	1	5	I	2	6	N	20	6	F	15	55	R	3	71	A	3	4	U	37	77	E	12	52	N	30	70	Z	39	79	I	21	61	M	2	6	M	2	6	E	1	5	R
			7	7	1	1	1	0	0	N	20	6	F	15	55	R	3	71	A	3	4	U	37	77	E	12	52	N	30	70	Z	39	79	I	21	61	M	2	6	M	2	6	E	1	5	R
3	7	Z	7	8	U	3	7	G	1	5	L	2	63	E	14	54	I	22	62	C	4	44	H	17	5	D	5	45	A	1	41	S	33	73	I	18	5	S	3	7	T	3	7	E	8	4
			0	0	8	8	8	6	6	L	2	63	E	14	54	I	22	62	C	4	44	H	17	5	D	5	45	A	1	41	S	33	73	I	18	5	S	3	7	T	3	7	E	8	4	

7. Substitutionsverfahren

7.1. Manuelles Fernschreiben verschlüsseln nach Dienstanweisung GVS 16/50 MfS. BStU*19

Zitat:

Der Klartext wird wie folgt verschlüsselt:

5,2/3,7/4,5/2,9/ u.s.w.

Zeile, Spalte Schlüsselstabelle = Klartextzeichen

Schlüssel Nr.374 5,3=E oder 7,9=A

Satzzeichen werden wie folgt geschrieben:

"."=X ":"=R "-"=U "?"=A "="=B

Zwischenräume werden ausgelassen.

Fernschreibkopf sieht wie folgt aus:

-MFS -BERLIN SCHL.NR 374 FS:NR:12 18.10.50 0900 UHR MEIER=

Beispiel:

Klartext:

"An das Ministerium fuer Staatssicherheit Berlin
Abteilung Nachrichtenwesen

Fernschreibmaschine ist in Berlin gestohlen.

Verwaltung fuer Staatssicherheit Brandenburg
gez. S c h r e i b e r, vp-kdr."

Fernschreibformular und Geheimtext:

"-MFS-POTSDAM SCHL.NR.374 FS.NR.12 18.10.50 0950 UHR KRELLMANN=

AN DAS

MINISTERIUM FUER STAATSSICHERHEIT BERLIN

ABTEILUNG NACHRICHTENWESEN

12,1/2,2/10,4/3,3/7,1/7,2/10,3/9,1/2,2/5,1/2,5/15,3/6,1/10,1/7,2/
1,2/5,1/8,1/1,4/9,4/7,1/13,12/14,4/8,2/10,7/1,7/9,1/6,2/11,2/2,1/
9,3/3,2/6,3/2,9/1,1/7,3/6,2/9,2/9,3XX

VERWALTUNG FUER STAATSICHERHEIT BRANDENBURG

GEZ. S C H E I B E R VP-KDR.

/	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	O	N	Y	E	I	A	S	N	R	S	Y	F	Z	X	J
2	H	E	E	Y	V	L	C	N	E	P	I	R	B	C	Y
3	A	E	N	Q	A	S	H	O	G	H	L	A	L	O	M
4	E	Y	A	R	H	X	A	Y	I	R	H	Q	C	I	X

5	I	L	X	F	J	H	U	R	C	D	M	Y	F	Y	L
6	A	B	S	A	Y	C	L	K	A	X	T	L	A	V	T
7	E	C	H	L	U	B	G	O	Y	B	N	H	V	D	R
8	N	N	U	J	W	Y	C	M	N	S	V	F	X	U	P
9	R	T	G	I	Z	N	V	N	Y	X	A	K	I	L	G
10	S	C	H	R	K	B	X	M	S	N	L	R	H	B	A
11	U	I	O	H	D	L	C	R	N	Q	X	X	W	Y	V
12	F	A	J	X	X	A	F	C	N	L	M	G	T	S	G
13	D	X	U	W	P	T	L	X	M	U	L	T	B	A	I
14	Z	T	K	I	K	U	C	V	D	A	N	K	U	H	A
15	Y	H	M	L	F	L	A	L	B	G	L	H	P	H	R

7.2. Fernschreibschlüssel DORA BStU*201

Einsatz eines Hand- und Maschinenschlüssels, unter Nutzung der Enigma
 Ministerium des Innern

Rostock, den 4.8.54

der Regierung der
 Deutschen Demokratischen Republik
 Kasernierte Volkspolizei
 Verwaltung Volkspolizei - See
 Stab/ 8. Abteilung

E N T W U R F

A r b e i t s a n w e i s u n g
 - -

über die Handhabung des
 Fernschreibschlüssel "Dora" (FSD)

F.d.r.
(W e d e r)
Leutnant.

- 2 -

Der Fernschreibschlüssel "Dora" ist ein Maschinenschlüssel zum Verschlüsseln vertraulicher und geheimer Nachrichten welche per Draht übermittelt werden.

Die Handhabung des Maschinenschlüssel ist nur den dafür zugelassenen Personal zu unterweisen.

Der Maschinenschlüssel hat einen mechanischen und einen elektrischen Teil. Beide Teile sind gegen Stoss - und Schlagwirkungen sehr empfindlich. Aus diesen Grund muss beim Transport der Maschine mit grosser Vorsicht umgegangen werden.

Näheres über die elektrisch mechanische Betriebsvorschrift siehe in die dafür bestimmte Arbeitsanweisung.

Der Verschlüsseln eines Spruches:

Zum Ver- und Entschlüsseln eines Spruches wird eine Parole benötigt.

Die Parole enthält:

- a.) Die Steckverbindung des Tages.
- b.) Die Zahlentauschtafel für die Kenngruppen.
- c.) Die Umsetztabelle für den Spruchschlüssel.

Diese Parole ändert sich jeweils um 24,00 Uhr. Die Einstellung der Steckverbindung wird vom Personal selber vorgenommen.

Ein verschlüsseltes Fernschreiben besteht aus:

1. Uhrzeitgruppe
2. Gruppenszahl
3. Kennzahl
4. Schlüsselgruppe
5. Text
6. Unverschlüsselte An- und Unterschrift nach Tarntabelle.

Die Uhrzeitgruppe wird vom Absender angegeben. Die Gruppenzahl ergibt sich aus der Länge des Spruches.

- 3 -

- 3 -

Der Spruchschlüssel dient zur Lösung des Spruches.

Zur Herstellung des Spruchschlüssels wird benötigt:

- Die Uhrzeitgruppe und das Tagesdatum (z. B. 17,35 am 06.)
- Eine willkürlich gewählte 3-stellige Zahl als Kenngruppe.
- Die Umsetztabelle der Parole

Beispiel: Uhrzeitgruppe + Datum 1 7 3 5 0 6
 willkür.l.gew.Kennzahl 4 3 8

 2 1 3 8 1 4

Es ist dabei zu beachten das die Kennzahl unter die 2.- 4. und 6. der Uhrzeitgruppe mit Datum gesetzt wird.

Diese Lösung 21 38 14 ist die Maschineneinstellung zur Lösung des Spruchschlüssels.

Bei diesem Beispiel ist aber die 2. Zahlengruppe nicht im Bereich von 1 - 26 und könnte demzufolge nicht eingestellt werden.

In diesen Fällen wird die Zahl welche ausserhalb des Bereiches 1 - 26 liegt durch 2 geteilt. Also ist die Zahl 38 zur Zahl 19 geworden. Ist die Zahl so hoch das sie bei einmal Teilen noch nicht in das Bereich fällt so ist sie solange zu teilen, bis sie in das Bereich 1 - 26 fällt.

Also müssen jetzt die Zahlen

21 19 14

in den Fernstern der Maschine eingestellt werden.

Dann wählen wir uns eine willkürlich zusammengestellte 4-stellige Buchstabengruppe

Zum Beispiel: Q W M Y

Diese drücken wir nacheinander durch den eingestellten Schlüssel.

Ergibt dann: E I G U

Diese 4 Buchstaben kommen in die erste Fernschreibgruppe und stellen den verschlüsselten Spruchschlüssel dar.

Zum Verschlüsseln des Textes wird in die Maschine der unverschlüsselte Spruchschlüssel (QWMY) gemäss der Umsetztabelle eingestellt. Dazu werden nur die ersten drei Buchstaben benötigt.

- 4 -

Also +: Q = 13
 W = 24
 M = 25

Jetzt werden diese drei Zahlengruppen in die Fenster der Maschine eingestellt. Mit dieser Einstellung wird dann die 2. Reihe der Schlüsselgruppen verschlüsselt.

Das Verschlüsseln des Textes:

Um ein schnelleres Ver- und Entschlüsseln zu ermöglichen, wird hier ein kombiniertes Verfahren angewandt. Beim Eintragen des Klartextes in die Schlüsselgruppen werden die Buchstaben einmal in die linke und andermal in die rechte Seite einzeln eingetragen.

Schlüsselgruppen

1	b t i f	█	█
2		█ e r f t █	
3	x o o t	█	█
4		█ s f r m █	
5	e d n x	█	█
6		█ l u g x █	

Also B in das 1. Kästchen der linken 1. Gruppe
 E " " 1. " " rechten 2. "
 T " " 2. " " linken 1. "
 R " " 2. " " rechten 2. "
 i " " 3. " " linken 1. "

u. s. w.

Nach diesen Eintragungen werden die Buchstaben der rechts stehenden Gruppen mit der eingestellten Maschine durchgedrückt und die aufleuchtenden Buchstaben in die linke Spalte zwischen die schon stehenden Buchstaben eingeschoben.

Umstehend aufgeführtes Beispiel sieht dann so aus:

B	T	I	F	
M	C	L	G	<-----ERFT
X	O	O	T	
Q	S	D	R	<-----SFRM
E	D	N	X	
O	C	Q	B	<-----LUGX

Der abgabebereite Fernschreibspruch für die Übermittlung sieht zusammengesetzt wie folgt aus:

17,35 = Uhrzeitgruppe
7 = Gruppenzahl
438 = Kennzahl

	E	I	G	U	=	Schlüsselgruppe
	B	T	I	F	-	
	M	C	L	G		
	X	O	O	T		
Anschrift +	Q	S	D	R	->	der verschl. Text
Absender	E	D	N	X		
	O	C	Q	B	-	

Alle im Text vorkommenden Zahlen werden in Buchstaben geschrieben. Dazu wird nach folgenden Schema verfahren:

1 =	EIN	6 =	SEX
2 =	ZWO	7 =	SIB
3 =	DRI	8 =	ACT
4 =	VIR	9 =	NEN
5 =	FUF	0 =	NUL

Als Satzzeichen werden die Buchstaben wie bisher angewendet.
Zahlen werden stets einzeln geschrieben, das Zusammenziehen von
Zahlen ist nicht gestattet.

Das Entschlüsseln:

Beim Entschlüsseln wird in umgekehrter Reihenfolge verfahren.

1. Spruchschlüssel ermitteln (Uhrzeitgruppe, Datum, Umsetztabelle)
2. Jede 2. Gruppe mit richtig eingestellten Spruchschlüssel entschlüsseln.
3. Buchstaben der linken und rechten Reihe zusammensetzen.

Jede Gruppe auch die letzte Gruppe muss eine volle 4-stellige
Buchstabengruppe ergeben.

6.8.1954

E/P G/Q I/R K/S M/T O/U C/V D/W J/X F/Y
B/Z A/H

1 2 3 4 5 6 7 8 9 0
8 9 7 6 5 0 1 2 3 4

01 02 03 04 05 06 07 08 09 10 11 12 13
H J V E Y O A G N P R K Q

14 15 16 17 18 19 20 21 22 23 24 25 26
B X C Z U L S F T D W M I

7.8.1954

G/Q A/H J/C L/D N/E P/F R/Y T/M V/I X/O
Z/K B/S

1 2 3 4 5 6 7 8 9 0
9 0 8 2 4 7 1 6 5 3

01 02 03 04 05 06 07 08 09 10 11 12 13

L	T	F	Z	P	A	X	I	C	V	N	E	Y
14	15	16	17	18	19	20	21	22	23	24	25	26
R	G	W	B	S	D	J	K	U	H	M	Q	O

7.3. ATLAS, Auslandshandelsvertretung Chiffrierverfahren nach Gebrauchsanweisung A und B ^{BSTU*114}

Die Gebrauchsanweisung A ist in allen Ländern anzuwenden in denen die [Chiffriergenehmigung](#) vorliegt bzw. das Versenden von chiffrierten Telegrammen toleriert wird.

Die Chiffrierung, nach Gebrauchsanweisung A, der durch das [Codebuch](#) gewandelten Klartexte wurden mit dem [Verfahren 001](#) durchgeführt.

Beispiel:

Klartext: "Abkommen 60 abgelehnt."
 HKtxt: "0132 0166"
 001: "3597 1247"
 GTX: "3629 1303"

Die Gebrauchsanweisung B ist in den Ländern anzuwenden in denen der ACME Code [zugelassen](#) ist.

Die vierstellige Codegruppe beschreiben die Zeile und Spalte des [ACME Codes](#) der die Substitution bildet.

Die ACME Tabellen bilden hier den Schlüssel.

Beispiel:

Klartext: "Abkommen 60 abgelehnt."
 HKtxt: "0132 0166"
 ACME: "uuogb wboba"

Schlüsselverwaltung bei beiden Verfahren:

Die Schlüsselunterlagen sind wie folgt verteilt: Die Handelsvertretung erhält 1 Exemplar, das Außenhandelsministerium erhält 1 Exemplar und die Abteilung XI Referat 2 des MfS die dritte Ausfertigung der Schlüsselunterlagen.

Der Schlüsselwechsel erfolgt aller drei Monate, bei Kompromittierung oder erhöhten Nachrichtendichte sofort.

Der Schlüsselwechsel wird angekündigt mit der Codegruppe "0000".

Bei Anwendung des Verfahren B ist die Codegruppe "acme" voranzustellen.

Durch das MfS damals nichterkannte Fehler bzw. Mangel der beiden Verfahren: Beide Verfahren nutzen das gleiche Codebuch. Durch die Anwendung des

Verfahrens 001 und der Substitution durch ACME wird bei spruchgleichen Klartexten der Schlüssel 001 und des ACME kompromittiert.

Erkannt wurde aber das das Verfahren ACME keinerlei Sicherheit der Information bietet. Mit der [ACME-Software](#) können entsprechende Listen erstellt werden.

7.4. MOSSAD Verfahren, beschrieben in "Der MOSSAD" S.22. Lit. [*Mossad](#)

Beschrieben als Mossad-Doppel-Kodiersystem.

Die phonetischen Laute werden mittels einer Substitutionstabelle durch Zahlen ersetzt.

Beispiel: ABDUL in AB = 7, DUL in 21.

Die gebildeten Ziffern erhält einen weiteren Buchstaben oder Ziffer.

Beispiel: A7O 21B

Die Substitutionstabelle wird wöchentlich gewechselt.

Zur Übertragung der Nachricht wird diese gesplittet:

Sendung 1: A7O

Sendung 2: 21B

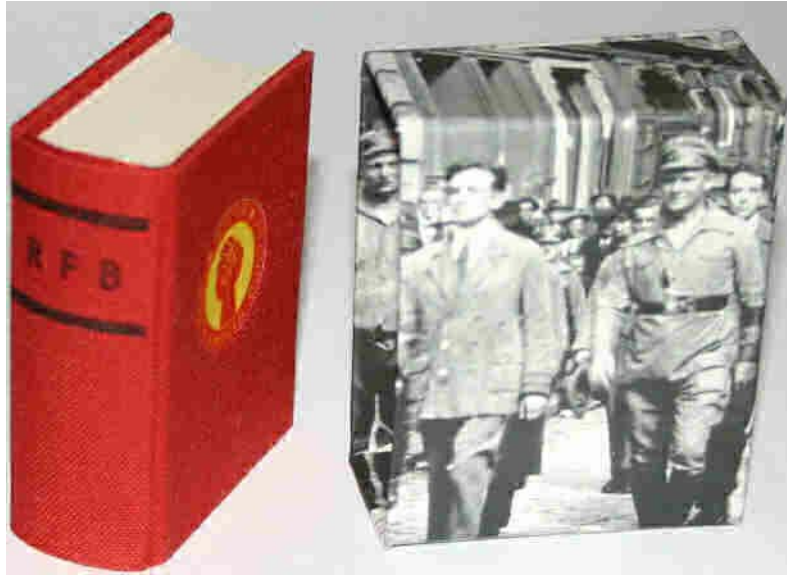
Welche Sendung zuerst erfolgt und wie die Splittung erfolgt ist nicht dokumentiert.

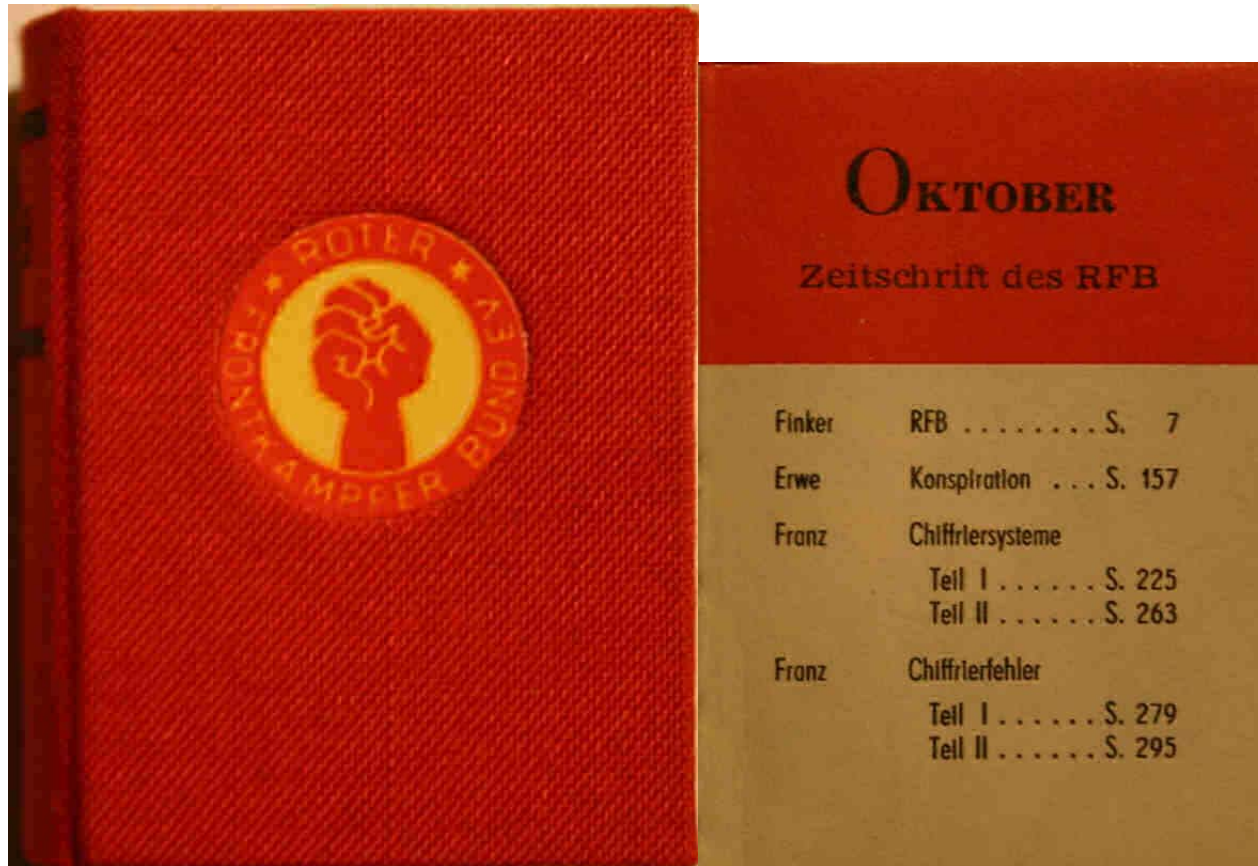
8. Beschreibung eine manuellen Chiffrierverfahrens in einem Minibuch des MfS [Sammler*17](#)

Softwareumsetzung für Windows per eMail

Es wird vom [Original](#) abgewichen um eine verbesserte Verschlüsselung zu erreichen.

DAS VERFAHREN IST TROTZDEM NICHT SICHER





8.1. Das Original, Autor: Franz. ^{Sammler*17} [die Modifikation Original Version 2](#)

"Vigenere Beaufort" Chiffrierschritte
Vorgeschichte zu dem Verfahren:
Das Verfahren wurde entwickelt aus den Forderungen
der Beschlüssen des 10. EKKI Plenums
der Kommunistischen Internationale. In dem gefordert
wurde die Listen der leitenden Kader gedeckt zu führen.

Erstellen einer Chiffrierzahl:

Der Autor benutzt als einfach zu merkende Zahl den Geburtstag des

Urgroßvater: 28.6.1845, also Teil 1 der Zahl ist 2861845.

Teil 2 ist die Quersumme aus o.g. Zahl = 34, Ergebnis 286184534.

In Teil 3 erfolgt das auffüllen der fehlenden Zahlen 7, 9 und 0.

Die erzeugte Chiffrierzahl lautet jetzt:

2 8 6 1 8 4 5 3 4 7 9 0

Wobei jede Zahl vorkommen muß.

Wandeln des Buchstabenvorrates in eine 5 x 5 Tabelle

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Wandeln des Textes "Alfred Krause, Stuttgart, Wilhelmstraße 137" erfolgt:

Der Buchstabe A wird mit dem ersten Zeichen der Chiffrierzahl vorwärtsgezählt $A + 2 = c$

$L + 8 = t$, das erfolgt solange bis die Chiffrierzahl aufgebraucht ist.

Dann wird wieder mit der 2 begonnen.

Achtung hier wird ein weiterführender Druckfehler übernommen!

Aus der Zahlenfolge: 2 8 6 1 8 4 5 3 4 7 9 0 wurde 2 8 6 1 8 4 5 3 5 7 9 0

In der Beschreibung ist der Fehler durchgehend. Es wird weiterfolgend hingewiesen das die Zahlen noch Mischen kann Es wird hier nicht beschrieben.

2	8	6	1	8	4	5	3	5	7	9	0	2	8	6	1	8	4	5	3	5	7	9	0	2	8	6	1	8	4	5
A	L	F	R	E	D	K	R	A	U	S	E	S	T	U	T	G	A	R	T	W	I	L	H	E	L	M	S	T	R	
c	t	m	s	n	h	p	u	f	b	b	e	u	b	a	u	b	l	f	u	y	d	s	l	k	n	r	n	a	x	w

Das Chifftrat wird nicht oder wieder willkürlich getrennt:

CTMSNHPUFBBEUBAUBLFUYDSLKNRNAXW, oder **ctm snhpufb beuba ublfu ydsl knrnaxw**.

Die Zahlen werden wieder mittels eines Chiffrierwortes gewandelt, dabei muß jeder Buchstabe nur einmal auftreten: **"HeilMoskau"**.

Also wird aus der Straßennummer 137 == **HIS**.

Der gesamte Spruch lautet: **CTMSNHPUFBBEUBAUBLFUYSLKNRNAXWHIS**

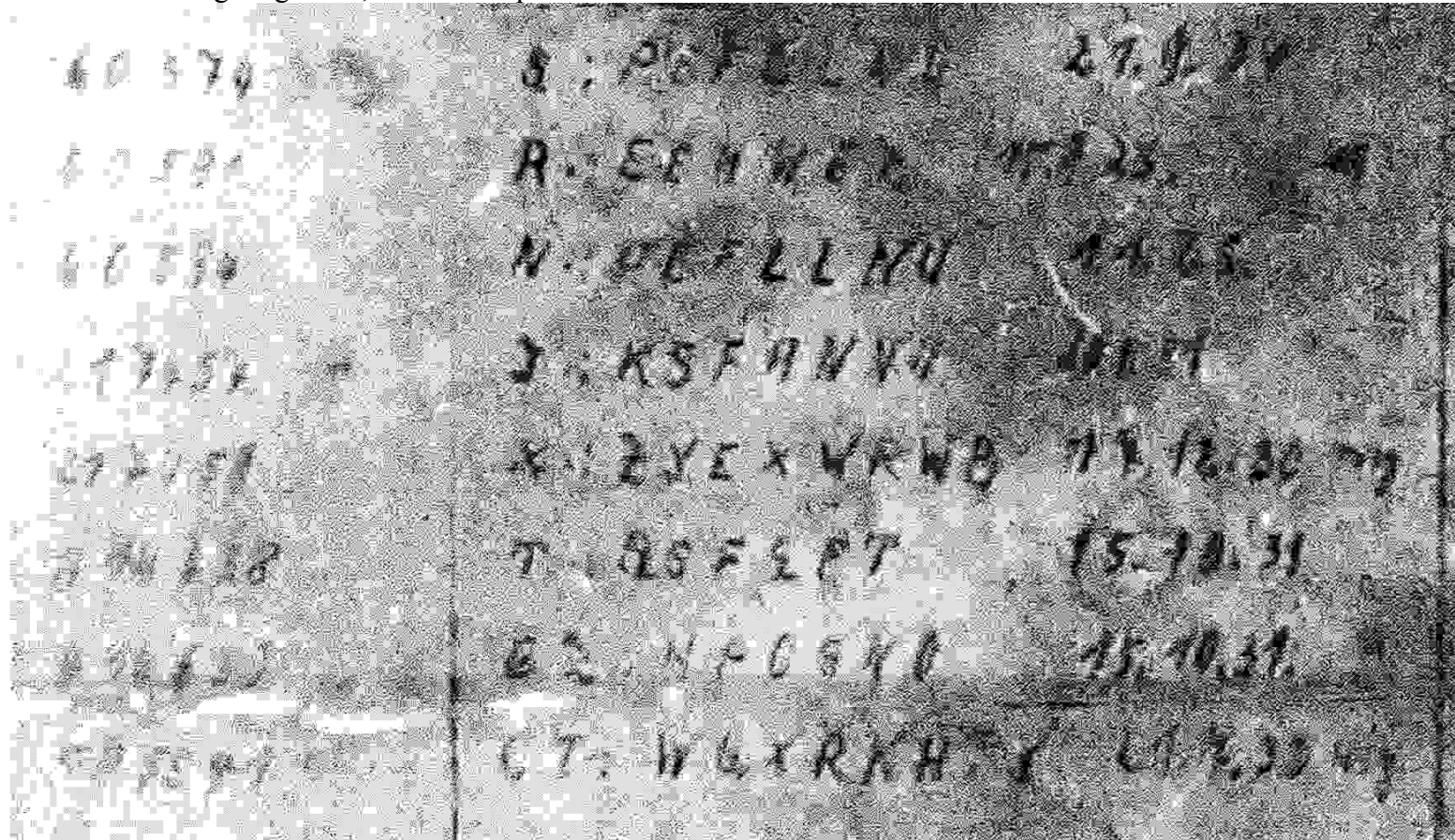
Zitat:

Dieses System hat folgende Vorzüge:

1. Jedes schriftliches Aufbewahren des
2. Chiffrierschlüssels, erfahrungsgemäß eine
3. ständige Gefahrenquelle, fällt fort. So-
4. wohl die zum Chiffrieren von Schrift-
5. wörtern benötigte Chiffrierzahl als auch
6. das zum Chiffrieren von Zahlen benötigte
7. Kennwort können leicht behalten werden.
8. Ein unbefugtes Dechiffrieren ist bei
9. diesem System aufs äußerste erschwert.
10. Wenn auch in dem Klartext ein beliebi-
11. ger Buchstabe mehrmals vorkommt, so
12. erscheinen doch im chiffrierten Text im-
13. mer andere Buchstaben. Im oben ge-
14. wählten Beispiel enthält das Wort Stutt-
15. gart nicht weniger als vier T, an deren
16. Stelle im Chiffretext die Buchstaben
17. B, U, C und Y erscheinen. Dadurch ist
18. das Entziffern ohne Kenntnis der be-
19. nutzten Chiffrezahl absolut unmöglich.
20. (Daß bei praktischer Anwendung dieses
21. Systems weder das von uns als Beispiel
22. benutzte Kennwort noch die Chiffrezahl
23. verwandt werden darf, ist selbstver-
24. ständlich. Es gibt ja an anderen Stelle un-
25. zählige andere Zusammenstellungen.)
26. Sowohl das Chiffrieren als auch das
27. Dechiffrieren erfordert bei einiger
28. Übung, gemessen an anderen Systemen,
29. verhältnismäßig we-
30. nig Zeit.
31. Somit kann diese Methode als für die
32. Zwecke der Partei absolut brauchbar
33. bezeichnet werden. Wir werden in der
34. nächsten Nummer des "Oktober" noch
35. auf einige andere Systeme, die gleichfalls
36. verwendbar sind, eingehen.

In der Denkschrift "350 Jahre Entwicklung des Chiffrierwesens" [BStU*97](#)

ist eine Originalliste der Mitglieder der KPD, Ortsgruppe Lobstädt - Bezirk Leipzig - aus dem Jahre 1933 zu sehen. Das 1945 aus einem Blechbehälter der sich in einer Küche befand. Hier wird ein Auszug dargestellt, da die Bildqualität sehr schlecht ist.



8.2. Die Modifikation [Original Version 1](#) [Original Version 2](#)

"Vigenere Beaufort" Chiffrierschritte

Erstellen einer willkürlichen Chiffrierzahl:

Wobei jede Zahl vorkommen muß, die Zahl groß sein sollte und Zahlen mehrfach vorkommen.

z. B.: **31415926535897932084626430832795** ein verändertes PI
 Erstellen eines willkürlichen Chiffrierwortes: **GEHEIMSAEKRETAER**
 Wandeln des Buchstabenvorrates in eine 5 x 5 Tabelle

G	E	H	I	M
S	A	K	R	T
B	C	D	F	L
N	O	P	Q	U
V	W	X	Y	Z

Wandeln des Textes "Alfred Krause, Stuttgart, Wilhelmstraße 137" erfolgt:
 Der Buchstabe A wird mit dem ersten Zeichen der Chiffrierzahl vorwärtsgezählt $A + 3 = t$
 $L + 1 = n$, das erfolgt solange bis die Chiffrierzahl aufgebraucht ist.
 Dann wird wieder mit der 31415... begonnen.

3	1	4	1	5	9	2	6	5	3	5	8	9	7	9	3	2	0	8	4	6	2	6	4	3	0	8	3	2	7	9
A	L	F	R	E	D	K	R	A	U	S	E	S	T	U	T	T	G	A	R	T	W	I	L	H	E	L	M	S	T	R
t	n	p	t	a	w	t	l	c	x	b	t	l	o	i	d	c	g	l	d	n	y	t	q	s	e	x	k	k	o	p

Das Chiffrat wird nicht oder wieder willkürlich getrennt:
TNPTAWTLCXBTLOIDCGLDNYTQSEXKKOP, oder **TNP TAWTL CXBTLOIDC GLD NY TQSE XKKOP**.
 es kann auch standardgemäß in Fünfergruppen gesendet werden:
RNPTA_WTLCW_BTLOI_DCGLD_NYTQS_EXKKO_P

Die Zahlen werden wieder mittels eines Chiffrierwortes gewandelt, dabei muß
 jeder Buchstabe nur einmal auftreten: "**HeilMoskau**".
 Also wird aus der Straßenummer 137 == **HIS**.
 Der gesamte Spruch lautet: **TNPTAWTLCXBTLOIDCGLDNYTQSEXKKOPHIS**

8.3. Das Original Version 2, Autor: Franz. Sammler*17 [Original Version 1 die Modifikation](#)
 "Alberti" Chiffrierschritte

Auch hier wird mit einem Schlüsselwort gearbeitet:

z. B.: **H o l z a r b e i t e r**

Es wird eine Tabelle erstellt in dem in alphabetischer Ordnung untereinander schreibt.

Es ergibt sich aus der Länge des Schlüsselwortes ein 12 x 12 große Tabelle:

RS	1	2	3	4	5	6	7	8	9	10	11	12
1	H	O	L	Z	A	R	B	E	I	T	E	R
2	I	P	M	A	B	S	C	F	K	U	F	S
3	K	Q	N	B	C	T	D	G	L	V	G	T
4	L	R	O	C	D	U	E	H	M	W	H	U
5	M	S	P	D	E	V	F	I	N	X	I	V
6	N	T	Q	E	F	W	G	K	O	Y	K	W
7	O	U	R	F	G	X	H	L	P	Z	L	X
8	P	V	S	G	H	Y	I	M	Q	A	M	Y
9	Q	W	T	H	I	Z	K	N	R	B	N	Z
10	R	X	U	I	K	A	L	O	S	C	O	A
11	S	Y	V	K	L	B	M	P	T	D	P	C
12	T	Z	W	L	M	C	N	Q	U	E	Q	B

Auch hier hat der Fehlerteufel beim Autor zugeschlagen
Zeile 11 und 12 Spalte 12, die Buchstaben B und C sind vertauscht.

Zitat:

Wollen wir nun chiffrieren, so suchen wir
uns die Buchstaben im angefertigten
Schlüssel und bezeichnen sie durch
Zahlen in folgender Weise:

9/7 10/8 8/11 5/1 2/10
5/9 10/4 11/1 9/3 4/7
3/3 3/8 6/4 2/12 5/5
3/6 7/10

9/7 bedeutet also 9. Reihe, 7. Buchstabe;

10/8 ist 10. Reihe, 8 Buchstabe usw., bei der Entzifferung kommt demnach das Wort KOMMUNISTENGESETZT heraus.

Bei der Anwendung dieses Systems sind folgende Regeln zu beachten:

1. Das Schlüsselwort muß mindestens 10 bis 12 Buchstaben enthalten und ist so zu wählen, daß im Schlüssel alle Buchstaben mehrmals vorkommen, so daß genügend Spielraum zur Auswahl der Buchstaben vorhanden ist.

2. Der Schlüssel muß unbedingt jedesmal zum Chiffrieren so wie zum Dechiffrieren neu angefertigt werden und ist sofort nach dem Gebrauch zu vernichten.

Bei einem ähnlichen System benutzt man als Schlüssel die vereinbarte Seite eines vereinbarten Buches.

Die Seite wird entweder von vornherein fest verabredet, oder sie steht in einem Verhältnis zum Datum der chiffrierten Mitteilung. Ist z. B. die Mitteilung mit dem 24. datiert, so gilt die Seite 24 oder eine verabredete Anzahl Seiten weiter.

Bei der Auswahl der Buchstaben verfährt man ähnlich wie bei dem vorher beschriebenen System. Auch hat das noch den Vorteil, daß zur Mitteilung ganze Worte verwenden kann. In unserem Beispiel nehmen wir den "Oktober", Jahrgang 5, Nr. 1, und zwar Seite 22.

W e r n e r Berlin
4/19 2/9 4/2 9/5 12/4 1/10 25/2/1

Alexander s t r.

24/13/1 1/5 2/6 5/5

Dieses Beispiel zeigt die kombinierte Anwendung von Buchstaben und Worte.

Die Buchstaben sind der vereinbarten Seite entnommen. Bei den Worten ist jedesmal die Seitenanzahl mitanzugeben.

Bei diesem Chiffriersystem wird im Gegensatz zu den vorher beschriebenen

Systemen darauf angewiesen, den Schlüssel (hier also das Schlüsselbuch) zur Hand zu haben, was bei der praktischen Anwendung natürlich ein Nachteil ist. Auch können wir nur solche Genossen dieses Chiffriersystem empfehlen, die über eine größere Anzahl von Büchern verfügen. Daß nicht wie in unserem Beispiel den "Oktober" als Schlüsselbuch benutzt, braucht wohl nicht besonders näher begründet zu werden.

9.1. Die Beschreibung des Operativen Vorgang "Hans" bzw. IMB "Welle" ^{BStU*25}

Beschreibung des Dechiffrieren gefunkter Meldungen:

Es wird gesprochen das Meldungskennzeichen z. B.: 124 124 124
gefolgt von der Zeilenbezeichnung z. B.: 36165 und der
Gruppenanzahl z. B.: 13.

Es werden fünf Einsekundentöne anschließen gesendet und
es folgt die eigentliche Meldung z. B.:

07070 25659 66445 34930 79507 82080 27771 19786 15656 09584 29381 47091
69072 WIEDERHOLE
07070 25659 66445 34930 79507 82080 27771 19786 15656 09584 29381 47091
69072 ENDE.

Jetzt wird im aktuellen Schlüsselheft die entsprechende Zeilenbezeichnung gesucht, es ist immer die erste Nummerngruppe der linken Spalte. Die nächste Zahlengruppe (2. Spalte) wird nun zum Dechiffrieren herangezogen. Beispiel der Dechiffriertabelle:

36158	39920	84927	75423	43124
65448	95367	47077	68398	62530
66253	58366	61286	69623	89479
22781	35802	26913	52697	54330
44896	80954	53014	46519	18061
33050	53202	88903	09695	44661
35924	68811	41070	14781	12935
74853	17191	39250	99372	13425
63338	80660	61262	02957	30867
21344	86559	84002	00850	49681
18677	90931	40678	53304	07913
38391	63768	36076	73238	32353

Programm zum Erstellen der Dechiffriertabelle [Download](#)

Also die Gruppe 39920 ist die erste der folgenden Gruppen zum dechiffrieren des Spruches.

Zum entschlüsseln wird die Addition ohne Übertrag benutzt.

z. B.: 07070

39920 ergibt $0 + 3 = 3$, $7 + 9 = 6$, $0 + 9 = 9$, $7 + 2 = 9$

36990

Spruch:	07070	25659	66445	34930	79507	82080	27771	19786	15656	09584	29381	47091	69072
Schlüssel:	39920	84927	75423	43124	65448	95367	47077	68398	62530	66253	58366	61286	69623
Addition :	36990	09576	31868	77054	34945	77347	64748	77074	77186	65737	77647	08277	28695

Es erfolgt die Wandlung der Zahlen in den Klartext mit der Matrix:

1-A	70-L	80-W	90-/	00-0
2-N	71-Ä	81-M	91-X	01-1
3-R	72-B	82-O	92-Y	02-2
4-E	73-C	83-Ö	93-Z	03-3
5-I	74-D	84-P	94-,	04-4
6-S	75-F	85-Q	95-.	05-5
	76-G	86-T	96-?	06-6
	77-H	87-U	97-!	07-7
	78-J	88-Ü	98-()	08-8
	79-K	89-V	99--	09-9

Spruch:	07070	25659	66445	34930	79507	82080	27771	19786	15656	09584	29381	47091	69072
Schlüssel:	39920	84927	75423	43124	65448	95367	47077	68398	62530	66253	58366	61286	69623
Addition:	36990	09576	31868	77054	34945	77347	64748	77074	77186	65737	77647	08277	28695
Klartext:	RS-0	. G	RAT U	L IE	RE; I	H REG	ED U	L D	H AT	SIC H	G EL	O H	NT .
Klartext:	RS-0	. GRATULIERE;	IHRE	GEDULD	HAT	SICH	GELOHT.						

9.2. Die Beschreibung des Chiffrierverfahren von U.S. Agenten in der VR Polen. Lit.*[Crvptologia](#) Sammler*87

Zur Wandlung des empfangenen Geheimtextes in Zifferntext verwendete der Agent die [persönliche Substitutionstabelle](#).

Im Beispiel von Jan Bury wird der empfangene Geheimtext (GTX): 23565 92822 58625 78523 46655 23155 mit der [Substitutionstafel](#) in Buchstabentext umgewandelt:

23 56 59 28 22 58 62 57 8 58 3 4 66 55 23 1 55
O I D M Q C Y J R C E A A H O K H

Als nächstes wird der Schlüssel zum Dechiffrieren benötigt.
Dieser wird mittels eines Kodebuches, beim Agenten wurde ein
Firmenkatalog festgestellt. In diesem Beispiel wurde ein Versbuch verwendet.
Zum Ermitteln der richtigen Seite werden die Anzahl der Tages,
des Jahres, der Funksendung plus 10 ermittelt.
Ist also der Sendetermin der 24. März 1974 so ergibt das der 83. Tag + 10 = 93.
(31(Jan) + 28(Febr) + 24(März) = 83 + 10 = 93)
Der Tag der Funksendung entspricht der Zeile des Versbuches.
Der so ermittelte Vers, aus Seite 93 Zeile 24, wird jetzt in
ein 10 x 10 Kasten geschrieben:

T A R G E S I N L O
S U N C K A N N K O
S T B A R E Z E I T
V E R L O R E N C E
H E N W E N N E T W
A E I N E W E N I C
E R H A R N L O S E
U R S A C H E V O K
L I E G T B I O C H
E M I E W E N N I N

Abb.: Kasten, der Zeilenweise gefüllt und Spaltenweise ausgelesen wird.

Mittels einer Vigenertabelle wird aus dem GTX und der Spaltenweise
ausgelesenen Buchstaben ein weiterer Zwischentext gebildet.

abcdefghijklmnopqrstuvwxy
a ZYXWVUTSRQPONMLKJIHGFEDCBA
b YXWVUTSRQPONMLKJIHGFEDCBAZ
c XWVUTSRQPONMLKJIHGFEDCBAZY
d WVUTSRQPONMLKJIHGFEDCBAZXY
e VUTSRQPONMLKJIHGFEDCBAZYXW
f UTSRQPONMLKJIHGFEDCBAZYXWV
g TSRQPONMLKJIHGFEDCBAZYXWVU
h SRQPONMLKJIHGFEDCBAZYXWVUT
i RQPONMLKJIHGFEDCBAZYXWVUTS
j QPONMLKJIHGFEDCBAZYXWVUTSR
k PONMLKJIHGFEDCBAZYXWVUTSRQ

l ONMLKJIHGFEDCBAZYXWVUTSRQP
 m NMLKJIHGFEDCBAZYXWVUTSRQPO
 n MLKJIHGFEDCBAZYXWVUTSRQPON
 o LKJIHGFEDCBAZYXWVUTSRQPONM
 p KJIHGFEDCBAZYXWVUTSRQPONML
 q JIHGFEDCBAZYXWVUTSRQPONMLK
 r IHGFEDCBAZYXWVUTSRQPONMLKJ
 s HGFEDCBAZYXWVUTSRQPONMLKJI
 t GFEDCBAZYXWVUTSRQPONMLKJIH
 u FEDCBAZYXWVUTSRQPONMLKJIHG
 v EDCBAZYXWVUTSRQPONMLKJIHGF
 w DCBAZYXWVUTSRQPONMLKJIHGF
 x CBAZYXWVUTSRQPONMLKJIHGFED
 y BAZYXWVUTSRQPONMLKJIHGFEDC
 z AZYXWVUTSRQPONMLKJIHGFEDCB

Abb.: Vigenertabelle zum Entschlüsseln.

GTX: OI DMQCYJRCEAAHOKH
 Kasten: TSSVHAEULEEEABAMEE
 KT: **SZESCXXWXPRZYSZLO**

Der Klartext in Englisch: SIX xx IN x [have] ARRIVED.
 Der Klartext in Deutsch: Sechs xx in x [bin] angekommen.

In einem weiteren Beispiel eines U.S. Agenten in der VR Polen wurde einfacher gearbeitet. Der Klartext wurde in Ziffern umgewandelt, entsprechend der Stellung im Alphabet mit führender Null. (A = 01, B = 02, ... L = 12, .. T = 20)
 Der GTX, Zahlensendung, wird mit einem OTP modula 10 subtrahiert.
 Das Produkt entsprechend der einfachen Zahlenwandlung ergibt den Klartext.
 Beispiel:

57238 72135 62253 45955 77989
 ----- 20727 61223 95033 72948
 ----- 52418 05030 50922 05041
 ? x r e c e i v e d

9.3. Die Beschreibung des Chiffrierverfahren von U.S. Agenten in der UdSSR. [Link*104](#)

95 1100

ДЛЯ РАСШИФРОВКИ

24765	93659	55146	09380	18882	67898	69598
25341	88038	31282	39057	21708	51305	66499
65096	02819	74377	27960	20471	53361	18687
19226	31329	55134	83869	26588	24850	81322
01334	80225	37061	13995	88627	07293	53021
90865	91712	80927	18799	71311	57151	71976
98890	61224	59636	08076	65747	36834	49525
95428	50476	06584	38300	37155	75549	11968
43041	83175	29737	88523	76769	29465	47144
77230	19601	57378	51440	48030	63857	15846
32548	48508	71999	22399	86499	22365	91365
57311	83798	06280	74855	58916	46616	07784
10464	00582	08702	30607	80017	50120	76361
93610	38382	57828	27710	00947	00977	02927
53217	20255	20839	63759	74408	60213	32159
31617	14857	97505	25301	14258	36792	42161
52190	32626	07392	88180	32382	22884	82072
39585	92345	44974	09467	88114	50678	84634
44347	73204	49702	60171	56691	11969	32188
06460	37447	02998	93679	05391	96625	21874
85784	28585	57163	61054	85038	41729	76885
12105	61287	69331	72620	98079	56863	59622
94389	88086	36174	39492	54706	56234	49308
79967	13807	72453	07594	89680	63806	18102
65413	91747	01977	31100	62600	78129	31020
09685	11575	35283	37365	15236	28014	82731
35772	51501	01308	09111	40637	41959	81825
69421	13874	28982	52087	95908	43908	06689
64308	31000	08437	64768	79907	58033	78288
39151	32450	44942	53264	04459	19196	33063
57000	78066	10301	31438	87160	08879	10617
41192	47297	79960	45748	24756	60210	83200
91761	48988	10844	64704	86812	61530	69324
03174	79631	96669	88017	31989	32177	73058
94449	59824	50666	22217	36665	78788	88951
92675	67604	01497	28710	65502	37546	76036
84157	68553	92307	42962	21660	78980	52154
57646	07563	92053	84974	34262	59764	68318
65986	82656	13413	64402	77821	46528	50330
43525	90572	90038	01483	75550	94795	48699

Ausschnitt aus den aufgefundenen Wurmschlüssel.
Die Analyse der Wurmtabellen läßt nichts gutes ahnen.

10.1. Auszug aus der Beschreibung des Doppelwürfel TTS der tschechischen Exilregierung, dokumentiert: [Crypto-World^{*100}](#)

Autor: Jozef Kollár, KMaDG, SvF STU in Bratislava

Chiffre:

- [I](#), TTS
- [II](#), STT
- [VIII](#), TTS
- [IX](#), SP
- [X](#), STP
- [XIII](#), TS
- [EVA](#), TT
- [MARTA](#), SP
- [Ružena](#), SP

Chiffre TTS

Dieser Algorithmus wurde von der tschechischen Exilregierung in London verwendet. Stabskapitän Moravek benutzte den Chiffre TTS. In der Literatur [\[3\]](#) Hanák und [\[5\]](#) Janeček sind die Verfahren beschrieben.

Die Bezeichnung TTS stammt von den Abkürzungen Transposition(T), Substitution(S) und Passwort(P), hier Kennwort. Die Reihenfolge der Buchstaben gibt die Reihenfolge der Verfahren an.

In diesem Fall: Zweifache Transposition (Doppelwürfel) mit anschließender Substitution.

Allgemeine Beschreibung und Beispiele der Chiffrierung

Die folgende Beschreibung bezieht sich auf [\[3\]](#) Janeček. Zur Umsetzung von Kennwörter wurden Bücher vereinbart. Die Auswahl der Kennwörter legt fest das diese 12 Zeichen und in einigen anderen Varianten 17 Zeichen lang sind. Für jeden Tag des Monats wird die Substitutionstabelle verschoben.

Die Liste zur Festlegung der Kennwortlänge, könnte so ausgesehen haben:

1-18-21; 2-14-17 ... 13-15-19 ... 30-16-19; 31-18-15

Die erste Zahl bezieht sich auf den Tag der Verschlüsselung, die zweite und dritte Zahl bestimmt die Länge des Kennwortes der ersten und zweiten Transpositionstabelle.

Die Substitutionstabelle nutzt nicht alle 45 Zeichen des tschechischen Alphabets. Es werden zusätzlich Ziffern 0 bis 9 und vier Sonderzeichen eingesetzt. Die Substitutionstabelle, in seiner Grundform, in Tabelle 1, ist aus der Literatur [\[5\]](#), sowie [\[2\]](#) entnommen.

0	1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---	---

0		A	B	C	Č	D	E	Ě	F	G
1	H	I	J	K	L	M	N	O	P	Q
2	R	Ř	S	Š	T	U	V	W	X	Y
3	Z	Ž	•	?	-	/	1	2	3	4
4	5	6	7	8	9	0				

Tabelle 1: Das tschechische Alphabet mit 45 Zeichen, in der Hauptform.

Die Tabelle 1 entspricht der Substitution für den ersten Tag des Monats.

Wird ein längerer Text verschlüsselt wird dieser geteilt. Die Länge sollte 50 Zeichen haben und mit einem ganzen Wort enden. (Nach authentischen Unterlagen vom 11. 6. 1941, erwähnt in der Literatur [\[5\]](#).)

Zur Trennung wird das Zeichen "/" gesetzt.

Die Teile werden mit Buchstaben gekennzeichnet z. B.: /A ... A/, /B ...

Wobei /A das Ende des ersten Teiles markiert und A/ den Beginn des zweiten Teiles. Usw. usf.

Die Buchstaben die nicht in der Substitutionstabelle enthalten sind, sind entsprechend zu ersetzen. Z. B.: Ā durch A ersetzt, Ď durch D, usw.

Trennungen können mit dem Bindestrich oder anderen Sonderzeichen erfolgen. Um Mißverständnisse zu vermeiden können Leerzeichen durch Bindestriche oder andere Sonderzeichen ersetzt werden.

Als Buch, für das folgende Beispiel, wurde für die Kennwörter "Simon Singh: Book of Code and Chiffre (Ausgabe 2003)" verwendet. Der Text wird verschlüsselt am 13., es wird wie folgt Verfahren. Am 13. des Monats die Zeile 13 auf der Seite 13. Für das Beispiel wurden zwei 12 Zeichen lange Kennwörter für die Transpositionen verwendet.

Kennwort 1: KLADĀM PŘĪBĚH

Kennwort 2: Y O POLITICKŮC

Entsprechend der o.g. Festlegung sind die Kennwörter auf 15 und 19 Zeichen zu erweitern.

Die Buchstaben werden jetzt alphabetisch ausgezählt:
A = 1, 2, 3, B = 4 ...

In diesem Beispiel werden folgende Transpositionstabellen erzeugt:

K	L	A	D	A	M	P	R	I	B	Ě	H	K	L	A
9	11	1	5	2	13	14	15	8	4	6	7	10	12	3

Tabelle 2: Ersten Transpositionstabelle

Y	O	P	O	L	I	T	I	C	K	Y	C	Y	O	P	O	L	I	T
17	9	13	10	7	3	15	4	1	6	18	2	19	11	14	12	8	5	16

Tabelle 3: Zweite Transpositionstabelle

Als Klartext verwenden wir ein Zitat von Seneca (Philosoph):
"Poznáš, že neexistuje nic, oc by se nepokusila lidská odvaha, a i ty sám se staneš divákem i jedním z tech, kdo se pokoušejí o velké věci. Seneca"

Die Übersetzung ins deutsche lautet:
"Sie wissen, dass es etwas gibt, über die sie für die menschliche Mut versucht hatte, und auch sie selbst zu einem Zuschauer und einer derjenigen, die zu großen Dingen versucht werden."

Das Original in Latein:
"Videbis nihil humanae audaciae intemptatum erisque et

spectator et ipse pars magna conantium."

Dieser Text ist zu lang (113 Zeichen ohne Leerzeichen, Komma und Punkt). Daher werden drei Teile gebildet. Leerzeichen werden durch Bindestrichen ersetzt. Verwendet werden nur Buchstaben die in der Substitutionstabelle vorhanden sind.

POZNAŠ-ŽE-NEEXISTUJE-NIC-OC-BY-SE-NEPOKUSILA-LIDSKA/A

A/ODVAHA-A-I-TY-SAM-SE-STANEŠ-DIVAKEM-I-JEDNIM-Z-TECH/B

B/KTO-SE-POKOUŠEJI-O-VELKE-VECI.SENECA

Die Substitutionstabelle wird um 13 Positionen verschoben, siehe Tabelle 1 und Tabelle 4.

0	1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---	---

0		-	/	1	2	3	4	5	6	7
1	8	9	0	A	B	C	Č	D	E	Ě
2	F	G	H	I	J	K	L	M	N	O
3	p	Q	R	Ř	S	Š	T	U	V	W
4	X	Y	Z	Ž	:	?				

Tabelle 4: Die Substitutionstabelle für den 13ten.

Als erstes werden die drei Teile in die erste Transpositionstabelle geschrieben:

9	11	1	5	2	13	14	15	8	4	6	7	10	12	3
P	O	Z	N	A	Š	-	Ž	E	-	N	E	E	X	I
S	T	U	J	E	-	N	I	C	-	O	Č	-	B	Y
-	S	E	-	N	E	P	O	K	U	S	I	L	A	-
L	I	D	S	K	A	/	A							

Teil 1: POZNAŠ-ŽE-NEEXISTUJE-NIC-OČ-BY-SE-NEPOKUSILA-LIDSKA/A

9	11	1	5	2	13	14	15	8	4	6	7	10	12	3
A	/	O	D	V	A	H	A	-	A	-	I	-	T	Y

-	S	A	M	-	S	E	-	S	T	A	N	E	Š	-
D	I	V	A	K	E	M	-	I	-	J	E	D	N	I
M	-	Z	-	T	Ě	C	H	/	B					

Teil 2: A/ODVAHA-A-I-TY-SAM-SE-STANEŠ-DIVAKEM-I-JEDNIM-Z-TĚCH/B

9	11	1	5	2	13	14	15	8	4	6	7	10	12	3
B	/	K	T	O	-	S	E	-	P	O	K	O	U	Š
E	J	I	-	O	-	V	E	L	K	E	-	V	E	C
I	•	S	E	N	E	C	A							

Teil 3: B/KTO-SE-POKOUŠEJI-O-VELKE-VECI.SENECA

Anschließend wird der Text aus der ersten Transpositionstabelle in die zweite Transpositionstabelle übertragen.
 Beginnend mit der Spalte 1 wird diese spaltenweise in die erste Zeile der zweiten Transpositionstabelle übertragen.
 Fortlaufend mit der Spalte 2 usw. usf.

17	9	13	10	7	3	15	4	1	6	18	2	19	11	14	12	8	5	16
Z	U	E	D	A	E	N	K	I	Y	-	-	-	U	N	J	-	S	N
O	S	E	Č	I	E	C	K	P	S	-	L	E	-	L	O	T	S	I
X	B	A	Š	-	E	A	-	N	P	/	Ž	I	O	A				

Transposition 2 Teil 1, aus Transposition 1 Teil 1

17	9	13	10	7	3	15	4	1	6	18	2	19	11	14	12	8	5	16
O	A	V	Z	V	-	K	T	Y	-	I	A	T	-	B	D	M	A	-
-	A	J	I	N	E	-	S	I	/	A	-	D	M	-	E	D	/	S
I	-	T	Š	N	A	S	E	Ě	H	E	M	C	A	-	-	H		

Transposition 2 Teil 2, aus Transposition 1 Teil 2

17	9	13	10	7	3	15	4	1	6	18	2	19	11	14	12	8	5	16
K	I	S	O	O	N	Š	C	P	K	T	-	E	O	E	K	-	-	L
B	E	I	O	V	/	J	•	U	E	-	-	E	S	V	C	E	E	A

Transposition 2 Teil 3, aus Transposition 1 Teil 3

Der Text wird wieder Spaltenweise beginnend mit der Spalte 1 ausgelesen:

IPN-LŽEEEEKK-SSYSPI--TUSBDČŠU-OJOEEANLANCANIZOX--/-EI

YIĚA-M-EATSEA/-/HVNNMDHAA-ZIŠ-MADE-VJTB--K-S-SO-IIAETDC

PU--N/C.-EKEOV-EIEOOSKCSIEVŠJLAKBT-EE

Entsprechend der Vorschrift werden die Buchstaben ersetzt, mittels der Substitutionstabelle [4](#). Die Ziffern werden in Fünfergruppen geschrieben. Nichtabgeschlossene, unvollständige, Fünfergruppen werden willkürlich aufgefüllt mit den Ziffern 5, 6, 7, 8, 9, . Bedingt durch die Art der Substitutionstabelle treten diese nicht so häufig auf.

Die Funksprüche erhalten folgenden Kopf:
Spruchnummer - Zeichenanzahl - Tag.

045-110-13
23302 80126 43181 81825 25013 43441 34301 32301 01363 73414
17163 53701 29242 91818 13282 61328 15132 82342 29400 10102
01182 38473

046-110-13
41231 91301 27011 81336 34181 30201 02223 82828 27172 21313
01422 33501 27131 71801 38243 61401 01250 13401 34290 12323
13183 61715

047-080-13
30370 10128 02154 40118 25192 93801 18231 82929 29342 51534
23183 83524 26132 51436 01181 88591

In der Literatur [\[3\]](#) und [\[5\]](#) wird auf die Aspekte der Dechiffrierung, auch mittels historisch belegten Dokumenten eingegangen.

Literatur:

- [1] Grošek Otokar, Vojvoda Milan, Zajac Pavol: Klasické šifry STU v Bratislave, 2007
- [2] Hanák Vítězslav: Muži a radiostanice tajné války Elli Print, 2002

- [3] Janeček Jirí: Gentlemani (ne)ctou cizí dopisy Books Bonus A, 1998; S. 49 - 60
 [4] Janeček Jirí: Odhalená tajemství šifrovacích klícu minulosti Naše vojsko, 1994; S. 253 - 268
 [5] Janeček Jirí: Válka šifer - výhry a prohry ceskoslovenské vojenské rozvedky (1939-1945) Votobia, 2001

Chiffre II

Chiffre II ist vom Typ STT.

0	1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---	---

0		A	B	C	Č	D	Ď	E	Ě	F
1	G	H	I	J	K	L	M	N	Ň	O
2	P	Q	R	Ř	S	Š	T	Ť	U	V
3	W	X	Y	Z	Ž	•	?	-	/	,
4	:	1	2	3	4	5	6	7	8	9
5	0									

Tabelle 1: Substitutionstabelle mit 50 Zeichen

J	E	M	O	Ž	N	E	J	E	P	R	O	J
4	1	7	9	13	8	2	5	3	11	12	10	6

Erste Transpositionstabelle

V	Ě	T	Š	I	B	E	Z	P	E	C	N	V	Ě	T	Š	I
15	5	13	11	7	1	3	17	10	4	2	9	16	6	14	12	8

Zweite Transpositionstabelle

Klartext:

Cokoliv se přihodí řádnému muži, to ponese s vyrovnanou myslí;
 bude si vědom, že to přišlo z božského ustanovení, podle něhož se
 vše řídí.

Seneca

Hergerichteter Klartext:

COKOLIV-SE-PŘIHODI-ŘADNEMU-MUŽI, TO-
PONESE-S-VYROVNANOU-MYSLI-BUDE-SI/A

A/VEDOM, ŽE-TO-PŘIŠLO-Z-BOŽSKEHO-
USTANOVENI, PODLE-NEHOŽ-SE-VŠE-ŘIDI. SENECA

Substitution des ersten Textes:

03 19 14 19 15 12 29 37 24 07 37 20 23 12 11 19 05 12 37 23
01 05 17 07 16 28 37 16 28 34 12 39 26 19 37 20 19 17 07 24
07 37 24 37 29 32 22 19 29 17 01 17 19 28 37 16 32 24 15 12
37 02 28 05 07 37 24 12 38 01

Substitution des zweiten Textes:

01 38 29 07 05 19 16 39 34 07 37 26 19 37 20 23 12 25 15 19
37 33 37 02 19 34 24 14 07 11 19 37 28 24 26 01 17 19 29 07
17 12 39 20 19 05 15 07 37 17 08 11 19 34 37 24 07 37 29 25
07 37 23 12 05 12 35 24 07 17 07 03 01

Transposition-1 des ersten Zifferntextes:

4	1	7	9	13	8	2	5	3	11	12	10	6
---	---	---	---	----	---	---	---	---	----	----	----	---

0	3	1	9	1	4	1	9	1	5	1	2	2
9	3	7	2	4	0	7	3	7	2	0	2	3
1	2	1	1	1	9	0	5	1	2	3	7	2
3	0	1	0	5	1	7	0	7	1	6	2	8
3	7	1	6	2	8	3	4	1	2	3	9	2
6	1	9	3	7	2	0	1	9	1	7	0	7
2	4	0	7	3	7	2	4	3	7	2	9	3
2	2	2	1	9	2	9	1	7	0	1	1	7
1	9	2	8	3	7	1	6	3	2	2	4	1
5	1	2	3	7	0	2	2	8	0	5	0	7

Transposition-2 des zweiten transponierten Textes:

15	5	13	11	7	1	3	17	10	4	2	9	16	6	14	12	8
----	---	----	----	---	---	---	----	----	---	---	---	----	---	----	----	---

1	3	7	3	4	2	7	1	9	2	2	0	0	7	1	7	1
1	3	7	2	7	0	3	0	7	2	2	1	7	2	7	0	3
1	0	6	3	9	2	8	0	5	1	9	1	3	7	3	2	0
1	1	9	1	4	2	7	1	9	1	4	2	9	0	1	2	5
0	3	9	2	7	1	4	1	5	3	5	3	1	9	0	3	3
7	0	2	3	7	3	4	6	8	3	0	3	4	2	7	0	4
0	5	7	9	1	5	3	7	2	9	1	7	0	7	5	2	5
1	9	1	0	0	7	1	7	1	6	1	9	3	9	1	8	3
2	0	2	4	2	3	0	6	1	7	3	7	2	8			

Kopf der Meldung:

xxx-yyy-zz

xxx Fernschreibnummer
 yyy Anzahl der Zeichen
 zz Tag

037-140-21

11232 00779 93982 14722 26521 13701 15391 61200 30307 22057
 36221 43004 17213 13371 31497 52472 20238 02161 30172 70721
 32999 37784 17222 32911 09197 75184 71211 82321

038-150-21

20221 35732 29450 11373 87443 10221 13396 73301 30590 72709
 27984 79477 10213 05345 30112 33797 97595 82113 23123 90470
 22302 87769 92712 17310 75111 11070 12073 91403 21001 16776

Chiffre VIII

Chiffre VIII ist vom Typ TTS.

Codewort:

C	H	O	B	O	T	N	I	C	A
3	5	8	2	9	0	7	6	4	1

In der Substitutionstabelle werden Ziffern und Zeichen mit eingefügt. Die Ziffern werden in die Spalten entsprechend dem Spaltenkopf eingetragen. Jetzt werden die Felder diagonal gefüllt. Von links nach rechts und von oben nach unten. Beginnend mit A bis Ž und abschließend mit den Interpunktionszeichen.

Substitutionstabelle:

3	5	8	2	9	0	7	6	4	1
---	---	---	---	---	---	---	---	---	---

3	M	/	-	F	Ě	O	O	H	V	1
5	X	N	?	2	G	F	P	P	I	W
8	3	Y	O	!	Y	H	G	-	-	J
2	B	Ř	Z	P	A	Z	I	H	4	R
9	C	5	S	Ž	Q	B	Ž	J	I	R
0	K	Č	C	Š	•	R	C	6	K	J
7	K	L	D	Č	T	:	7	Č	A	L
6	Ě	L	8	E	D	U	,	Ř	D	B
4	T	F	M	M	9	E	V	"	S	E
1	A	U	G	N	N	0	Ě	W	-	Š

Tabelle: Chiffre VIII

Mehrfachersetzungstabelle

A	B	C	Č	D	E	Ě	F	G	H	I	J	K	L	M	N	O
28	68	19	30	57	86	24	90	07	76	64	41	13	35	98	02	79
67	46	14	31	53	85	58	82	29	91	03	75	38	52	89	20	94
33	55	48	12	39	50	97	06	74	61	43	15	18	32	80	27	96

P	Q	R	Ř	S	Š	T	U	V	W	X	Y	Z	Ž	-	:	,
60	47	16	51	83	25	88	22	93	05	08	72	69	40	23	36	54
01		65	62	49	10	37	56	84	21		77	66	44	73		

04	45																		99		
																			71		

Substitutionstabelle nach der Verschiebung
entsprechend dem Schlüssel:

8	2	9	0	7	6	4	1	3	5
---	---	---	---	---	---	---	---	---	---

9	M	/	-	F	Ě	O	O	H	V	1
0	X	N	?	2	G	F	P	P	I	W
7	3	Y	O	!	Y	H	G	-	-	J
6	B	Ř	Z	P	A	Z	I	H	4	R
4	C	5	S	Ž	Q	B	Ž	J	I	R
1	K	Č	C	Š	•	R	C	6	K	J
3	K	L	D	Č	T	:	7	Č	A	L
5	Ě	L	8	E	D	U	,	Ř	D	B
8	T	F	M	M	9	E	V	"	S	E
2	A	U	G	N	N	0	Ě	W	-	Š

Substitution der Interpunktion und Zahlen:

"	•	/	?	!	1	2	3	4	5	6	7	8	9	0
81	17	92	09	70	95	00	78	63	42	11	34	59	87	26

Klartext:

Co je nad kámen tvrdší, co nad vodu měkčí být může?
Tvrký však kámen voda měkká vyhloubí přec.

Ovidius

Hergerichteter Klartext:

CO-JE-NAD-KAMEN-TVRDŠI, CO-NAD-VODU-MĚKČI-BYT-MUŽE?
TVRDY-VŠAK-KAMEN-VODA-MĚKKA-VYHLOUBI-PŘEC.OVIDIUS

Einfügen von TER. und ICA. in den Klartext.

ICA sind die letzten drei Buchstaben des Schlüsselwortes CHOBOT**ICA**.

TER ist der Empfänger in Londen.

TER.CO-JE-NAD-KAMEN-TVRDŠI, CO-NAD-VODU-MĚKČI-BYT-MUŽE?
TVRDY-VŠAK-KAMEN-VODA-MĚKKA-VYHLOUBI-PŘEC.OVIDIUS.ICA

Substitution in Zifferntext:

88861 61719 79234 18573 02285 79913 67985 02071 37936 55325
64541 49423 27333 97384 96572 29989 24383 00371 68728 82380
56408 60937 93455 37773 84102 81899 13679 88502 71937 93933
23895 83818 28738 47276 35942 24643 99606 25048 17969 36457
03568 31743 19679

Auffüllung der Fünfergruppen mit zufällig "9"

Chiffrierung Mod(10) mit Passwort: 82907 64135, bzw.
das verschobene umgesetzte CHOBOTNICA.

Text: 88861 61719 79234 18573 02285 79913 67985 02071 37936
Schlüssel: 82907 64135 82907 64135 82907 64135 82907 64135 82907
Nachricht: 60768 25844 51131 72608 84182 33048 49882 66106 19833

Text: 55325 64541 49423 27333 97384 96572 29989 24383 00371
Schlüssel: 64135 82907 64135 82907 64135 82907 64135 82907 64135
Nachricht: 19450 46448 03558 09230 51419 78479 83014 06280 64406

Text: 68728 82380 56408 60937 93455 37773 84102 81899 13679
Schlüssel: 82907 64135 82907 64135 82907 64135 82907 64135 82907
Nachricht: 40625 46415 38305 24062 75352 91808 66009 45924 95476

Text: 88502 71937 93933 23895 83818 28738 47276 35942 24643
Schlüssel: 64135 82907 64135 82907 64135 82907 64135 82907 64135
Nachricht: 42637 53834 57068 05792 47943 00635 01301 17849 88778

Text: 99606 25048 17969 36457 03568 31743 19679
Schlüssel: 82907 64135 82907 64135 82907 64135 82907
Nachricht: 71503 89173 99866 90582 85465 95878 91576

Das zufällige Indikatorzeichen am Anfang: 98xxx wird aufgefüllt
mit drei zufälligen Zahlen.

Das Indikatorzeichen am Ende erfolgt aus der Berechnung:
 $9 + 8 \text{ Mod}(10) = 7$ und $8 + 8 \text{ Mod}(10) = 6$; es wird aufgefüllt mit
drei zufälligen Zahlen.

Gesendet Spruch:

029-225-18

98634 60768 25844 51131 72608 84182 33048 49882 66106 19833
19450 46448 03558 09230 51419 78479 83014 06280 64406 40625
46415 38305 24062 75352 91808 66009 45924 95476 42637 53834
57068 05792 47943 00635 01301 17849 88778 71503 89173 99866
90582 85465 95878 91576 **76102**

Chiffre IX

Chiffre IX ist vom Typ SP

0	1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---	---

0		A	B	C	Č	D	E	Ě	F	G
1	H	I	J	K	L	M	N	O	P	Q
2	R	Ř	S	Š	T	U	V	W	X	Y
3	Z	Ž	-	•	:	,	”	/	?	!
4	1	2	3	4	5	6	7	8	9	0

Substitutionstabelle, 49 Zeichen

Schlüsselwort: Čas je moudřejší zo vřetkřých radcov

Č	A	S	J	E	M	U	D	R	E	J	Š	I	Z	O	V	Š	E	T	K	Y	C	H	R	A	D	C	O	V
5	1	21	13	8	16	25	6	19	9	14	22	12	29	17	26	23	10	24	15	28	3	11	20	2	7	4	18	27

Verschiebung des Schlüsselwortes:

U	D	R	E	J	Š	I	Z	O	V	Š	E	T	K	Y	C	H	R	A	D	C	O	V	Č	A	S	J	E	M
25	6	19	9	14	22	12	29	17	26	23	10	24	15	28	3	11	20	2	7	4	18	27	5	1	21	13	8	16

Klartext:

Smrti nikdo nemůžē uniknout, avřak zbabělřý útěk před smrtí je horří než sama smrt. Cicero

SMRTI NIKTO NEMUŽE UNIKNOUT, AVřAK ZBABELY UTEK/A
A/PRED SMRTI JE HORřI NEŽ SAMA SMRT. CICERO.UDR

UDR ist der Indikator für die erste Folge des verschobenen Schlüsselwortes.
Sowie ein Indikator für die folgende doppelte Verschlüsselung.

Substitution in Zifferntext:

22152 02411 61611 13241 77160 61525 31068 25161 11316 17252
43501 26230 11363 00201 02071 42972 52406 13370 **17867**

01371 82106 05822 15202 41161 20671 01720 23118 16063 16220
11501 72215 20243 30311 03062 01733 25052 **08667**

Gruppe 7867 und 8667 sind Auffüllungen.

Für die anschließende Chiffrierung ist der Schlüssel das verschobene Schlüsselwort.

Chiffriert:

Teil 1:

Text: 2 2 1 5 2 0 2 4 1 1 6 1 6 1 1
Schlüssel: 2 5 6 1 9 9 1 4 2 2 1 2 2 9 1
Nachricht: 4 7 7 6 1 9 3 8 3 3 7 3 8 0 2

Text: 1 3 2 4 1 7 7 1 6 0 6 1 5 2 5
Schlüssel: 7 2 6 2 3 1 0 2 4 1 5 2 8 3 1
Nachricht: 8 5 8 6 4 8 7 3 0 1 1 3 3 5 6

Text: 3 1 0 6 8 2 5 1 6 1 1 1 3 1 6
Schlüssel: 1 2 0 2 7 4 1 8 2 7 5 1 2 1 1
Nachricht: 4 3 0 8 5 6 6 9 8 8 6 2 5 2 7

Text: 1 7 2 5 2 4 3 5 0 1 2 6 2 3 0
Schlüssel: 3 8 1 6 2 5 6 1 9 9 1 4 2 2 1
Nachricht: 4 5 3 1 4 9 9 6 9 0 3 0 4 5 1

Text: 1 1 3 6 3 0 0 2 0 1 0 2 0 7 1
Schlüssel: 2 2 9 1 7 2 6 2 3 1 0 2 4 1 5
Nachricht: 3 3 2 8 0 2 6 4 3 2 0 4 4 8 6

Text: 4 2 9 7 2 5 2 4 0 6 1 3 3 7 0
Schlüssel: 2 8 3 1 1 2 0 2 7 4 1 8 2 7 5

Nachricht: 6 0 2 8 3 7 2 6 7 0 2 1 5 4 5

Text: 1 7 8 6 7

Schlüssel: 1 2 1 1 3

Nachricht: 2 9 9 7 0

Teil 2:

Text: 0 1 3 7 1 8 2 1 0 6 0 5 8 2 2

Schlüssel: 2 5 6 1 9 9 1 4 2 2 1 2 2 9 1

Nachricht: 2 6 9 8 0 7 3 5 2 8 1 7 0 1 3

Text: 1 5 2 0 2 4 1 1 6 1 2 0 6 7 1

Schlüssel: 7 2 6 2 3 1 0 2 4 1 5 2 8 3 1

Nachricht: 8 7 8 2 5 5 1 3 0 2 7 2 4 0 2

Text: 0 1 7 2 0 2 3 1 1 8 1 6 0 6 3

Schlüssel: 1 2 0 2 7 4 1 8 2 7 5 1 2 1 1

Nachricht: 1 3 7 4 7 6 4 9 3 5 6 7 2 7 4

Text: 1 6 2 2 0 1 1 5 0 1 7 2 2 1 5

Schlüssel: 3 8 1 6 2 5 6 1 9 9 1 4 2 2 1

Nachricht: 4 4 3 8 2 6 7 6 9 0 8 6 4 3 6

Text: 2 0 2 4 3 3 0 3 1 1 0 3 0 6 2

Schlüssel: 2 2 9 1 7 2 6 2 3 1 0 2 4 1 5

Nachricht: 4 2 1 5 0 5 6 5 4 2 0 5 4 7 7

Text: 0 1 7 3 3 2 5 0 5 2 0 8 6 6 7

Schlüssel: 2 8 3 1 1 2 0 2 7 4 1 8 2 7 5

Nachricht: 2 9 0 4 4 4 5 2 2 6 1 6 8 3 2

Zyklisch überschlüsselt mit 5699422976,
aus der Folge **256199142212291726**
das entspricht der Anfangsfolge UDREJŠIZOV

Teil 1:

Text: 4 7 7 6 1 9 3 8 3 3 7 3 8 0 2

Schlüssel: 5 6 9 9 4 2 2 9 7 6 5 6 9 9 4

Nachricht: 9 3 6 5 5 1 5 7 0 9 2 9 7 9 6

Text: 8 5 8 6 4 8 7 3 0 1 1 3 3 5 6

Schlüssel: 2 2 9 7 6 5 6 9 9 4 2 2 9 7 6

Nachricht: 0 7 7 3 0 3 3 2 9 5 3 5 2 2 2

Text: 4 3 0 8 5 6 6 9 8 8 6 2 5 2 7

Schlüssel: 5 6 9 9 4 2 2 9 7 6 5 6 9 9 4

Nachricht: 9 9 9 7 9 8 8 8 5 4 1 8 4 1 1

Text: 4 5 3 1 4 9 9 6 9 0 3 0 4 5 1

Schlüssel: 2 2 9 7 6 5 6 9 9 4 2 2 9 7 6

Nachricht: 6 7 2 8 0 4 5 5 8 4 5 2 3 2 7

Text: 3 3 2 8 0 2 6 4 3 2 0 4 4 8 6

Schlüssel: 5 6 9 9 4 2 2 9 7 6 5 6 9 9 4

Nachricht: 8 9 1 7 4 4 8 3 0 8 5 0 3 7 0

Text: 6 0 2 8 3 7 2 6 7 0 2 1 5 4 5

Schlüssel: 2 2 9 7 6 5 6 9 9 4 2 2 9 7 6

Nachricht: 8 2 1 5 9 2 8 5 6 4 4 3 4 1 1

Text: 2 9 9 7 0

Schlüssel: 5 6 9 9 4

Nachricht: 7 5 8 6 4

Teil 2:

Text: 2 6 9 8 0 7 3 5 2 8 1 7 0 1 3

Schlüssel: 5 6 9 9 4 2 2 9 7 6 5 6 9 9 4

Nachricht: 7 2 8 7 4 9 5 4 9 4 6 3 9 0 7

Text: 8 7 8 2 5 5 1 3 0 2 7 2 4 0 2

Schlüssel: 2 2 9 7 6 5 6 9 9 4 2 2 9 7 6

Nachricht: 0 9 7 9 1 0 7 2 9 6 9 4 3 7 8

Text: 1 3 7 4 7 6 4 9 3 5 6 7 2 7 4

Schlüssel: 5 6 9 9 4 2 2 9 7 6 5 6 9 9 4

Nachricht: 6 9 6 3 1 8 6 8 0 1 1 3 1 6 8

Text: 4 4 3 8 2 6 7 6 9 0 8 6 4 3 6

Schlüssel: 2 2 9 7 6 5 6 9 9 4 2 2 9 7 6

Nachricht: 6 6 2 5 8 1 3 5 8 4 0 8 3 0 2

Text: 4 2 1 5 0 5 6 5 4 2 0 5 4 7 7

Schlüssel: 5 6 9 9 4 2 2 9 7 6 5 6 9 9 4

Nachricht: 9 8 0 4 4 7 8 4 1 8 5 1 3 6 1

Text: 2 9 0 4 4 4 5 2 2 6 1 6 8 3 2
 Schlüssel: 2 2 9 7 6 5 6 9 9 4 2 2 9 7 6
 Nachricht: 4 1 9 1 0 9 1 1 1 0 3 8 7 0 8

Umsetzung der Zifferntexte in Buchstabentexte:

Substitutionstabelle mit dem Kennwort:

Čas je mûdřejší zo vřetkûých radcov

1	2	3	4	5	6	7	8	9	0
---	---	---	---	---	---	---	---	---	---

C	A	S	J	E	M	U	D	R	I
Z	O	V	T	K	Y	H	B	F	G
L	N	P	Q	W	X				

Umsetzung des Chiffprat in Buchstabentext:

Teil 1:

Chiffre: 9 3 6 5 5 1 5 7 0 9 2 9 7 9 6
 Text: R S M E K C W U I F A R H F Y

Chiffre: 0 7 7 3 0 3 3 2 9 5 3 5 2 2 2
 Text: G U H V I P S O R E V K N A O

Chiffre: 9 9 9 7 9 8 8 8 5 4 1 8 4 1 1
 Text: F R F U R D B D W J Z B T L C

Chiffre: 6 7 2 8 0 4 5 5 8 4 5 2 3 2 7
 Text: X H N D G Q E K B J W A P O U

Chiffre: 8 9 1 7 4 4 8 3 0 8 5 0 3 7 0
 Text: D F Z H T Q B S I D E G V U I

Chiffre: 8 2 1 5 9 2 8 5 6 4 4 3 4 1 1
 Text: B N L K R A D W M J T P Q C Z

Chiffre: 7 5 8 6 4
 Text: H E B Y J

Teil 2:

Chiffre: 7 2 8 7 4 9 5 4 9 4 6 3 9 0 7

Text: U A D H J R E T F Q M S R I U

Chiffre: 0 9 7 9 1 0 7 2 9 6 9 4 3 7 8

Text: G F H R C I U O F Y R J V H B

Chiffre: 6 9 6 3 1 8 6 8 0 1 1 3 1 6 8

Text: X F M P Z D Y B G L C S Z X D

Chiffre: 6 6 2 5 8 1 3 5 8 4 0 8 3 0 2

Text: M Y N K B L V W D T I B P G A

Chiffre: 9 8 0 4 4 7 8 4 1 8 5 1 3 6 1

Text: R D I Q J U B T C D E Z S X L

Chiffre: 4 1 9 1 0 9 1 1 1 0 3 8 7 0 8

Text: Q C F Z G R L C Z I V B H G D

Fernschreibkopf:

cccce pppdd hhMMD Dtttt

cccc FsNr.

e Füllzeichen oder

Versand mit einem oder zwei regelmäßige Schlüsselwort

ppp Fünfer-Gruppenzahl

dd Chiffrierdatum

hh Anzahl der Verschiebung des Schlüsselwortes.

MMDD Monat/Tag -Sendetag-

tttt Uhrzeit, 24 Stundenangabe

Fernschreibende ist die Folge rückwärts angefügt.

ttttD DMMhh ddppp ecccc

Fernschreibkopf für Text 1 und 2

03163 02709 25081 31800

03171 02609 25081 31800

Fernschreibende für Text 1 und 2

00813 18052 90720 36130

00813 18052 90620 17130

Die vollständige Meldung lautet:

03163 02709 25081 31800 47761 93833 73802 85864 87301 13356
43085 66988 62527 45314 99690 30451 33280 26432 04486 60283
72670 21545 29970 00813 18052 90720 36130

03171 02609 25081 31800 26980 73528 17013 87825 51302 72402
13747 64935 67274 44382 67690 86436 42150 56542 05477 29044
45226 16832 00813 18052 90620 17130

in Buchstabentexten:

ISCMA IAUGR OEIDZ VLBGI RSMEK CWUIF ARHFY GUHVI PSORE VKNAO
FRFUR DBDWJ ZBTLC XHNDG QEKBJ WAPOU DFZHT QBSID EGVUI BNLKR
ADWMJ TPQCZ HEBYJ IGBLV ZDIEO RGUAI AMCSI

ISCUJ IAMGR OEIDZ VLBGI UADHJ RETFQ MSRIU GFHRC IUOFY RJVHB
XFMPZ DYBGL CSZXD MYNKB LVWDT IBPGA RDIQJ UBTC D EZSXL QCFZG
RLCZI VBHGD IGBLV ZDIEO RGMAI JUCSI

Chiffre X

Chiffre X ist vom Typ STP

Substitutionstabelle 49

0	1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---	---

0		A	B	C	Č	D	E	Ě	F	G
1	H	CH	I	J	K	L	M	N	O	P
2	Q	R	Ř	S	Š	T	U	V	W	X
3	Y	Z	Ž	•	:	,	”	/	?	-
4	1	2	3	4	5	6	7	8	9	0

Schlüsselwort:

Nikto nežije bez viny

N	I	K	T	O	N	E	Ž	I	J	E	B	E	Z	V	I	N	Y
10	5	9	14	13	11	2	18	6	8	3	1	4	17	15	7	12	16

																				9
																				14
																				13
																				11
																				2

Spaltenweise auslesen der Ziffern, beginnend mit Spalte 1 usw.usv.

13910 10210 13252 61801 05404 71122 61178 07559 01501 80016
02072 86352 70616 11174 81172 39966 10303 68112 15559 67511
11132 11015 10821 24146 21013

73105 10108 92320 78001 91120 60110 60311 35245 18821 63511
17551 70037 07391 82234 26561 63270 01266 50217 08600 10561
38027 21253 61052

Überschlüsseln der Ziffern mit dem zweiten Schlüsselwort:

Chiffre: 13910 10210 13252 61801 05404 71122 61178 07559 01501
Schlüssel: 18683 14171 57121 61059 14131 12186 83141 71571 21610
Nachricht: 21593 24381 60373 22850 19535 93208 44219 78020 22111

Chiffre: 80016 02072 86352 70616 11174 81172 39966 10303 68112
Schlüssel: 59141 31121 86831 41715 71216 10591 41311 21868 31417
Nachricht: 39157 33193 62183 11321 82380 91663 70277 31161 99529

Chiffre: 15559 67511 11132 11015 10821 24146 21013
Schlüssel: 15712 16105 91413 11218 68314 17157 12161
Nachricht: 20261 73616 02545 22223 78135 31293 33174

Teil 2:

Chiffre: 73105 10108 92320 78001 91120 60110 60311 35245 18821
Schlüssel: 18683 14171 57121 61059 14131 12186 83141 71571 21610
Nachricht: 81788 24279 49441 39050 05251 72296 43452 06716 39431

Chiffre: 63511 17551 70037 07391 82234 26561 63270 01266 50217
Schlüssel: 59141 31121 86831 41715 71216 10591 41311 21868 31417
Nachricht: 12652 48672 56868 48006 53440 36052 04581 22024 81624

Chiffre: 08600 10561 38027 21253 61052

Schlüssel: 15712 16105 91413 11218 68314

Nachricht: 13312 26666 29430 32461 29366

Am Ende der Meldung wird z. B. das Datum und die Uhrzeit der nächsten Sendung kodiert und verschlüsselt.

Sowie eine evtl. Warnung.

Erste Zeile: Tag und Uhrzeit

Zweite Zeile: zwei Zahlen bilden Modulo 10 die Zahl in der ersten Zeile
z. B. $7 + 5 \text{ Mod}(10) = 2$, $9 + 8 \text{ Mod}(10) = 7$, Tag **27**

Dritte Zeile: ersten 3 Codegruppen des verschlüsselten Textes

Diese drei Gruppen signalisiert auch eine Warnung, ob die Meldung ohne "Druck" erzeugt wurde. D. h. der Agent war arritiert.
In diesem Fall wird eine "0" in der Meldung erscheinen.

Nachricht 1:

Tag, Uhrzeit: 2 7 1 1 3 0
Zvolené cifry: 7 5 9 8 0 6 5 8 3 6 7 5 5 1 4
Codegruppe 1-3: 2 1 5 9 3 2 4 3 8 1 6 0 3 7 3
Nachricht: 9 6 4 7 3 8 9 1 1 7 3 5 8 8 7

Hier wird ein "0" Alarm gesetzt:

Nachricht 2:

Tag, Uhrzeit: 2 7 1 1 3 0
Zvolené cifry: 6 6 5 2 3 4 7 2 9 5 8 2 8 5 3
Codegruppe 1-3: 8 1 7 8 8 2 4 2 7 9 4 9 4 4 1
Nachricht: 4 7 2 **0** 1 6 1 4 6 4 2 1 2 9 4

Gesendeter Text:

017-140-14

21593 24381 60373 22850 19535 93208 44219 78020 22111 39157
33193 62183 11321 82380 91663 70277 31161 99529 20261 73616
02545 22223 78135 31293 33174 96473 89117 35887

018-130-14

81788 24279 49441 39050 05251 72296 43452 06716 39431 12652
48672 56868 48006 53440 36052 04581 22024 81624 13312 26666
29430 32461 29366 47201 61464 21294

Chiffre XIII

mit der Tabelle "W":

.	:	,	-	/	!	?	0	1	2	3	4	5	6	7	8	9
WA	WB	WC	WD	WE	WF	WG	WH	WI	WJ	WK	WL	WM	WN	WO	WP	WQ

Das Schlüsselwort lautet, Zitat Umberto Eco (1932):

Ak je pravý nepriateľ príliš silný,
je potrebné nájsť si slabšieho.

Das Schlüsselwort wird gebildet durch die Verschiebung, entsprechend dem Datum. Es wird keine Interpunktion und Leerzeichen verwendet.

riateľ príliš silný je potrebné nájsť si slabšieho Ak je pravý nep

Die zu versendende Nachricht:

V chmurných dňoch roku 1940 jsme stáli zády ke zdi,
střežice pobřeží.

Der hergerichtete Klartext lautet:

VXXCHMURNYCHQQDNECHXXROKUQQWIWQWLWHXXJSMEQQS
TALIXXZADYQQKEXXZDIWCSTRREZZICEQQPOBRREZZIWA

Die mit dem Schlüsselwort und dem hergerichteten Klartext gefüllte
Transpositionstabelle:

Form 8																
--------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

R	I	A	T	E	L	P	R	I	L	I	S	S	I	L	N	Y	J	E	P	O	T	R	E
17	5	1	22	2	10	15	18	6	11	7	20	21	8	12	13	24	9	3	16	14	23	19	4

V	X	X	C	H	M	U	R	N	Y	C	H	Q	Q	D	N	E	C	H	X	X	R	O	K
								U	Q	Q	W	I	W	Q	W								
L	W	H	X	X	J	S	M	E	Q	Q	S	T	A	L	I	X	X	Z	A	D	Y	Q	Q
									K	E	X	X	Z	D	I	W							
C	S	T	R	R	E	Z	Z	I	C	E	Q	Q	P	O	B	R	R	E	Z	Z	I	W	A

Auslesen des Textes entsprechend der Transpositionstabelle:

XHTHX RHZEK QAXWS NUEIC QQEEQ WAZPC XRMJE YQQKC DQLDO NWIIB
 XDZUS ZXAZV LCRMZ OQWHW SXQQI TXQCX RRYIE XWR

Setzen einer Indikatorgruppe an den Anfang des Spruches.
 Die Indikatorgruppe setzt sich zusammen aus den ersten beiden
 Buchstaben des Schlüsselwortes sowie dessen letzten Buch-
 staben und die letzten beiden Buchstaben des Klartextes:

RI E WA

RIEWA XHTHX RHZEK QAXWS NUEIC QQEEQ WAZPC XRMJE YQQKC DQLDO
 NWIIB XDZUS ZXAZV LCRMZ OQWHW SXQQI TXQCX RRYIE XWR

Auffüllen der Fünfergruppen.
 Hier erfolgt die Auffüllung mit der Kennung der Tabelle die
 angewendet wurde. In diesem Fall WP = 8.

RIEWA XHTHX RHZEK QAXWS NUEIC QQEEQ WAZPC XRMJE YQQKC DQLDO
 NWIIB XDZUS ZXAZV LCRMZ OQWHW SXQQI TXQCX RRYIE XWRWP

Die abschließende Substitution wird wieder mit dem Schlüssel-
 wortdurchgeführt. Die Zeilen 1 bis 5 kann als gesonderter
 Schlüssel behandelt werden.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

1	A	K	J	E	P	R	V	Y	N	I	T	L	S	O	B	H	M	Q	U	W	X	Z	C	D	F	G
2	K	J	E	P	R	V	Y	N	I	T	L	S	O	B	H	M	Q	U	W	X	Z	C	D	F	G	A
3	J	E	P	R	V	Y	N	I	T	L	S	O	B	H	M	Q	U	W	X	Z	C	D	F	G	A	K
4	E	P	R	V	Y	N	I	T	L	S	O	B	H	M	Q	U	W	X	Z	C	D	F	G	A	K	J
5	P	R	V	Y	N	I	T	L	S	O	B	H	M	Q	U	W	X	Z	C	D	F	G	A	K	J	E

Zu sendender Text nach der letzten Substitution:

045-095-13
 QIVGP DNZTK QNKYB MKGGC OZVLV MQVYX CKKUV DUBSN FQUOV EQOVU
 ODTLR DPKDC GFJJG LPWHE BQFTA UFUWS WFURK QUALN DDWGW

Dadurch das alle Indikatoren verschlüsselt sind kann erst im Entschlüsselungsprozeß ermittelt werden ob der Bearbeiter unter "Druck" gearbeitet hat.

Chiffre EVA

Das Chiffre EVA ist eine TT-Chiffrierung. Transposition-Transpositon.

Die Klartextzeichen erhalten keine weitere Wandlung, außer das sie in 26 Buchstaben des lateinischen Alphabet umgesetzt werden.

Als Trennzeichen wird das Paar QQ oder XX verwendet.

Substitution von Ziffern und Zeichen erfolgt mit der Tabelle "W":

.	:	,	-	/	!	?	0	1	2	3	4	5	6	7	8	9
WA	WB	WC	WD	WE	WF	WG	WH	WI	WJ	WK	WL	WM	WN	WO	WP	WQ

Klartext: Snaž se, abys nikdy nic nedělal proti vůli.

Ktxt: SNAZ SE,ABYS NIKDY NIC NEDLAL PROTI SVE VULI.

hKtxt: SNAZXXSEWCABYSQQNIKDYYXXNICQQNEDLALXXPROTIQQSVEXXVULIWA

Die Länge des Schlüsselwortes und die Paramter des Dreieck wird wie folgt berechnet:

- d = die Schlüssellänge
- k = die Klartextelänge
- n = die Hühe des Dreiecks

Zu Beachten ist: $k \leq n^2$, bzw. $n \geq \sqrt{k}$ oder $= k^{1/2}$

$$d = 2n - 1$$

es ergibt sich in diesem Fall

$$k = 65, n \geq \sqrt{65} = 8,1$$

n muß also mindestens 9 betragen.

$$d = 2n - 1 = 2 * 9 - 1 = 17$$

$$d = 17, n = 9$$

Schlüsselwort: M A S I R U J E A J E N O G A L A

Transpostionsfolge: 13 1 16 9 15 17 10 5 2 11 6 8 14 7 3 12 4

Der hKtXt beginnt mit dem Anfang des Schlüsselwortes MAS und dem Ende des Klartextes: WA
 Am Ende des hKtXt wird MAS in umgekehrter Reihenfolge angefügt sowie ein vereinbartes Kürzel zu SAMVY

Auffüllen des Transpositions-Dreieck mit dem Klartext:

										M														
										A	S	W												
										A	S	N	A	Z										
										X	X	S	E	W	C	A								
										B	Y	S	Q	Q	N	I	K	D						
										Y	X	X	N	I	C	Q	Q	N	E	T				
										E	L	A	L	X	X	P	R	O	T	I	Q	Q		
										S	V	E	X	X	V	U	L	I	W	A	S	A	M	V
Y																								
13	1	16	9	15	17	10	5	2	11	6	8	14	7	3	12	4								

Im nächsten Schritt wird das Dreieck spaltenweise ausgelesen und in die nächste Transpositionstabelle zeilenweise eingetragen:

13	1	16	9	15	17	10	5	2	11	6	8	14	7	3	12	4
----	---	----	---	----	----	----	---	---	----	---	---	----	---	---	----	---

S	L	P	C	Q	E	N	S	M	M	Q	U	X	I	Q	S	S
A	W	O	Q	I	C	Z	A	Q	D	A	T	N	K	A	E	L
Y	V	X	N	S	X	A	I	R	Q	N	W	A	W	V	Y	S
I	E	D	X	A	X	B	V	E	X	L	X	Y	X			

Das Ergebnis der zweiten Transposition wird wieder Spaltenweise ausgelesen:

LWVEM QREQA VSLSS AIVQA NLIKW YUTWX CQNXN ZABMD QXSEY SAYIX
 NAYQI SAPOX DECXX

Vor den Spruch wird die Gruppenanzahl, die Kennung und die Kenngruppen gesetzt, sowie am Ende die Dienstgruppe (Kenngruppe):

Die Kenngruppe besteht aus dem ersten Zeichen des Schlüsselwortes,

der laufenden Spruchnummer 21 = WJWI, der Höhe des Dreiecks 09 = WHWQ und einem zufällig gewählten Buchstaben.

MWJWI WHWQD

017 GR

MWJWI WHWQD LWVEM QREQA VSLSS AIVQA NLIKW YUTWX CQNXN ZABMD
 QXSEY SAYIX NAYQI SAPOX DECXX MWJWI WHWQD

Chiffre MARTA

Klartext: Ostatně se domívám, že je potřeba zničit Kartágo.

Leerzeichen werden mit 7,8,9 substituiert.

Substitutionstabelle 49

0	1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---	---

0		A	B	C	Č	D	E	Ě	F	G
1	H	CH	I	J	K	L	M	N	O	P
2	Q	R	Ř	S	Š	T	U	V	W	X
3	Y	Z	Ž	•	:	,	”	/	?	-
4	0	1	2	3	4	5	6	7	8	9

hKtxt: OSTATNĚ SE DOMNIVAM, ŽE JE POTREBA ZNIČIT KARTAGO.

Substituiert:

18232 50125 17077 23068 05181 61712 27011 63532 06913 06719
 18252 10602 01831 17120 41225 91401 21250 10918 33

Der hergerichtete Klartext wird aufgefüllt mit zufällig gewählten Elementen 7,8 und 9.

Es gibt 2 Schlüsselsätze, -wörter, das vom 1. bis 15. und das ab 16. bis 31. gültig ist.

1. Aj, zde leží **zem ta před okem mým slzy** ronícím.
2. Dříve **kolébka, nyní národu máho** rakev.

Schlüsselwort, ausgezählt entsprechend seiner Stellung im Alphabet:

Z E M T A P Ř E D O K E M M Y M S L Z Y
 19 3 8 16 1 13 14 4 2 12 6 5 9 10 17 11 15 7 20 18

Der Schlüssel bildet den Anfang der Schlüsselreihe,
 die nachfolgenden Ziffern sind die Ergebnisse der Chiffrierung.

hKtxt: 18232 50125 17077 23068 05181 61712 27011 63532 06913 06719
 Schlüssel: **19381 61131 44212 65910 17111 57201 82751 31125 65128 98897**
 GTX: 27513 11256 51289 88978 12292 18913 09762 94657 61031 94506

hKtxt: 18252 10602 01831 17120 41225 91401 21250 10918 33978
 Schlüssel: 81229 21891 30976 29465 76103 19450 69947 13149 33170
 GTX: 99471 31493 31707 36585 17328 00851 80197 23057 66048

Spruchkopf: FsNr. - Wortzahl - Datum

054-095-10

27513 11256 51289 88978 12292 18913 09762 94657 61031 94506
 99471 31493 31707 36585 17328 00851 80197 23057 66048

Chiffre Růžena

Klartext:

Jestliže mně dáte šest řádků napsaných rukou toho nejčestnějšího
 muže, já v nich najdu něco za co ho budem moct pověsit.
 Zitat Kardinal Richelieu

Anwendung der Substitutionstabelle Česká 49, Marta/Růžena.

0	1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---	---

0		A	B	C	Č	D	E	Ě	F	G
1	H	CH	I	J	K	L	M	N	O	P
2	Q	R	Ř	S	Š	T	U	V	W	X
3	Y	Z	Ž	•	:	,	”	/	?	-
4	0	1	2	3	4	5	6	7	8	9

Herrgerichteter Klartext (hKtxt):

JESTLIŽE MNĚ DATE ŠEST ŘÁDKU NAPSANÝCH RUKOU TOHO
 NEJČESTNEJŠIHO MUŽE, JA V NICH NAJDU NĚCO ZA CO
 HO BUDEM MOCT POVĚSIT.

Aufteilung des hKtxt in 2 Blöcke:
JESTLIŽE MNĚ DATE ŠEST ŘADKU NAPSANYCH
RUKOU TOHO NEJČESTNEJŠIHO/A

A/MUŽE, JA V NICH NAJDU NĚCO
ZA CO HO BUDEM MOCT POVĚSIT.

Leerzeichen werden fortlaufend aufgefüllt mit 5, 6, 7, 8, 9.

Substituierter Text:

13062 32515 12320 65161 70760 50125 06724 06232 58220 10514
26917 01192 30117 30115 21261 41826 62518 10187 17061 30406
23251 70613 24121 01837 01

01371 62632 06351 30152 76171 21171 70113 05267 17070 31893
10150 31861 01870 22605 06168 16180 32591 91827 07231 22533

Dem ersten Block wird vorangestellt das Datum 23., die 33
steht für den Punkt

Aufgefüllt wird mit zufällig gewählten Zahlen von 5 bis 9.

23331 30623 25151 23206 51617 07605 01250 67240 62325 82201
05142 69170 11923 01173 01152 12614 18266 25181 01871 70613
04062 32517 06132 41210 18370 **15968**

01371 62632 06351 30152 76171 21171 70113 05267 17070 31893
10150 31861 01870 22605 06168 16180 32591 91827 07231 22533

Schlüsselwort gebildet aus den deutschen Wörtern des Datum:
Montag der 23. Die Buchstaben werden entsprechend ihrer
Wertigkeit durchgezählt, A = 1, D = 2 ... Z = 14.

M	O	N	T	A	G	Z	W	E	I	D	R	E	I
8	10	9	12	1	5	14	13	3	6	2	11	4	7

Die Zehner werden weggelassen und daraus wurde gebildet:

8 0 9 2 1 5 4 3 3 6 2 1 4 7

für die Chiffriertabelle 1 und 2.

Chiffrierung:

	Schlüsseltable													
	8	10	9	12	1	5	14	13	3	6	2	11	4	7

10.	2	3	3	3	1	3	0	6	2	3	2	5	1	5
Schl.	7	8	0	9	2	1	5	4	3	3	6	2	1	4
Add.	9	1	3	2	3	4	5	0	5	6	8	7	2	9

9.	1	2	3	2	0	6	5	1	6	1	7	0	7	6
Schl.	4	7	8	0	9	2	1	5	4	3	3	6	2	1
Add.	5	9	1	2	9	8	6	6	0	4	0	6	9	7

8.	0	5	0	1	2	5	0	6	7	2	4	0	6	2
Schl.	8	0	9	2	1	5	4	3	3	6	2	1	4	7
Add.	5	9	1	2	9	8	6	6	0	4	0	6	9	7

7.	3	2	5	8	2	2	0	1	0	5	1	4	2	6
Schl.	0	9	2	1	5	4	3	3	6	2	1	4	7	8
Add.	3	1	7	9	7	6	3	4	6	7	2	8	9	4

6.	9	1	7	0	1	1	9	2	3	0	1	1	7	3
Schl.	5	4	3	3	6	2	1	4	7	8	0	9	2	1
Add.	4	5	0	3	7	3	0	6	0	8	1	0	9	4

5.	0	1	1	5	2	1	2	6	1	4	1	8	2	6
Schl.	6	2	1	4	7	8	0	9	2	1	5	4	3	3
Add.	6	3	2	9	9	9	2	5	3	5	6	2	5	9

4.	6	2	5	1	8	1	0	1	8	7	1	7	0	6
----	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Schl.	9	2	1	5	4	3	3	6	2	1	4	7	8	0
Add.	5	4	6	6	2	4	3	7	0	8	5	4	8	6

3.	1	3	0	4	0	6	2	3	2	5	1	7	0	6
Schl.	4	3	3	6	2	1	4	7	8	0	9	2	1	5
Add.	5	6	3	0	2	7	6	0	0	5	0	9	1	1

2.	1	3	2	4	1	2	1	0	1	8	3	7	0	1
Schl.	1	5	4	3	3	6	2	1	4	7	8	0	9	2
Add.	2	8	6	7	4	8	3	1	5	5	1	7	9	3

1.	5	9	6	8										
Schl.	2	1	4	7	8	0	9	2	1	5	4	3	3	6
Add.	7	0	0	5										

Tab. 1: Block 1

	Schlüsseltable													
	8	10	9	12	1	5	14	13	3	6	2	11	4	7

8.	0	1	3	7	1	6	2	6	3	2	0	6	3	5
Schl.	8	0	9	2	1	5	4	3	3	6	2	1	4	7
Add.	8	1	2	9	2	1	6	9	6	8	2	7	7	2

7.	1	3	0	1	5	2	7	6	1	7	1	2	1	1
Schl.	0	9	2	1	5	4	3	3	6	2	1	4	7	8
Add.	1	2	2	2	0	6	0	9	7	9	2	6	8	9

6.	7	1	7	0	1	1	3	0	5	2	6	8	1	7
Schl.	5	4	3	3	6	2	1	4	7	8	0	9	2	1

Add.	2	5	0	3	7	3	4	4	2	0	6	7	3	8
------	---	---	---	---	---	---	---	---	---	---	---	---	---	---

5.	0	7	0	3	1	8	9	3	1	0	1	5	0	3
Schl.	6	2	1	4	7	8	0	9	2	1	5	4	3	3
Add.	6	9	1	7	8	6	9	2	3	1	6	9	3	6

4.	1	8	6	1	0	1	8	7	0	2	2	6	0	5
Schl.	9	2	1	5	4	3	3	6	2	1	4	7	8	0
Add.	6	0	7	6	4	4	1	3	2	3	6	3	8	5

3.	0	6	1	6	8	1	6	1	8	0	3	2	5	9
Schl.	4	3	3	6	2	1	4	7	8	0	9	2	1	5
Add.	4	9	4	2	0	2	0	8	6	0	2	4	6	4

2.	1	9	1	8	2	7	0	7	2	3	1	2	2	5
Schl.	1	5	4	3	3	6	2	1	4	7	8	0	9	2
Add.	2	4	5	1	5	3	2	8	6	0	9	2	1	7

1.	3	3												
Schl.	2	1	4	7	8	0	9	2	1	5	4	3	3	6
Add.	5	4												

Tab. 2: Block 2

Fernschreibkopf: Datum 23 und Monat 04 aufgefüllt mit einer Zufallszahl 23047, 23042 sowie weiterer Erkennungsgruppen 26234, 27109.

Diese Gruppe wird gebildet aus einer vereinbarten Kenngruppe addiert mit den Tag und Monat:

Tag / Monat /Zufallsz.	23047	23042
FsNr. / Zufallsz.	03297	04167
Erkennungsgruppe	26234	27109

Die Kenngruppe wird gebildet aus der Fs-Nummer 03 und für den folgenden

Block 04 sowie 297 und 167 stellen Zufallszahlen dar.

28 GR

23047 91323 **26234** 45056 87295 91298 66040 69785 93304 90861
09317 97634 67289 44503 73060 81094 63299 92535 62595 46624
37085 48656 30276 00509 11286 74831 55179 37005

22 GR

23042 81292 **27109** 16968 27721 22206 09792 68925 03734 42067
38691 78692 31693 60076 44132 36385 49420 20860 24642 45153
28609 21754

10.2. Doppelwürfel der HV A, NVA und BW, dokumentiert: [1960](#)

Das Doppelwürfelverfahren, auch Doppel-Transposition genannt, es wird behauptet das die nichtquadratische Transposition sicher wäre. Und das die quadratische Transposition leicht zu brechen ist. Das beide nicht sicher sind kann man bei [Klaus Wagner](#), [Markus Wolf](#), [Otto Leiberich](#) und [F.L. Bauer](#) nachlesen.
Hier die Auszüge aus [Wagner](#) und [Wolf](#)

*"Welken muß die Blüte in der Zeiten Flucht.
aber im Gemüte bleibt die reife Frucht"*

Dieses Dichterwort fand man in der Handschrift eines Bonner Journalisten in dessen Notizkalender, als Beamte des Bundeskriminalamtes im Februar 1964 die Wohnung des der geheimdienstlichen Agententätigkeit Verdächtigen durchsuchten. Es war den Entschlüsselungsexperten im Bundesamt für Verfassungsschutz nicht unbekannt, hatten sie doch mit Hilfe amerikanischer Großrechner schon 1961 als den Merksatz eines Agenten ermitteln können, der damit die für ihn bestimmten verschlüsselten Durchsagen im Agentenfunk entschlüsseln konnte. Es war gelungen, das vom MfS bis Ende 1958 verwandte, im Abschnitt über nachrichtendienstliche Hilfsmittel noch näher zu erläuternde "Doppelwürfelverfahren" zu "knacken", außer dem Merksatz auch einzelne - wechselnde - Merkworte zu ermitteln und auf diesem Wege 58 Funksprüche zu dechiffrieren, die in der Zeit vom 26. Oktober 1957 bis zum 19. Dezember 1958 aufgefangen worden waren. Der Inhalt dieser Durchsagen - Glückwünsche zum Geburtstag Anfang September, benannte oder umschrieb Kontaktpersonen, Zugang zum Presseklub und berufliche Tätigkeiten im Raum Bad Kreuznach / Koblenz - wiesen in die Richtung des seit 1961 im Bonner Büro einer Nachrichtenagentur

tätig und für die Bereiche Parlament und Verteidigung zuständigen D.Sch.

...

Verschlüsselung und Entschlüsselung der Sprüche der HV A erfolgten bis Ende 1958 im sogenannten Doppelwürfelverfahren, wie im Fall "Sch." schon geschildert. Es beruhte auf einem für die Mehrzahl von Agenten gültigen Merkwort und einem individuellen, nur an einen einzelnen Mitarbeiter ausgegebenen Merksatz. Mit Hilfe des Merkwortes konnte eine Umsetztabelle gebildet werden, anhand deren Buchstaben in Zahlen, die Ziffern 0 bis 9, umgewandelt wurden. Sodann wurde der Merksatz, nunmehr zur Umwandlung von Zahlen in Buchstaben, in ein Quadrat mit insgesamt 100 Buchstabenfeldern, notfalls mehrere Male hintereinander, eingetragen. Mit Hilfe dieses Quadrats und der darin eingetragenen dritte Gruppe des gesendeten Funkspruchs wurden sodann in einem bestimmten Verfahren eine Schlüsselzahl und zwei sogenannte Lösungen ermittelt, die ihrerseits Ausgangspunkt für die Erstellung zweier "Schlüsselkästen" waren, in deren senkrechte Spalten der Funkspruch eingetragen und anschließend mit der Umsetztabelle zum Klartext entschlüsselt wurde. Ein kompliziertes Verfahren, das sich gleichwohl nicht bewährt hat, denn der westdeutsche Verfassungsschutz konnte, wie erwähnt, darin eindringen. Es wurde deshalb 1959 ... das OTP-Verfahren eingesetzt.

Aus:
Schriftreihe des Fachbereichs Öffentliche Sicherheit
Klaus Wagner "Spionageprozesse"
in Bearbeitung Guido Korte
Brühl bei Köln Mai 2000

In M. Wolfs Buch "Spionagechef im geheimen Krieg" steht auf Seite 269:

Hierzu muß ich erläutern, daß mein Dienst in den 50er Jahren ein sowjetisches Chiffriersystem verwendet hatte, bis wir erfuhren, daß westliche Dienste es mittels EDV geknackt hatten und die Telegramme nicht nur dechiffrierten, sondern sogar nach Empfängern zuordnen konnten. Daraufhin zogen wir das System aus dem Verkehr und überprüften, wieweit unsere Leute in der Bundesrepublik durch von uns versandte Telegramme gefährdet waren.

Im Beispiel 1 wird die quadratische doppelte Transposition beschrieben,

im [Beispiel 2a](#), [2b](#) und [2c](#) wird versucht die nichtquadratische doppelte Transposition darzustellen. Es gibt z.Zt. keine Darstellung der nichtquadratischen doppelten Transposition. Diese ist bei längeren Texten [angeblich](#) schwer oder gar nicht zu brechen sind. Wichtig ist das wenn OTP dazu verwendet wird, das nach Erreichen des Schlüsselendes neue Schlüssel zu benutzen sind!

Beispiel 1:

Vorbereitung:

Dem Chiffrierten Spruch vorangestellt ist z. B. die Nummer des nächstgültigen Spruchschlüssels bzw. Kenngruppe aus einem [Kenngruppen/Spruchschlüsselheftes](#). 15 OWNCEXJWGH, oder 15 294637518. Als verkürzte Form kann je nach Textlänge z. B. ein 5 Zeichen langes Codewort benutzen: CODIE oder 25314. Das Buchstabencodewort muß in Zahlen umgewandelt werden. In: 15243. Sind im Codewort zwei gleiche Buchstaben werden diese fortlaufend weitergezählt: CODIERER ergibt 16253748, in diesem Fall das R ist 7 und nachfolgende R die 8.

Jetzt wird eine Tabelle gebildet anhand der Länge der Kenngruppe/Schlüsselgruppe und gleich darunter der Klartext:

<u>2</u>	<u>9</u>	<u>4</u>	<u>6</u>	<u>3</u>	<u>7</u>	<u>5</u>	<u>1</u>	<u>8</u>
D	A	S	I	S	T	D	E	R
K	L	A	R	T	E	X	T	D
E	R	H	I	E	R	V	E	R
S	C	H	L	U	E	S	X	S
E	L	T	W	E	R	D	E	N
<u>S</u>	<u>O</u>	<u>L</u>	<u>X</u>	<u>L</u>	<u>E</u>	<u>U</u>	<u>O</u>	<u>X</u>

Nun wird entsprechend der Spaltennummerierung das Chifftrat ausgelesen:

1. Spalte: ETEXEO / 2. Spalte: DKESES usw. usf.

ergibt: etexeodkesessteuelsahhtldxvsduirilwxterererdrsnxalrchlo

Spruch übertragen in der Art:

15 04 0396 wostok 944
etexe odkes esste uelsa
hhtld xvsdu irilw xtere
rerdr snxal rchlo
011 soroka 944 013

Spruch-Kenngruppe, Tagesdatum, Spruchnr., Empfänger, Text,
Wort - Gruppenanzahl, Absender, Fs-Platz

Beispiel 2a:

Das Verfahren hat Ähnlichkeit mit dem "Fleißner-Verfahren".

Auch als Raster, Drehraster oder Fleißnerraster

beschrieben, siehe 'Kryptologie' F.L. Bauer.

Im Fleißner-Verfahren wird mit einer gelochten/gestanzten Schablone

eine Tabelle mit dem Klartext gefüllt und die Schablone insgesamt

drei mal gedreht. Leere Felder werden als Blender gefüllt.

Die Transposition wird wie oben beschrieben in einer Tabelle durchgeführt

leere Felder werden mit willkürlichen Füllzeichen aufgefüllt.

Es wird eine leere Tabelle mit 10 x 99 Zeichen gebildet.

Die Position des Klartextzeichens wird mit der Position, der

im Schlüssel vorgegebenen Position, vertauscht.

Im Schlüssel steht:

X 0 1 2 3 4 5 6 7 8 9

00 17 07 49 07 95 36 04 39 39 01

01 49 76 40 06 49 00 ..

02 ..

Der Klartext lautet wie oben: DAS IST DER KLARTEXT

Die leere Tabelle wird jetzt wie folgt gefüllt:

Das "D" steht an Pos. 00/0, im Schlüssel 00/0 steht "17".

Also Zeile 17 Position 0 schreiben wir ein "D".

Das "A" steht an Pos. 00/1, im Schlüssel 00/1 steht "07".

Also Zeile 07 Pos. 1 erscheint jetzt das A.

Hier kann auch die Doppelungen, Zahlen, Zeichen und Leerzeichen

transponieren oder durch vereinbarte Zeichen ersetzt werden.

Zum Dechiffrieren gibt es zur Vereinfachung eine Dechiffriertabelle.

Diese ist "Spiegelgleich" wie die Chiffriertabelle aufgebaut.

An Zeile 17 Pos. 0 müssen Sie die 00 finden.

Also wird das Zeichen aus der Zeile 17 Pos 0 in Zeile 00 Pos 0 gesetzt.

Das Verfahren ist sehr zeitaufwendig und sehr sicherer.

Gefahren und Sicherheitsproblem stellt die Herstellung, Verteilung und

sichere Lagerung des Schlüssel dar.

Beispiel 2b:

Die Transposition wird nicht wie oben beschrieben in einer Tabelle sondern

Stringulär durchgeführt. D. h. es gibt keine Zeilen / Spalten sondern

nur die aktuelle und die zu errechnende/ermittelnde neue Position.

Im Schlüssel sind je Schlüsselnummer 2 Permutationen des Alphabets abgedruckt. Unter den Klartext werden die Permutationsreihen geschrieben:

Klartext = DAS IST DER KLARTEXT DER HIER VERSCHLUESSELT WERDEN SOLLXzwsputmrncbvglafkodjx
01-1 = ZEKRPDWLBOVUHMAQFTXJNCISYGHNZDPEKICTLBVAOYSQXWJGMURFUAHCTKNRJVSZQYBGIDPELMXFOW
Chiffre = addsathkets_l_eir_re_rtx_dsuc_e_riserldesvtnlheew_eroclgadblvpzfkwlrstxsuxonm

Zum ausfüllen der unbesetzten Stellen, des Klartextes, einer Permutationsreihe wird, wie hier dargestellt, aufgefüllt. Und zwar mit der zweiten Reihe der zweiten Permutationsreihe. Ab dort wird kleingeschrieben. Es dient auch als Blender.

Das "D" in der Pos. 0 geht jetzt in die Pos 26 (Z) der ersten Permutationsreihe über.
Das "A" in der Pos. 1 geht in die Pos 5 (E).
Die Transposition erfolgt jetzt immer Blockweise in 26 Schritten.

Ein Angriff dieses Chiffre ist möglich aber sehr schwer durchführbar. Möglich wird er durch die Permutationstabellen und deren Schrittlänge von 26. Es wiederholt sich zwar nicht der Schlüssel aber ab Position 27 kann man bei diesem Verfahren mit einem neuen Schlüssel rechnen. Hier greift bei einem Angriff auch das Wissen über die Enigma-Dechiffrierung! Gefahren und Sicherheitsproblem stellt die Herstellung, Verteilung und sichere Lagerung des Schlüssel dar.

Beispiel 2c:

Mittels zweier Permutationsgruppen, der Schlüssel, erfolgt eine Substitution und darauf eine Transposition.

Klartext = DASISTDERKLARTEXTDERHIER
01-1 = ZEKRPDWLBOVUHMAQFTXJNCISYG
Substitut = rzxbxjrptvuztjpsjrptlbptXX
01-2 = HNZDPEKICTLBVAOYSQXWJGMURF
Chiffre = jzbtbxbrplrupzpxrxjvtttpsx

Aufgrund der Substitution ist die Lösung der Transposition erschwert.

10.3. Doppelwürfe der HV A Agenten, 1959

Vorwort:

Das hier beschriebene Verfahren GRANIT E 160 entspricht dem im vorherigen Kapitel 10.2. beschriebenen Doppelwürfel der HV A. Es liegt nahe dass es sich um das Chiffrierungsverfahren handelt,

die in den 1970ern zu der Verhaftung von Günter Guillaume führte.

Chiffre "Granit" Verfahren: E 160 ^{BStU *225}

Lfd.

Nr.	Inhaltsangabe	Ex	Blatt-Nr.	Bemerkungen
1	<u>Gebrauchsanweisung</u> für Chiffre "Granit"	1	1 - 7	GVS 1064/59
2	<u>Hinweis</u> zum Gebrauch der Chiffre "Granit"	1	8 - 10	GVS 1065/59
3	<u>Hinweis</u> für Chiffrierung u. Dechiffrierung 160	1	11	

E 160 GVS 1064/59 1. Exemplar 7 Blatt

Gebrauchsanweisung für das Chiffrierverfahren GRANIT / 160

0 Chiffriermittel :

Zwischen den Korrespondenten werden vereinbart:

- ein Buch,
- ein Schlüsselwort,
- eine fünfstellige Schlüsselzahl.

Beispiel: Buch: "Die Abderiten" von Christoph Martin Wieland;

- ein Schlüsselwort: Rheinast.
- eine fünfstellige Schlüsselzahl: 65792

1 Chiffrierung :

11 Herrichtung des Klartextes:

Der Klartext wird zur Chiffrierung so hergerichtet, daß er nur noch Buchstaben und Zeichen enthält, die in der Schlüsselmatrix, die in 12 gebildet wird, vorhanden sind.

Insbesondere ist zu beachten:

- a) ä, ö, ü und ß werden als ae, oe, ue und ss geschrieben.
j wird durch ii ersetzt.
- b) Vor und nach jeder in Ziffern geschriebenen Zahl wird das Zahlensignal (zs) gesetzt und jede Ziffer dreimal hintereinander geschrieben.
- c) Satzzeichen werden nur dann gesetzt, wenn sie zum Verständnis des Textes notwendig sind. ein Fragezeichen wird dann durch zwei Punkte(..) gesetzt.

Beispiel: Klartext: Jeder Zwischenfall bei Unternehmen Edelweiß am 12. März ist möglichst zu vermeiden.
Bericht bis 1. April.

Hergerichteter Klartext: Iieder Zwischenfall bei Unternehmen Edelweiss am zs 111

222 zs Maerz ist moeglichst
zu vermeiden. Bericht bis
zs 11 zs April.

12 Herstellung der Schlüsselmatrix:

Den Buchstaben und Zeichen des Klartextes werden Zahlen zugeordnet, wozu eine mit Hilfe des vereinbarten Schlüsselwortes hergestellte Schlüsselmatrix benutzt wird.

Die Schlüsselmatrix besteht aus 10 Spalten und 3 Zeilen.

Die Spalten werden mit den Ziffern 0 - 9 in einer vereinbarten konstanten Reihenfolge belegt. Die Spaltenziffern von zwei vereinbarten Spalten dienen außerdem zur Numerierung der 2. und 3. Zeile der Schlüsselmatrix

- 2 -

In die Schlüsselmatrix werden die voneinander verschiedenen Buchstaben des Schlüsselwortes, die restlichen Buchstaben des Normalalphabetes (außer J), das Zahlensignal (zs), Punkt (.) und Komma (,) in einer vereinbarten konstanten Reihenfolge eingetragen. Dabei werden die beiden Felder in der ersten Zeile, deren Spaltenziffern zur Numerierung der 2. und 3. Zeile der Schlüsselmatrix benutzt werden, freigelassen. Die Buchstaben in der ersten Zeile der Schlüsselmatrix werden durch die über ihnen stehenden Ziffern ersetzt, die Buchstaben und Zeichen in der zweiten und dritten Zeile durch die jeweils aus ihrer Zeilen- und Spaltenziffer gebildete zweistellige Zahl.

Beispiel: Schlüsselwort: RHEINAST

Schlüsselmatrix:	<u>0 1 2 3 4 5 6 7 8 9</u>
	R H E I N A S T
8	B C D F G K L M O P
9	Q U V W X Y Zzs . ,

Hergerichteter Klartext:

Ieder Zwischenfall bei Unternehmen Edelweiss am
zs 111222 zs Maerz ist moeglichst zu vermeiden
Bericht bis zs 111 zs April

Zifferntext: 332822096933691124
835868680239147204
218724282286932366

587971112229789520
963678788284863811
679691922087238224
802038117803697111
975890386

13 Herstellung der Raster:

Zur Chiffrierung werden zwei Raster - R1 und R2 - benötigt. Auf einer beliebigen Seite des Buches wird eine Zeile ausgewählt. Beginnend mit dem ersten Wort dieser Zeile, werden 10 aufeinanderfolgende Wörter des Buchtextes zur Herstellung von R1 und R2 bestimmt. Steht am Anfang dieser ausgewählten Zeile ein aus einer oder mehreren Silben bestehendes Ende eines Wortes, das auf der vorhergehenden Zeile beginnt, so zählt man dieses Wortende als ganzes Wort. In Ziffern geschriebene Zahlen und Zeichen (z. B. Satzzeichen) innerhalb des Buchtextes werden weggelassen.

- 3 -

R1 und R2 werden folgendermaßen gebildet:

Die ersten fünf Wörter dienen zur Herstellung von R1, die letzten fünf zur Herstellung von R2. In den jeweils 5 Wörtern werden ä, ö, ü und ß durch ae, oe, ue und ss ersetzt. Jedem Buchstaben entspricht eine Rasterpalte. Die Buchstaben werden nach ihrem Vorkommen im Normalalphabet numeriert. Bei gleichen Buchstaben wird von links nach rechts numeriert. So ergibt sich eine Numerierung der Spalten von R1 und R2. Bei der Auswahl der 10 Wörter ist darauf zu achten, daß die folgenden Bedingungen erfüllt werden:

- a) Die Anzahl der Spalten von R1 bzw. R2 muß mindestens 15 sein.
- b) Die Spaltenanzahl von R1 und R2 müssen voneinander verschieden sein. Sind sie nicht voneinander verschieden, so ist der erste Buchstabe der für R2 verwendeten Wortfolge an den Schluß derselben nochmals zu setzen. Dadurch wird die Spaltenanzahl von R2 um 1 größer als die von R1.

Beispiel: Seite 129, Zeile 2, die 10 aufeinanderfolgenden Wörter des Buchtextes, die mit dem ersten Wort dieser Zeile beginnen: "... gute halten. Ich bin gewiß, daß er der feinste Mann ..."

R1:

G U T E H A L T E N I C H B I N G E W I S S
 7 21 19 4 9 1 14 20 5 15 11 3 10 2 12 16 8 6 22 13 17 18

R2:

D A S S E R D E R F E I N S T E M A N N
 3 1 17 18 5 15 4 6 16 9 7 10 12 19 20 8 11 2 13 14

14 Schlüsselung:

Der Zifferntext wird zeilenweise von links nach rechts in R1 eingetragen. In jedes Feld des Rasters wird nur eine Ziffer geschrieben. Nach Eintragung des Zifferntextes werden gegebenenfalls Blender zugefügt. Die Anzahl der einzusetzenden Blender ergibt sich aus den folgenden Bedingungen:

- a) Die Anzahl der Ziffern in R1 muß durch 5 teilbar sein.
- b) Die Anzahl der Ziffern in R1 darf nicht durch die Spaltenanzahl von R2 teilbar sein, d.h. R2 darf keine volle letzte Zeile enthalten.

Bei Chiffrierung verschiedener Klartexte sind verschiedene Blender zu wählen.

Beispiel:

R1:

7	21	19	4	9	1	14	20	5	15	11	3	10	2	12	16	8	6	22	13	17	18
3	3	2	8	2	2	0	9	6	9	3	3	6	9	1	1	2	4	8	3	5	8
6	8	6	8	0	2	3	9	1	4	7	2	0	4	2	1	8	7	2	4	2	8
2	2	8	6	9	3	2	3	6	6	5	8	7	9	7	1	1	1	2	2	2	9
7	8	7	5	2	0	9	6	3	6	7	8	7	8	8	2	8	4	8	6	3	8
1	1	6	7	9	6	9	1	9	2	2	0	8	7	2	3	8	2	2	4	8	0
2	0	3	8	1	1	7	8	0	3	6	9	7	1	1	1	9	7	5	8	9	0
3	8	6																			

Anzahl der Ziffern des Zifferntextes: 135, 135 ist durch 5 und nicht durch die Spaltenzahl von R2 teilbar. Demnach werden keine Blender eingesetzt.

Die Ziffern werden aus R1 spaltenweise von oben nach unten gemäß der Spaltennumerierung abgelesen und zeilenweise von

links nach rechts in R2 eingetragen. Die Ziffern werden aus R2 in derselben Weise wie aus R1 abgelesen und in Fünfergruppen eingeteilt.

Beispiel:

R2:

3	1	17	18	5	15	4	6	16	9	7	10	12	19	20	8	11	2	13	14
2	2	3	0	6	1	9	4	9	8	7	1	3	2	8	8	0	9	8	8
6	5	7	8	6	1	6	3	9	0	4	7	1	4	2	7	3	6	2	7
1	2	3	2	8	1	8	8	9	2	0	9	2	9	1	6	0	7	7	8
7	3	7	5	7	2	6	1	2	7	8	2	1	3	4	2	6	4	8	0
3	2	9	9	7	9	4	6	6	2	3	1	1	1	2	3	1	5	2	2
3	8	9	8	8	9	8	0	0	2	6	8	7	6	3	6	9	9	3	6
1	8	3	8	2	8	1	0	8	8	2	2	8	2	5					

Chiffretext: 25232 88967 45926 17331 96864 81668 77824 38160
 07408 36287 62368 02722 81792 18203 06193 12117
 88278 23878 02611 12998 99926 08373 79930 82598
 82493 16282 14235

15 Herstellung der Kenngruppe:

Die Schlüsselgruppe, die die zur Rasterherstellung ausgewählte Zeile angibt, besteht aus einer dreistelligen Seitennummer (S. 129 - 129) und einer zweistelligen Zeilennummer Z.2 - 02). Sie muß dem Empfänger chiffriert mitgeteilt werden.

Zu den 5 Ziffern der Schlüsselgruppe addiert man modulo 10 die 5 Ziffern der vereinbarten Schlüsselzahl. Das Ergebnis ist die Kenngruppe, die zweimal vor den Chiffretext gesetzt wird. So erhält man das vollständige Telegramm.

Beispiel:

Schlüsselgruppe:	12902
Die 5 Ziffern der vereinbarten Schlüsselzahl:	<u>65792</u>
Kenngruppe:	<u>77694</u>
Telegramm:	77694 77694 25232 88967 45926 17331 96864 81668 77824 38160 07408 36287 62368 02722 81792 18203 06193 12117 88278 23878 02611 12998 99926 08373 79930 82598 82493 16282 14235

2 Dechiffrierung :

Telegramm: 67395 67395 27239 51268 40892 77382 49929 41108
37931 38163 22829 32620 40987 41412 85088 22088
72280 45654 12620 27770 81889 34235 85800 38842
74888 81921 31881

Es gelten dieselben Vereinbarungen wie in 0 und 1.

21 Herstellung der Schlüsselmatrix: wie in 12.

22 Herstellung der Schlüsselgruppe:

Vor dem Chiffretext steht zweimal die Kenngruppe. Von den 5 Ziffern der Kenngruppe werden modulo 10 die 5 Ziffern der vereinbarten Schlüsselzahl subtrahiert. Das Ergebnis ist die Schlüsselgruppe.

Beispiel:

Kenngruppe: 67395
die 5 Ziffern der vereinbarten Schlüsselzahl: 65792
Schlüsselgruppe: 02603

Die ersten 3 Ziffern der Schlüsselgruppe geben eine Seite und die letzten beiden Ziffern eine Zeile im Buch an. Beginnend mit dem ersten Wort dieser Zeile, werden 10 aufeinanderfolgende Wörter des Buchtextes zur Herstellung von R1 und R2 bestimmt.

Beispiel: Schlüsselgruppe: 02603

Seite 26, Zeile 3, die 10 aufeinanderfolgenden Wörter des Buchtextes, die mit dem ersten Wort dieser Zeile beginnen:

"... fassen wie Wieland, der sich, mit Goethe zu reden, "auflehnt"."

23 Herstellung der Raster: wie in 13.

- 6 -

24 Entschlüsselung:

Die beiden Kenngruppen werden aus dem Telegramm gestrichen. Bevor die Ziffern des Chiffretextes in die Raster eingetragen werden, muß das Schema jedes Rasters aufgezeichnet werden. Dazu wird die Anzahl der Ziffern des Chiffretextes durch die Anzahl der Spalten des jeweiligen Rasters dividiert. Der Quotient ist dann gleich der Anzahl der vollen Zeilen des Rasters, der Rest ist gleich der Anzahl der besetzten Felder in der nächsten Zeile.

Beispiel: Anzahl der Ziffern des Chiffretextes: 125
Anzahl der Spalten des Rasters R1: 23

Anzahl der Spalten des Rasters R2: 24

125 : 23 = 5 Rest 10

125 : 24 = 5 Rest 5

R1 hat 5 volle Zeilen und in der 6. Zeile 10 Ziffern.

R2 hat 5 volle Zeilen und in der 6. Zeile 5 Ziffern.

Die Ziffern des Chiffretextes werden spaltenweise von oben nach unten gemäß der Spaltennumerierung in R2 eingetragen, zeilenweise von links nach rechts abgelesen und wiederum spaltenweise von oben nach unten gemäß der Spaltennumerierung in R1 eingetragen.

Beispiel:

R2:

14	12	19	9	17	3	20	10	4	24	22	18	5	2	6	15	1	23	8	13	7	11	16	21
0	1	9	2	2	4	8	2	7	3	7	0	4	5	4	8	2	8	3	0	3	0	5	3
8	4	3	2	0	0	5	6	7	1	4	8	9	1	1	0	7	1	8	8	7	9	4	8
8	1	4	8	2	8	8	2	3	8	8	1	9	2	1	4	2	9	1	8	9	8	1	8
7	2	2	2	7	9	0	0	8	8	8	8	2	6	0	5	3	2	6	2	3	7	2	4
2	8	3	9	7	2	0	4	2	1	8	8	9	8	8	6	9	1	3	2	1	4	6	2
2	5	5	3	7																			

R1:

10	1	19	20	6	16	22	12	7	23	13	8	15	2	17	4	5	9	18	21	14	3	11
8	0	2	0	3	8	1	1	7	2	9	1	2	8	0	2	0	8	2	9	1	0	8
1	1	8	4	2	8	3	9	1	2	1	0	7	2	5	8	5	7	3	8	8	4	2
4	9	3	2	0	8	2	2	4	5	8	7	9	7	3	3	3	9	7	8	7	5	3
8	2	9	1	0	8	1	1	8	5	9	1	0	3	2	0	8	4	0	6	2	4	8
2	2	7	8	5	2	4	4	9	3	8	8	0	7	6	3	4	8	4	9	2	8	8
8	4	2	8	6	6	6	2	1	7													

- 7 -

Die in R1 eingetragenen Ziffern werden zeilenweise von links nach rechts durch die ihnen nach der Schlüsselmatrix entsprechenden Buchstaben und Zeichen ersetzt. Dabei werden die nur zur Spaltennumerierung verwendeten Ziffern durch die ihnen entsprechenden Buchstaben ersetzt. Die Zeilenziffern werden mit der ihnen jeweils folgenden Ziffer zu einer zweistelligen Zahl zusammengefaßt und diese nach der Schlüsselmatrix durch das ihr entsprechende Element ersetzt. Das ergibt den hergerichteten Klartext und die Blender. Um den Klartext zu erhalten, müssen die in 11 unternommenen Schritte rückgängig gemacht werden.

Beispiel:

Klartext: Berichte über durchgeführte Aktionen werden am 3. Mai
durch Kurier gesendet. Kennwort: Singvogel.

Blender 66217

GVS 10765/59 1. Exemplar 3 Blatt

Hinweise zum Gebrauch des Chiffrierverfahrens GRANIT

- 0 Hinweise für den Chiffreur :
- 01 Für die Chiffrierung verschiedener Klartexte werden verschiedene Buchtextstellen benutzt. Die Buchtextstellen werden unsystematisch aufgesucht. Zu aufeinanderfolgenden Klartexten verwendete Buchtextstellen müssen in ihrem Wortbestand wesentlich voneinander verschieden sein.
- 02 Muß ein Chiffretext wegen Verstümmelung bei der Übermittlung noch einmal gesendet werden, so wird er ungeändert mit der gleichen Schlüsselgruppe gesendet. Muß ein Chiffretext wegen Verstümmelung bei der Chiffrierung noch einmal gesendet werden, so wird er durch Umordnung der Klartextteile, Umstilisierung und Benutzung von synonymen abgeändert und mit einer anderen Schlüsselgruppe (einem anderen Schlüssel) gesendet.
- 03 Bei der Übermittlung von Mischtext ist folgendes zu beachten:
1.) Die Klartextteile und die Chiffretextteile sind getrennt zu übermitteln.
2.) Aus dem Klartextteil darf für den Unbefugten keine Rekonstruktion des Chiffretextteiles möglich sein.
- 04 Der Klartext darf nicht weniger als 50 und nicht mehr als 400 Klarelemente umfassen. Kürzere Klartexte müssen durch Einsetzen von etwa 15 Blendern unter Berücksichtigung der in 14 angegebenen Bedingungen a) und b) erweitert werden.
Sind die Klartexte länger als 400 Klarelemente, so werden diese Klartexte in mehrere, den Bedingungen entsprechend lange Klartexte geteilt. Jeder dieser Klartexte wird bei der Chiffrierung als selbständiges Telegramm behandelt, d.h. mit eigener Schlüsselgruppe verschlüsselt.
- 05 Die Klartexte werden auf ein unbedingt notwendiges Minimum gekürzt.
- 06 Stereotype Klartexte werden durch Umordnung der Klartextteile, Umstilisierung, Benutzung von Synonymen und Weglassen unnötiger Angaben (Anreden, Unterschriften) vermeiden. Unbedingt zu unter-

lassen sind Namensunterschriften und Grußübermittlungen am Ende des Textes.

- 2 -

1 Hinweise für den Ausbilder :

11 Auswahl des Buches:

- a) Das auszuwählende Buch soll mindestens 250 Seiten enthalten.
- b) Mit verschiedenen Korrespondenten werden verschiedene Bücher vereinbart.
- c) Es können eventuell zwei verschiedene Bücher - eines zum Senden und eines zum Empfangen - vereinbart werden.
- d) Bei der Auswahl des Buches ist insbesondere folgendes zu beachten:
 - Das Buch muß so beschaffen sein, daß es sich nicht als Chiffriermittel verrät.
 - Es darf kein Tabellen-, Formel- oder Zeichenbuch sein.
 - Das Buch darf nicht in der DDR oder in einem anderen sozialistischen Staat verlegt sein.
 - Das Buch muß den Interessen des Korrespondenten entsprechen.
 - Ist ein Korrespondent im Besitz nur weniger Bücher, so ist seine Bibliothek systematisch mit Büchern aufzufüllen, die seinem Hauptinteresse entsprechen.
 - Schundliteratur ist - wenn viele Bücher vorhanden sind - ebenfalls als Interessengebiet zu betrachten, vor allem bei Jugendlichen. Dabei muß aber die unter a) angegebene Bedienung eingehalten werden.

12 Behandlung des als Chiffrierematerial vereinbarten Buches:

Das Buch darf nicht versteckt werden, aber auch nicht offen oder separat aufbewahrt werden. Es muß sich unter den zu diesem Fach- oder Interessengebiet gehörenden Büchern befinden und genau wie diese behandelt werden. Das Buch darf nicht durch besondere Abnutzung gegenüber den anderen Büchern hervorstechen, es darf auch nicht neu wirken.

Im Buch dürfen im Zusammenhang mit der Chiffrierung keinerlei Zeichen gemacht werden oder Seiten umgeknickt werden.

Fingerabdrücke und Bleistiftspuren unter dem verwendeten Text sind zu vermeiden. Der Korrespondent muß angewiesen werden, in gewissen Zeitabständen und vor allem vor und nach dem Chiffrieren das vereinbarte Buch und andere Bücher zu durchblättern, damit das vereinbarte Buch nicht durch die neuen Fingerabdrücke sofort

erkannt wird.

- 3 -

Es sollen jedoch nicht jedesmal alle Bücher durchblättert werden, da das bei Untersuchungen ebenfalls auffallen würde.

- 13 Auswahl des Schlüsselwortes:
Mit verschiedenen Korrespondenten werden verschiedene Schlüsselwörter vereinbart.
Die Schlüsselwörter werden von der Abteilung XI des MfS geliefert.
- 14 Auswahl der fünfstelligen Schlüsselzahl:
a) Die vereinbarte Schlüsselzahl darf höchstens zwei gleiche Ziffern enthalten.
b) Mit verschiedenen Korrespondenten werden verschiedene Schlüsselzahlen vereinbart.
c) Mit jedem Korrespondenten ist eine Schlüsselzahl zu vereinbaren, die er sich leicht einprägen kann, z. B. Geburtsdaten von Bekannten, Hut- Schuh-, Konfektionsgrößen, Telephonnnummern, Autonummern, Hausnummern oder andere Daten, die der Korrespondent mit besonderen, nicht zu vergessenden Ereignissen verknüpfen kann.
Die Auswahl dieser Gedächtnisstützen darf nicht stereotyp erfolgen.
- 15 Stellung der Kenngruppen:
Als Stellung der Kenngruppen im Telegramm können andere Plätze - z. B. am Ende des Chiffretextes - vereinbart werden.
- 16 Bei der Chiffrierzentrale sind die Schlüsselgruppen der Ein- und Ausgänge zu registrieren. Verwendet ein GM in gesetzmäßigem Zusammenhang stehende Schlüsselgruppen, so ist er im nächsten an ihn gerichteten Telegramm auf den Fehler aufmerksam zu machen.

GVS 1068/59 1. Exemplar 1 Blatt

- I. Chiffrierung
1. Erste 10 aufeinanderfolgende Wörter einer Zeile im Buch beliebig aufsuchen.
R1 aus ersten 5 Wörtern. R2 aus nächsten 5 Wörtern.

- Spaltenumerierung nach Stellung im Alphabet.
2. Klartext in Zifferntext umwandeln und zeilenweise in R1 eintragen.
Blender in R1 einsetzen (Anzahl der Ziffern in R1: eine durch 5 und nicht durch Spaltenzahl von R2 teilbare Zahl)
Ziffern aus R1 spaltenweise ablesen, zeilenweise in R2 eintragen und spaltenweise ablesen - ergibt Chiffretext.
 3. Kenngruppe = Schlüsselgruppe (Seite 3-stellig, Zeile 2-stellig)+
+ Schlüsselzahl.
Kenngruppe 2-mal im Chiffretext.

II. Dechiffrierung

1. Schlüsselgruppe = Kenngruppe - Schlüsselzahl.
2. Herstellung der Raster wie in I.1. Raster umranden !
3. Chiffretext (ohne Kenngruppen) spaltenweise von oben nach unten in R2 eintragen, zeilenweise ablesen und spaltenweise von oben nach unten in R1 eintragen.
Ziffern zeilenweise von links nach rechts in Klartext umwandeln.

11. Manuelle Chiffrierverfahren

11.1. Verfahren: JUPITER, TITAN-Z und SIRENE.

Die hier genannten manuellen Chiffrierverfahren wurden von den IM (Agenten) z. B. der BRD verwendet. Es fehlen noch Dokumente zu den Verfahren.

J U P I T E R Hauptverfahren
Absolut sicheres Ziffernverfahren. Anwendbar allein oder in Verbindung mit einem Schlüsselcode.
Die Substitutionstabelle wurde ab 1960 regelmäßig geändert.
Ab 1962 gab es eine dänische Substitutionstabelle. BStU^{*284}
HVA - Jupitertabellen: [Manuell](#), [T-307/3](#).
Beispieltext des [IM Kurras](#).
Software JUPITER für Windows auf der [Freeware](#) Seite.

T I T A N - Z Ziffern - Schlüsselcode
Nur anwendbar zur Textverkürzung mit einem absolut sicheren Ziffernverfahren.
HVA - TITAN-Z [Codebuch](#).

S I R E N E Schlüsselverfahren
Absolut sicheres Ziffernverfahren, nur anwendbar zur Über-

E307

01

0 23366 03237 74470 75102 27941 49432 52740 06252 87035 23682 66254

1 44392 01014 80115 85359 15899 77065 67490 37509 11042 81071 88303

2 69581 35776 27399 92920 11334 92731 29030 48226 22165 91691 59181

3 85958 84410 65836 97953 64138 53834 71913 32027 69751 28624 24197

4 29482 62241 29380 72628 07829 61803 39222 75100 64229 03379 10811

11.3. Verfahren "Code A ... D" und "Chiffre 9" BSTU *106

Im Buch [Geheimsprachen](#) von F.B. Wrixon wird auf S. 222 ff. ein algebraisches Verschlüsselungsverfahren erläutert.

Der Mathematikprofessor Lester Hill hatte 1929 dieses Verfahren entwickelt und veröffentlicht.

1950 erarbeitete das ZCO darauf basierend die Codes [A](#), [B](#), [B1](#), [B2](#), [C](#), [C1](#), [C2](#), [C3](#), [C4](#), [C5](#), [D/D2](#), [D3](#) und [Chiffre 9](#).

Bei allen folgenden Codeverfahren gelten folgende Festlegungen:

"a ... d" sind Ganzzahlen;

"x, y" sind nie Negativ und liegen im Wertebereich 00 ... 99;

"z" ist der in Ziffern substituierte Klartext;

"t" ist die Wiederholung des Buchstaben im Text;

"Schlüsselwort" oder Schlüsselsätze zur Bildung der Buchstaben-Ziffern-Buchstabensubstitution. Die Formel die als Brüche dargestellt werden dürfen nicht gekürzt werden. Je nach Codierverfahren werden die Zähler als x_1 und y_1 und die Nenner als x_2 und y_2 hier benannt. Aus ihnen werden die Codegruppen $x_1x_2y_1y_2$ gebildet.

Code A

Der Code A verwendet die lineare birationale Transformation. Der Verlängerungsfaktor beträgt 8. D.h. das Chifftrat ist achtmal so lang wie der Klartext. Schlüsselwort = "SCHULPFORTA DEGEN".

Auswahl der Formeln aus einer festgelegten [Formelmenge A](#).

$$\begin{array}{l} \text{Formel } (x_1) \quad 3z + t \\ X = \frac{\quad}{\quad} \\ (x_2) \quad z + 3 + t \end{array} \qquad \begin{array}{l} (y_1) \quad 2z + t + 1 \\ Y = \frac{\quad}{\quad} \\ (y_2) \quad z + 2t \end{array}$$

Formeln für die Umkehren (Dechiffrieren):

$$Z = \frac{3x - 1}{xy - 5x + 5y - 1} \qquad T = \frac{-x + 3}{xy - 5x + 5y - 1}$$

Wobei die Umkehrung von T nur zu Prüfzwecken verwendet werden kann. In der Dokumentation wird darauf hingewiesen das die Umkehrung von T weggelassen werden kann.

Substitutionsreihe aus der Schlüsselfolge:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11	16	2	12	13	7	14	3	18	20	22	5	24	15	8	6	26	9	1	10	4	25	23	21	19	17

Nachricht:

Klartext:	H	E	R	Z	L	I	C	H	E	N	G	L	Ü	C	K	W	U	N	S	C	H	
Subst.: (z)	3	13	9	17	5	18	2	3	13	15	14	5	4	13	2	22	23	4	15	1	2	3
(t)	1	1	1	1	1	1	1	2	2	1	1	2	1	3	2	1	1	2	2	1	3	3

x_1	10	40	28	52	16	55	07	11	41	46	43	17	13	42	08	67	70	14	47	04	09	12
x_2	06	16	12	20	08	21	05	09	19	18	17	11	07	22	08	25	26	10	21	04	11	12
y_1	08	28	20	36	12	38	06	09	29	32	30	13	10	30	07	46	48	11	33	04	08	10

y₂ 05 15 11 19 07 20 04 07 17 17 16 09 06 19 06 24 25 08 19 03 08 09

= 10060805401628152812201152203619160812075521382007050604114119291746183217431730161711
130913071006422230190808070667254624702648251410110847213319040707030911080812121009

Das Schlüsselwort hat 16 Buchstaben, jetzt wird die erste Ziffer mit 16 Mod(10) addiert.
die folgenden Ziffern immer mit dem Ergebnis der vorherigen Addition Mod(10).

16 + 1 = 7
7 + 0 = 7
7 + 0 = 7
7 + 6 = 3

= 77733116001797835346889057992898955346638356979996611771233221182343545262314674812922390
789033236634440468033433119966285726248557375723788900823125898822660033234422013467776

Diese ist jetzt in ein Schlüsselwortraster einzusetzen:

<u>S</u>	<u>C</u>	<u>H</u>	<u>U</u>	<u>L</u>	<u>P</u>	<u>F</u>	<u>O</u>	<u>R</u>	<u>T</u>	<u>A</u>	<u>D</u>	<u>E</u>	<u>G</u>	<u>E</u>	<u>N</u>
7	7	7	3	3	1	1	6	0	0	1	7	9	7	8	3
5	3	4	6	8	8	9	0	5	7	9	9	2	8	9	8
9	5	5	3	4	6	6	3	8	3	5	6	9	7	9	9
9	6	6	1	1	7	7	1	2	3	3	2	2	1	1	8
2	3	4	3	5	4	5	2	6	2	3	1	4	6	7	4
8	1	2	9	2	2	3	9	0	7	8	9	0	3	3	2
3	6	6	3	4	4	4	0	4	6	8	0	3	3	4	3
3	1	1	9	9	6	6	2	8	5	7	2	6	2	4	8
5	5	7	3	7	5	7	2	3	7	8	8	9	0	0	8
2	3	1	2	5	8	9	8	8	2	2	6	6	0	0	3
3	2	3	4	4	2	2	0	1	3	4	6	7	7	7	6

Es werden die Spalten alphabetisch ausgelesen und in Fünfergruppen notiert:

19533 88782 47356 31615 92796 21902 86692 92403 69678
99173 44007 19675 34679 27871 63320 07745 64261 71338
41524 97543 89842 38836 60312 90228 01867 42465 82058
26048 38175 99283 35230 73327 65723 36313 93932 4

Das Entschlüsseln des Geheimtextes erfolgt rückwärts:

- Raster
- Schlüssellänge subtrahiert Mod(10) mit der ersten Stelle,
nachfolgende mit dem Code des vorherigen Codes. $x_1 - x_2 \dots$
Ist der Minuend kleiner als der Subtrahend wird der Minuend mit 10 addiert.
(1) $7 - 16 = 1$
 $7 - 7 = 0$

$$7 - 7 = 0$$

$$(1) 3 - 7 = 6$$

$$3 - 3 = 0$$

$$(1) 1 - 3 = 8$$

- Anwendung der Umkehrfunktion, wobei die Umkehrfunktion nur für Prüfungszwecke verwendet werden kann.

$$Z = \frac{3 * \frac{10}{6} - 1}{\frac{10}{6} * \frac{8}{5} - 5 * \frac{10}{6} + 5 * \frac{8}{5} - 1}$$

$$Z = 3$$

- Substitution der Ziffern anhand des Schlüsselwortes.
3 = "H"

Code B

Der Code B verwendet die lineare ganze birationale Transformation.
Der Verlängerungsfaktor beträgt 4. D.h. das Chiffriertext ist viermal so lang wie der Klartext.
Das Schlüsselwort beinhaltet jeden Buchstaben nur einmal.
Auswahl der Formeln aus einer festgelegten [Formelmeng](#)e B.

Code B1

Schlüsselwort: "DORFTISCHLAMPEN"

Auswahl der Formeln aus einer festgelegten [Formelmeng](#)e B1.

$$\text{Formel: } X = 1 + 2z + t \qquad y = 2 + z + 2t$$

Formeln für die Umkehrung (Dechiffrieren):

$$Z = \frac{2x - y}{3} \qquad T = -\frac{x - 2y + 3}{3}$$

Substitutionsreihe aus der Schlüsselwortfolge:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11	23	8	1	14	4	24	9	6	25	26	10	12	15	2	13	16	3	7	5	17	18	19	20	21	22

Nachricht:

Klartext: T R E F F E M O N T A G A B E N D E I N K A R L
Subst.: (z) 5 3 14 4 4 14 12 2 15 5 11 24 11 23 14 15 1 14 6 15 26 11 3 10

(t) 1 1 1 1 2 2 1 1 1 2 1 1 2 1 3 2 1 4 1 3 1 3 1 1

X 12 08 30 10 11 31 26 06 32 13 24 50 25 48 32 33 04 33 14 34 52 26 09 22
Y 09 07 18 08 10 20 16 06 19 11 15 28 17 27 22 21 05 24 10 23 30 19 09 14

= 12090807301810081110312026160606321913112415502
82517492732332104053324141034235230261909092214

Diese Ziffern sind jetzt aus dem Schlüsselwortraster zu ersetzen:

0 1 2 3 4 5 6 7 8 9
D O R F T I S C H L
A M P E N B G J K Q
U V W X Y Z

und in Fünfergruppen notieren.:

ORDLA HUCFD MKVAU HIMVD EOPAW SVGUS XROLM FVORN VIBAP
KWZVJ YHRCE RPWEE ROUNA IFEER YOTVD ETWXZ NEDPG OLAQU
LRRMT

Das Entschlüsseln erfolgt in umgekehrter Richtung:

- Bildung des Schlüsselwortrasters;
- Auslesen der Ziffern anhand des Chiffrates;
- Berechnen der Umkehrfunktion, die Berechnung von T ist nicht zwingend notwendig;
- Ziffern Textsubstitution.

Code B2

Schlüsselwort mit mindestens 10 verschiedenen Buchstaben: SCHMETTERLINGSFLUEGEL

Auswahl der Formeln aus einer festgelegten [Formelmenge B2](#).

Formel: $X = z + t$ $y = 2z - t$

Formeln für die Umkehrung (Dechiffrieren):

$Z = -x - y$ $T = 2x - y$

Substitutionsreihe aus der Schlüsselfolge:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
15 19 2 25 5 12 11 3 9 16 22 8 4 10 20 17 26 7 1 6 13 24 18 14 21 23

Nachricht:

Klartext: T A G U N G D E S W E L T F R I E D E N S R A T E S I N B E R L I N
Subst.: (z) 6 15 11 13 10 11 25 5 1 18 5 8 6 12 4 9 5 25 5 10 1 7 15 6 5 1 9 10 19 5 7 8 9 10
(t) 1 1 1 1 1 2 1 1 1 1 2 1 2 1 1 1 3 2 4 2 2 2 2 3 5 3 2 3 1 6 3 2 3 4

X 07 16 12 14 11 13 26 06 02 19 07 09 08 13 08 10 08 27 09 12 03 09 17 09 10 04 11 13 20 11 10 10 12 14
Y 13 31 23 27 21 24 51 11 09 37 12 17 14 25 15 19 13 52 14 22 04 16 32 15 15 05 20 23 39 16 17 18 21 24

= 0713163112231427112113242651060091937071209170814132508151019081327
520914122203040916173209151015040511201323203911161017101812211424

Diese Ziffern sind jetzt aus dem Schlüsselwortraster zu ersetzen:

0 1 2 3 4 5 6 7 8 9
S C H M E T R L I N
G F U A B D J K O P
Q V W X Y Z

und in Fünfergruppen notieren.:

SLCMF RAVCH UXFBW Kfvhc FMUYW RDFQJ CFGUS XVNAK SLFUQ PSKGI
VEDMU ZSOCT VGFFG IFAUL DUSPF EFWUH QASEG NCJVK MUSNC TFSCT
QESZV FUGCA HAUSX NCFVR FGCLV SCIFU UCFEH E

Das Entschlüsseln erfolgt in umgekehrter Richtung:

- Bildung des Schlüsselwortrasters;
- Auslesen der Ziffern anhand des Chiffrates;
- Berechnen der Umkehrfunktion, die Berechnung von T ist nicht zwingend notwendig;
- Ziffern Textsubstitution.

Code C/C1

Bei diesem Code werden drei Codierverfahren angesetzt.

Der Verlängerungsfaktor beträgt 2.

D.h. das Chifftrat wird doppelt so lang wie der Klartext.

An festgelegten Stellen des Chiffrates werden Buchstaben eingefügt die bei der Entschlüsselung nicht beachtet werden. Diese Buchstaben kamen nicht oder kaum im Chifftrat vor.

Methode:

- a) Es wird nach jedem Buchstaben des Textes ein Buchstabe eingefügt.
- b) Nach jedem zweiten
- c) Nach jedem dritten
- d) Nach jedem vierten

e) Nach jedem fünften.

Schlüsselwort mit mindestens 10 verschiedenen Buchstaben: SPEKULATION

Substitutionsreihe aus der Schlüsselfolge:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
S	P	E	K	U	L	A	T	I	O	N		B	D	G	J	Q	V	X	Z	Y	W	R	M	H	F	C

Das Auffüllen der Substitutionstabelle erfolgt so das der nächste nicht benutzte Buchstabe abwechselnd vorn und hinten eingefügt wird. D.h. "B" ist "L" zugeordnet, "C" wird dem "Z" zugeordnet.

Nachricht:

Klartext:	H	A	N	S	P	L	O	E	T	Z	L	I	C	H	S	C	H	W	E	R	E	R	K	R	A	N	K	T	E	R	W	I	N
Subst.:	T	S	G	Z	Q	B	J	U	Y	C	B	I	E	T	Z	E	T	M	U	X	U	X	N	X	S	G	N	Y	U	X	M	I	G

Schlüsselraster:

S	P	E	K	U	L	A	T	I	O	N
T	S	G	Z	Q	B	J	U	Y	C	B
I	E	T	Z	E	T	M	U	X	U	X
N	X	S	G	N	Y	U	X	M	I	G

Spaltenweise auslesen:

JMUGTSYXMZZGBTYBXGCUISEXTINUUXQEN

Methode b) der Buchstabeneinfügung wird verwendet.

Die Buchstaben "A,O,F,H,K,L,P,VW" traten nicht im Code auf und werden jetzt zum Auffüllen verwendet.

Chiffprat: JMOUGATSFYXHMZKZGLBTPYBVXGWCUAISVEXLTIHNUOUXEQEAN

Das Entschlüsseln wie folgt:

- Streichen jedes dritten Buchstabens;
- Bildung der Substitutionstabelle entsprechend der Chiffriervorschrift;
- Substituieren des Textes

Code C2

Es wird kein Schlüsselwort gebildet sondern eine "Automorphie" des Alphabetes nach den Methoden:

a) Der Buchstabe "A" wird dem Buchstaben "Z", "B" > "X" zu und dieses fortlaufend.

Bsp.:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	M	Y	L	X	K	W	J	V	I	U	E	T	G	S	F	R	E	Q	D	P	C	O	B	N	A

b) Der Buchstabe "A" wird dem Buchstaben "Z", "C" > "Y"
zu und dieses fortlaufend.

Bsp.: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Z X V L R P N L J H F D B Y W U S Q O L K I G E C A

c) Es wird das Alphabet um 2 Buchstaben übersprungen.

Bsp.: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A D G J M I S V Y B E F N H Q T W Z C F I L O R U X

d) Das selbe wie unter c) nur rückwärts.

Bsp.: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
X U R O L I F C Z W T Q H N F E B Y V S I M J G D A

Kolonnenbildung (Kasten) des Zwischentextes nach den Methoden:

e) 6er Gruppen, Spaltenweise von links beginnend auslesen;

f) 8er Gruppen, Spaltenweise von links beginnend auslesen;

g) 10er Gruppen, Spaltenweise von links beginnend auslesen;

h) 12er Gruppen, Spaltenweise von links beginnend auslesen.

Beispiel:

Substitutionstabelle nach b):

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Z X V L R P N L J H F D B Y W U S Q O L K I G E C A

Nachricht:

Klartext: G E R H A R D K O M M T M I T T W O C H A B E N D N A C H H A L L E

Zwischentext: N R Q L Z Q L F W B B L B J L L G W V L Z X R Y L Y Z V L L Z D D R

Kasten e):

N R Q L Z Q
L F W B B L
B J L L G W
V L Z X R Y
L Y Z V L L
Z D D R

Zwischentext: NLBVLZRFJLYDQWLZZDLBLXVRZBGRQLQWL

Der Zwischentext wird jetzt wie folgt bearbeitet:

Nach dem ersten Buchstaben wird ein Leerzeichen eingefügt

nach 2 weiteren Buchstaben ... usw. usf. bis zur neunten

Buchstabengruppe danach geht es wieder mit einem Buchstaben weiter.

Zwischentext: N LB VLZ RFJL YDQWL ZZDLBL XVRZBGR LQLWYL

Jetzt füllen wir die Lücken mit einem beliebigen Buchstaben auf.

Chiffprat: NALBEVLZIRFJLUYDQWLEZZDLBLMXVRZBGRELQLWYL

Das Entschlüsseln läuft, entsprechend den Vereinbarungen hier b) und e), wie folgt ab:

- Entfernen der Auffüllungen, nach dem 1. - 2. - 3.
- Kasten entsprechend e) bilden und den Zwischentext bilden
- bilden der Substitutionstabelle nach b)
- Auflösen der Substitution

Code C3

Bilden eines Schlüsselwortes mit mindestens zehn verschiedenen Buchstaben.

Das Auffüllen der Substitutionstabelle erfolgt so das der nächste nicht benutzte Buchstabe abwechselnd vorn und hinten eingefügt wird.

D.h. "B" ist "K" zugeordnet, "F" wird dem "Z" zugeordnet.

Bilden eines Kastens anhand des Schlüsselwortes.

Auslesen, alphabetisch, der Spalten in 3er Gruppen.

Auffüllen der Lücken mit einem danach mit zwei dann wieder mit einem Buchstaben, usw. usf.

Beispiel:

Schlüsselwort: KURZHAARDACKEL

Substitutionstabelle:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	U	R	Z	H	A	D	C	E	L	B	G	J	N	P	S	V	X	Y	W	T	Q	O	M	I	F

Zwischentext: KJYPNWKDOXZHXOKHXJYWHWKDZHYLKCXHNY

Kasten:

K	U	R	Z	H	A	A	R	D	A	C	K	E	L
K	J	Y	P	N	W	K	D	O	X	Z	H	X	O
K	H	X	J	Y	W	H	W	K	D	Z	H	Y	L
K	C	X	H	N	Y								

Zwischentext: NJH WYY OWK KDH ZZN XXK XYX DHH YKK KWJ OLP HC

Chiffprat: NJHEW YYAEO WKBKD HIFZZ NMXXX VVXYX EDHHQ LYKKR KWJAE OLPZHC

Code C4

Bilden eines Schlüsselwortes mit mindestens zehn verschiedenen Buchstaben.

Die Substitution wird gebildet aus dem Schlüsselwort und der laufenden Nummer des bearbeiteten Spruches.
 Diese Nummer bildet den Beginn des Einsatzes des Schlüsselwortes in die Substitutionstabelle. Aufgefüllt wird dann nach rechts Beginnend.
 Bilden eines Kasten anhand des Schlüsselwortes.
 Spaltenweise, alphabetisch, auslesen in 4er Gruppen.
 Abwechselnd füllen des Zwischenraumes mit einem oder zwei Buchstaben.

Beispiel:

Es ist der 14. Spruch.

Schlüsselwort: PARTEIKONFERENZ

Substitutionstabelle:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	V	U	S	Q	M	L	J	H	G	D	C	B	P	A	R	T	E	I	K	O	N	F	Z	Y	X

Klartext: W A L Z W E R K F E T T S T E D T H I L F T L A U C H H A M M E R

Substitution: F W C X F Q E D M Q K K I K Q S K J H C M K C W O U J J W B B Q E

Kasten: P A R T E I K O N F E R E N Z
 F W C X F Q E D M Q K K I K Q
 S K J H C M K C W O U J J W B
 B Q E

Zwischentext: WKQF CKUI JQOQ MEKJ WKWD CFSB CJEK JXHQ B

Chiffprat: WKQFA CKUIZ YJQOQ MGEKJ VRWKW DACFS BPCJ EKMJX HQSSB

Zum Entschlüsseln entfernen wir die Auffüllungsbuchstaben.
 Bilden einen Kasten sowie die Substitutionstabelle und entschlüsseln damit die gebildeten Zwischentexte.

Code C5

Bilden eines Schlüsselwortes mit mindestens zehn verschiedenen Buchstaben. Einsetzen des Schlüsselwortes an der Position des ersten Buchstabens + Spruchnummer.
 Also "G" und Spruchnummer 2; Position = 7 + 2 = 9 = "I".
 Bilden eines Kasten. Auslesen, alphabetisch, der Spalten.
 Abwechselndes füllen mit ein, zwei oder drei Buchstaben.

Beispiel:

Schlüsselwort: GROSSGRUNDBESITZER

Substitutionstabelle:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 L M P Q V W X Y G R O S U N D B E I T Z A C F H J K

Klartext: G E W E R K S C H A F T L E R O R G A N I S I E R E N K A M P F A K T I O N E N
 Substitution: X V F V I O T P Y L W Z S V I D I X L N G T G V I V N O L U B W L O Z G D N V N

Kasten: G R O S S G R U N D B E S I T Z E R
 X V F V I O T P Y L W Z S V I D I X
 L N G T G V I V N O L U B W L O Z G
 D N V N

Zwischentext: WLLO ZUIZ XLDO VVWY NFGV VNNT IXGV TNIG SBIL OVDO
 Chiffprat: WLLOK ZUIZH JXLDO EEVW WYLNFGVEAV NNTEC RIXGV QTNIG YMSBI LEYO VDO

Zum Entschlüsseln entfernen wir die ein, zwei oder drei Buchstaben aus dem Chiffprat.
 Bilden einen Kasten und die Substitutionstabelle entsprechend dem Schlüsselwort.
 Und Entschlüsseln das Chiffprat.

Code D/D2

Bilden eines Schlüsselwortes mit mindestens zehn verschiedenen Buchstaben.
 Zuordnen der Zahlen entsprechend dem Schlüsselwort.
 Nun wird nach dem letzten Buchstaben ,des Schlüsselwortes, der zweite nicht belegte
 Buchstabe aufgesucht und mit der nächsten Ziffer belegt.
 Substitution des Klartextes.
 Jetzt wird von der ersten Ziffer die Länge des Schlüsselwortes abgezogen.
 Die weiteren Ziffern werden vom Ergebnis der vorherigen Subtraktion abgezogen.
 Bildung eines Kastens.

Beispiel:

Schlüsselwort: FARBFILMPRODUKTION

Substitutionstabelle:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 2 4 18 10 26 1 19 23 5 20 12 6 7 14 9 8 25 3 15 13 11 21 16 24 17 22

Klartext: Z U S A M M E N K U N F T A U F U N B E S T I M M T E N Z E I T P U N K
 T V E R S C H O B E N

Zwischentext: 22 11 15 2 7 7 26 14 12 11 14 1 13 2 11 1 11 14 4 26 15 13 5 7 7 13 26 14 22 26 5 13 8 11 14 12
 13 21 26 3 15 18 23 9 4 26 14

22 - 18 = 4 = B
 11 - 4 = 7 = M
 15 - 7 = 8 = P
 2 - 8 = (26+2) - 8 = 20 = J

$$7 - 20 = (26+7) - 20 = 13 = T$$

Zwischentext: BMPJTJLPBMMJQOAKAAXYZOXOBZCBZOBMMIPTTWQGBIQFT

Kasten: F A R B F I L M P R O D U K T I O N
 B M P J T J L P B M M J Q O A Q K A
 A X Y Z O X O B Z C B Z O B B M M I
 P T T W Q G B I Q F T

Chiffprat: MXTJZ WJZBA PTOQJ XGQMO BLOBP BIAIM BTKMB ZQPYT MCFAB QO

Das Entschlüsseln läuft wieder Rückwärts ab.
 Kasten bilden, Zwischentext jetzt Addieren, zuerst mit der Länge des Schlüsselwortes danach mit dem Produkt der vorherigen Addition.
 Hier mit Mod(26).
 Substitutionstabelle bilden und Klartext erarbeiten.

Code D3

Bei Code D3 handelt es sich um eine "Verbesserung" des Code D1.
 Bilden eines Schlüsselwortes mit mindestens zehn verschiedenen Buchstaben.
 Zuordnen der Zahlen entsprechend dem Schlüsselwort.
 Beginnend mit der laufenden Spruchnummer.
 Klartext substituieren und Mod(25) Addieren.
 Das erste Zeichen mit der Länge des Spruchschlüssels,
 die nachfolgenden mit der Summe der vorherigen Addition.
 Den Zwischentext in einen Kasten eintragen.
 Alphabetisch aus dem Kasten auslesen.

Beispiel:

Spruchnummer: 13
 Schlüsselwort: PRODUKTIONSGENOSSENSCHAFT
 Substitutionstabelle (Achtung Y fehlt):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Z
2	4	25	16	24	3	23	1	20	6	18	8	10	21	15	13	12	14	22	19	17	11	9	7	5

Klartext: D I E E R S T E N B E Z I R K S T A G E D E R R E P U B L I K I N R O S
 T O C K U N D S C H W E R I N G E B I L D E T
 Zwischentext. 16 20 24 24 14 22 19 24 21 4 24 5 20 14 18 22 19 2 23 24 16 24 14 14 24 13 17 4 8 20 18 20 21 14 15
 22 19 15 25 18 17 21 16 22 25 1 9 24 14 20 21 23 24 4 20 8 16 24 19

$$16 + 25 = 41 = 16 = D$$

$$20 + 16 = 36 = 11 = V$$

$$24 + 11 = 35 = 10 = M$$

24 + 10 = 34 = 9 = W
14 + 9 = 23 = = G

Zwischentext: DVMWG IRPWP QUQHT DMQMW CEPAH RJMKP JHSCH GUXXC UPBHH ABMET POQDV TMWF

Kasten:

```
P R O D U K T I O N S G E N O S S E N S C H A F T
D V M W G I R P W P Q U Q H T D M Q M W C E P A H
R J M K P J H S C H G U X X C U P B H H A B M E T
P O Q D V T M W F
```

Chiffprat: PMCAW KDQXQ BAEUU EVPSW IJTPH HXMFM MQWF TCDRO BJPQG DUMPW HRHMH TGPV

Zum Entschlüsseln geht man wieder rückwärts vor.
Bilden des Kasten und der Substitutionstabelle anhand des Schlüsselwortes.
Zwischentexte bilden, Subtraktion mit der Länge des Schlüsselwortes,
anschließend mit dem Ergebnis der vorherigen Subtraktion.

Code Chiffre 9

Bilden eines Schlüsselwortes das mindestens zehn verschiedene Buchstaben enthält.

Bilden der Substitutionstabelle, füllen durch abwechselndes Eintragen am Anfang und Ende der Tabelle.

Zwischentext mittels der Substitution bilden.

Addition Mod(26) mit der Schlüsselziffer der ersten Ziffer,
die nachfolgenden wieder mit dem Ergebnis der vorherigen Addition.

Bilden eines Kasten und ermitteln des Chiffrates.

Beispiel:

Schlüsselwort: BROCKENHAUS

Schlüsselziffer: 11

Substitutionstabelle:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	1	4	12	6	14	16	8	18	20	5	22	24	7	3	26	25	2	11	23	10	21	19	17	15	13

Klartext: T R E F F P U N K T M O N T A G B R A N D E N B U R G E R T O R
23 2 6 14 14 26 10 7 5 23 24 3 7 23 9 16 1 2 9 7 12 6 7 1 10 2 16 6 2 23 3 2

23 + 11 = 34 = 8 = H
2 + 8 = 10 = = U

Zwischentext: HUGCIIRAFSADWGQYGIBHJPNHIJUGIYIJ

Kasten:

B R O C K E N H A U S
H U G C I I R A F S A
D W G Q Y G I B H J P
N H I J U G I Y I J

Chiffprat: FHIHD NCQJI GGABY IYURI IGGIU WHAPS JJ

Die Entschlüsselung geschieht durch das Bilden des Kasten
und der Substitutionstabelle.

Die Bildung des Zwischentextes aus dem Kasten.

Subtraktion der ersten Ziffer mit der Schlüsselziffer.

Ist diese kleiner wird der ersten Ziffer die 26 hinzuaddiert und
dann mit der Schlüsselziffer subtrahiert.

Die folgenden Ziffern werden subtrahiert mit dem Ergebnis der
vorherigen Subtraktion unter Beachtung das wenn der Subtrahend
kleiner als der Minuend, der Subtrahend mit 26 zu addieren ist.

Bilden mit der Substitutionstabelle des Klartextes.

Formelmengen

Codieren

Umkehrung

Code A

Basis der Formelmenge von Code A:

$$X = \frac{a_1z + a_2t + a_3}{b_1z + b_2t + b_3} \quad Y = \frac{c_1z + c_2t + c_3}{d_1z + d_2t + d_3}$$

a.)

$$X = \frac{3z + t}{z + 3 + t} \quad Y = \frac{2z + t + 1}{z + 2t} \quad Z = \frac{3x - 1}{xy - 5x - 5y - 1} \quad T = \frac{-x + 3}{xy - 5x + 5y - 1}$$

b.)

$$X = \frac{z + t - 1}{z + 3t - 3} \quad Y = \frac{z + 2t - 1}{z + t} \quad Z = \frac{3xy - y}{-2xy + x + 1} \quad T = \frac{-3xy + x + y + 1}{-2xy + x + 1}$$

c.)

$$X = \frac{2z + t - 1}{z + 2t - 1} \quad Y = \frac{z + t + 1}{z + 2t - 2} \quad Z = \frac{-2xy - 3x - 2y + 3}{x - 3y + 1} \quad T = \frac{xy - 2y + 2x - 4}{x - 3y + 1}$$

d.)

$$X = \frac{3z + t - 3}{2z + 2t - 3}$$

$$Y = \frac{2z + t + 1}{z + 3t - 3}$$

$$Z = \frac{3xy - 5x - 6y + 4}{4xy + 2x - 8y + 1}$$

$$T = \frac{3xy + 8x - 6y - 9}{4xy + 2x - 8y + 1}$$

e.)

$$X = \frac{z + t}{2z + t - 2}$$

$$Y = \frac{2z + 2t - 2}{z + t + 1}$$

$$Z = \frac{-3xy - 2x - y - 2}{xy - 2x}$$

$$T = \frac{4xy + y + 2}{xy - 2x}$$

f.)

$$X = \frac{z + 3t}{2z + t - 1}$$

$$Y = \frac{z + 2t - 1}{z + t}$$

$$Z = \frac{xy - x - 3}{xy + 2y - 3y - 1}$$

$$T = \frac{-xy - x + 1}{xy + 2y - 3x - 1}$$

Code B

Basis der Formelmeng von Code B:

$$X = a_1 + b_1z + c_1t$$

$$Y = a_2 + b_2z + c_2t$$

$$Z = \frac{c_2x - c_1y + c_1a_2 - a_1c_3}{b_1c_2 - c_1b_2}$$

$$T = \frac{b_2x - b_1y + b_1a_2 - a_1b_2}{b_1c_2 - c_1b_2}$$

Code B1

a.)

$$X = 1 + 2z + t$$

$$Y = 2 + z + 2t$$

$$Z = \frac{2x - y}{3}$$

$$T = -\frac{x - 2y + 3}{3}$$

b.)

$$X = 1 + z + 2t$$

$$Y = -1 + 2z + 2t$$

$$Z = -x + y + 2$$

$$T = \frac{2x - y - 3}{2}$$

c.)

$$X = -2 + 2z + 2t$$

$$Y = z + 2t$$

$$Z = x - y + 2$$

$$T = \frac{-x + 2y - 2}{2}$$

d.)

$$X = -3 + z + 2t$$

$$Y = z + t$$

$$Z = \frac{x - 3y + 3}{-2}$$

$$T = \frac{-x + y - 3}{-2}$$

e.)

$$X = 3z + t$$

$$Y = -1 + 2z + t$$

$$Z = -1 + x + y$$

$$T = 3 - 2x + 3y$$

f.)

$$X = -1 + z + t$$

$$Y = -2 + z + 2t$$

$$Z = 2x - y$$

$$T = -x + y + 1$$

g.) $X = -2 + 2z + t$ $Y = 1 + z + t$ $Z = 3 + x - y$ $T = -4 - x + 2y$

Code B2

a.) $X = z + t$ $Y = 2z + t$ $Z = -x + y$ $T = 2x - y$

b.) $X = 2z + t$ $Y = z - 3t$ $Z = \frac{2x - y}{5}$ $T = \frac{-x + 2y}{5}$

c.) $X = z + 2t$ $Y = 2z + t$ $Z = \frac{-x + 2y}{3}$ $T = \frac{2x - y}{3}$

11.4. Manuelles Chiffrierverfahren PYTHON

Zentrales Chiffrierorgan der DDR

BStU [*159](#)

Geheime Verschlusssache!
GVS-ZCO/123/75

Ausfertigung Nr. 0704

**Gebrauchsanweisung
zum Verfahren
PYTHON (manuell)**

1976

Zentrales Chiffrierorgan der DDR

BStU*

Geheime Verschlusssache!

**Gebrauchsanweisung
zum Verfahren
PYTHON (manuell)**

1976

GVS-ZCO/123/75 - Blatt 2

Die "Gebrauchsanweisung zum Verfahren PYTHON (manuell)",
GVS-ZCO/123/75, wird erlassen und tritt mit Wirkung vom
01.06. 1976 in Kraft.

Berlin, den 01. 06. 1976

Leiter ZCO

gez. Birke
Oberst

3

GVS-ZCO/123/75 - Blatt 3

Inhaltsverzeichnis

	Seite
1. Zweckbestimmung	<u>7</u>

2.	Chiffriermittel	<u>8</u>
2.1.	Allgemeines	<u>8</u>
2.2.	Schlüsselunterlagen	<u>8</u>
2.2.1.	Schlüsselheft	<u>8</u>
2.2.2.	Additionsreihe	<u>9</u>
2.2.3.	Kenngruppentafel	<u>9</u>
2.2.4.	Kontrolle der Additionsreihen und Kenngruppentafeln	<u>10</u>
2.2.5.	Wechsel der Schlüsselunterlagen	<u>10</u>
2.3.	Bereichsinterne Herrichtung	<u>11</u>
3.	Chiffrieren	<u>12</u>
4.	Dechiffrieren	<u>13</u>
5.	Sicherheitsbestimmungen	<u>14</u>
6.	Beispiele	<u>16</u>
Anlage 1: Öffnungsvorschrift für Schlüsselhefte		<u>18</u>

1. **Zweckbestimmung**

Das Chiffreverfahren "PYTHON (manuell)" dient in Verbindung mit der ["Vorschrift für Ziffernadditionsverfahren \(manuell\)", GVS-ZCO/122/75](#), zur Bearbeitung von Klartexten.

Es ist nur für manuelle Bearbeitung vorgesehen. Das Verfahren "PYTHON (manuell)" gewährleistet bei ordnungsgemäßer Anwendung absolute Sicherheit für die chiffrierte Nachricht.

Mit dem Verfahren können individuelle und zirkulare Verkettungen abgewickelt werden.

2. **Chiffriermittel**

2.1. **Allgemeines**

Zum Verfahren " P Y T H O N (manuell)" gehören folgende Chiffriermittel:

- Vorschrift für Ziffernadditionsverfahren (manuell),
- Substitutionstafel [TAPIR](#)
- Schlüsselunterlagen: Schlüsselhefte mit Kenngruppentafeln,
- Gebrauchsanweisung zum Verfahren PYTHON (manuell).

2.2. **Schlüsselunterlagen**

2.2.1. **Schlüsselheft**

Die Additionsreihen sind in Schlüsselheften untergebracht. Jedes Exemplar einer Serie enthält eine Kenngruppentafel, die soviel Kenngruppen umfaßt wie das Heft Additionsreihen enthält.

Auf der Verpackung sind in der Regel folgende Kennzeichnungen enthalten:

- Typ-Nr.,
- "I" (individueller Verkehr: Auflage 2),
- "Z" (zirkularer Verkehr: Auflage 3 und höher;
- Serien- und Exemplarnummer: Wenn nicht anders angewiesen, dient Exemplar 1 zum Chiffrieren. Die übrigen Exemplare dienen zum Dechiffrieren.

Auf der Innenseite der Schlüsselhefte befinden sich Raum für folgende Eintragungen:

- Nr. der entnommenen Additionsreihe,
- Datum der Entnahme der Additionsreihe,
- Unterschrift des Bearbeiters.

Das Öffnen der Schlüsselhefte erfolgt entsprechend der Öffnungsvorschrift (siehe [Anlage 1](#)) und ist mit Angabe des Datums zu signieren.

Das Öffnen der Hefte und die Entnahme von Additionsreihen darf nur erfolgen wenn sie unmittelbar zum Chiffrieren bzw. Dechiffrieren verwendet werden sollen.

2.2.2. **Additionsreihe**

Die Additionsreihen sind, gegen vorzeitige Einsichtnahme geschützt, im Schlüsselheft untergebracht. Jede Additionsreihe besteht aus 40-50 fünfstelligen Zifferngruppen. Die Additionsreihen sind fortlaufend numeriert. Sie sind in dieser Reihenfolge zu verwenden.

Jede Additionsreihe darf zum Chiffrieren nicht mehr als einmal benutzt werden!

Die Entnahme der Additionsreihen ist in der Entnahmetabelle durch Datum und Unterschrift nachzuweisen. Über **freigelegte nichtbenutzte Additionsreihen** ist zusätzlich Nachweis zu führen. Auf dem Heftumschlag ist zu vermerken "Nr. ... bis ... nicht benutzt (Datum, Unterschrift)". Falls nicht anders angewiesen, sind diese Additionsreihen bis zur Bearbeitung des nächsten Spruches im Heft, bei Dienstschluß im versiegelten Umschlag beim Schlüsselheft mit Angabe der Geheimhaltungsstufe, aufzubewahren. Als ungültig gekennzeichnete Additionsreihen und Additionsreihen mit Beschädigungen, die das Chiffrieren beeinträchtigen, dürfen nicht zum Chiffrieren verwendet werden. Das Chiffrieren ist dann mit der nächstfolgenden noch nicht verwendeten Additionsreihe **neu** zu beginnen. Wenn nicht anders angewiesen, sind zur Bearbeitung benutzte und aus dem Heft gelöste unbenutzte Additionsreihen innerhalb von 48 Stunden zu vernichten. Über die Vernichtung der Additionsreihen ist Nachweis zu führen.

2.2.3. **Kenngruppentafel**

Die Kenngruppentafel ist als Tabelle im Heft befestigt untergebracht und darf nicht vom Heft getrennt werden. Sie enthält als Kenngruppen fünfstellige Zifferngruppen. Jeder Additionsreihe ist entsprechend ihrer Numerierung eindeutig eine Kenngruppe zugeordnet. Die Kenngruppen sind spaltenweise von oben nach unten, in der Reihenfolge

tafel zu entnehmen ([Beispiel 1](#)).
Werden mehrere Additionsreihen zum Chiffrieren eines Klartextes verwendet, so ist nur die Kenngruppe der zuerst benutzten Additionsreihe als erste und letzte Gruppe dem Chiffretext anzufügen. Kenngruppen benutzter Additionsreihen sind in der Kenngruppentafel zu streichen ([Beispiel 1](#)).

2.2.4. Kontrolle der Additionsreihen und Kenngruppentafeln

Vor Beginn des Chiffrierens bzw. Dechiffrierens sind die Kenngruppentafeln und die Additionsreihen wie folgt auf Fehler zu überprüfen:

- a) Additionsreihen und Kenngruppentafeln, die keine oder eine falsche Seriennummer bzw. Numerierung aufweisen, sind aus dem Zusammenhang mit der entsprechenden Seriennummer bzw. Numerierung zu kennzeichnen. Additionsreihen dieser Art dürfen nicht zum Chiffrieren verwendet werden.
- b) Bei der Bearbeitung in Additionsreihen bzw. Kenngruppentafeln auftretende Fehlzeichen sind durch nachfolgende Substitution in Ziffern umzusetzen:
Fehlzeichen: q w e r t y u i o p
Ziffer: 1 2 3 4 5 6 7 8 9 0
- c) Anstelle einzelner fehlender Ziffern in den Fünfergruppen der Kenngruppentafeln ist die Ziffer "0" einzusetzen.

2.2.5. Wechsel der Schlüsselunterlagen

Die Leitstelle (verantwortliche Chiffrierstelle) ordnet den Wechsel und die Außerkraftsetzung von Schlüsselunterlagen an.

neue Schlüsselunterlagen anzufordern, so daß ein kontinuierlicher Chiffrierverkehr gewährleistet ist.

2.3. **Bereichsinterne Herrichtung**

Das Verfahren "PYTHON (manuell)" ist absolut sicher. Bei Notwendigkeit kann durch den Leiter des jeweiligen Chiffrierdienstes eine von der in der zugewiesenen Vorschrift für Ziffernadditionsverfahren abweichende bereichsinterne Herrichtung der Klartexte angewiesen werden.

11

3. **Chiffrieren**

Zum Chiffrieren des Zwischentextes ist die nächstfolgende noch **nicht benutzte Additionsreihe zu verwenden**. Diese wird dem Empfänger durch die Kenngruppe mitgeteilt. Beim Chiffrieren eines zirkularen Spruches ist am Anfang des Textes vor die Kenngruppe die Unterscheidungsgruppe "zzzzz" zu setzen.

Reicht die Anzahl der Fünfergruppen der Additionsreihe nicht aus, so ist die nächstfolgende Additionsreihe (beachte [Abschnitt 2.2.2.](#)) in gleicher Weise zu benutzen. Sind die Additionsreihen eines Schlüsselheftes verbraucht, so ist das nächstfolgende für diesen Verkehr vorgesehene Heft zu benutzen (in der Regel das mit der nächsthöheren Seriennummer versehene Heft).

Bleiben Fünfergruppen einer Additionsreihe beim Chiffrieren des Zwischentextes unbenutzt, so sind sie nicht mehr zu verwenden.

Jede Fünfergruppe der Additionsreihe darf zum Chiffrieren nicht mehr als einmal benutzt werden.

12

GVS-ZCO/123/75 - Blatt 7

4. **Dechiffrieren**

Anhand der Stellung der Kenngruppe in der gültigen Kenngruppentafel, die Kenngruppe spaltenweise von oben nach unten - in der Reihenfolge der Spalten von links nach rechts abgezählt - wird die Nummer der ersten für den Spruch bestimmten Additionsreihe bestimmt ([Beispiel 1](#) und [2](#)).

Die Kenngruppen, deren zugeordneten Additionsreihen zum Dechiffrieren des Spruches benutzt wurden, sind zu streichen.

Für das Dechiffrieren des Chiffretextes **ist die durch die Kenngruppe bestimmte Additionsreihe zu verwenden.**

Reicht die Anzahl der Fünfergruppen der Additionsreihe zum Dechiffrieren nicht aus, ist die nächstfolgende Additionsreihe (beachte [Abschnitt 2.2.2.](#)) in gleicher Weise zu benutzen. Sind die Additionsreihen eines Schlüsselheftes verbraucht, ist das nächstfolgende für diesen Verkehr vorgesehene Heft zu benutzen (in der Regel das mit der nächsthöheren Seriennummer versehene Heft).

5. Sicherheitsbestimmungen

V o r k o m m n i s s e	S o f o r t m a ß n a h m e n
(1) Verwendung der Kenngruppentafel als Additionsreihe	
a) vor Übermittlung des so bearbeiteten Spruches:	Fehler korrigieren.
b) nach Übermittlung des so bearbeiteten Spruches:	Mitteilung an Leitstelle. Leitstelle weist Außerkraftsetzung aller Exemplare der Schlüsselserie oder Verwendung einer noch nicht benutzten Additionsreihe als Kenngruppentafel an.
(2) Verwendung des Eingangsexemplars zum Chiffrieren	
a) vor Übermittlung des so	Fehler korrigieren.

bearbeiteten Spruches: | Vorzeitig gelöste Additionsreihen im versiegelten Umschlag
 | durch den Leiter der Chiffrierstelle aufbewahren oder Mitteilung an
 | empfangende Chiffrierstelle über Vernichtung der vorzeitig ge-
 | lösten Additionsreihen des Eingangsexemplars.

14

GVS-ZCO/123/75 - Blatt 8

V o r k o m m n i s s e	S o f o r t m a ß n a h m e n
b) nach Übermittlung des so bearbeiteten Spruches:	Feststellen, ob mit Ausgangsmaterial der Gegenstelle schon ein Spruch bearbeitet und übermittelt wurde. Mitteilung an emp- fangende bzw. absendende Chiffrierstelle. Mögliche Kompromittierung beachten! In diesem Fall Mitteilung über Kompromittierung der betreffenden Textteile an die Ab- sender und Empfänger der Nachricht.
(3) Kompromittierung der Kenngruppentafel	Keine Sofortmaßnahme erforderlich!

15

6. **Beispiele**

Beispiel 1: Kenngruppentafel

07349	65088	85538	43918	30230	
30833	04867	28890	49265	31933	
50020	08494	10334	99980	26102	
37968	88661	55231	07696	57075	
94189	15295	80797	68463	22723	
48253	68873	23169	01738	58468	
13261	39248	39402	88751	39254	
32661	99570	65704	90194	85812	
81241	14992	05634	09043	63523	053285
58539	59215	18150	69262	16486	

Der 13. Additionsreihe ist die Kenngruppe 08494 zuge-
ordnet.

Beispiel 2: 13. und 14. Additionsreihe

11194	30270	81029	97833	96055	
23380	96212	23644	70299	79339	
16770	29812	89803	44601	89613	
92406	54785	21222	87335	28142	
52194	13621	80191	07188	42673	
08519	52894	12849	27088	44533	
58952	61480	91177	36571	40609	
92773	89765	29674	25982	71326	053285
46518	57183	91714	74050	80680	13
36291	85063	98846	99050	02274	

16

GVS-ZCO/123/75 - Blatt 9

67072	91827	05181	38813	82033	
63792	18069	64706	28819	32675	
74404	84211	41400	23092	71478	
76176	70382	52876	48834	05274	
12819	89131	07839	67541	55975	
99545	63000	47415	25257	35342	053285
40119	25534	22219	89491	33089	14
60918	65053	93351	76483	77800	
60579	67032	72586	77630	48314	
37942	92095	19070	75248	07420	

17

Anlage 1

Öffnungsvorschrift für Schlüsselhefte

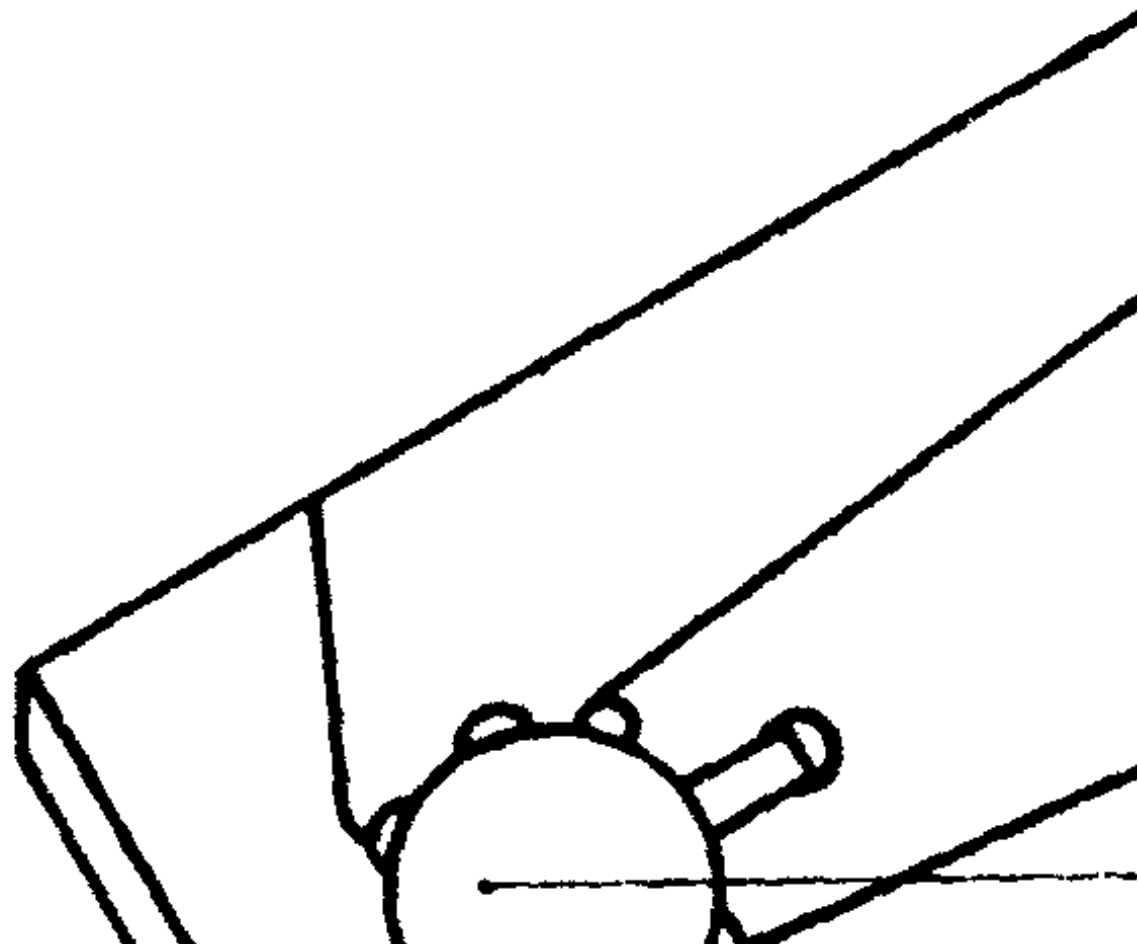
1. Vor dem Öffnen des Schlüsselheftes ist zu prüfen, ob **Siegel und Umschlag unbeschädigt** sind.

2. Zum **Öffnen** des Schlüsselheftes muß

- der Kontrollmetallring unter dem Siegel abgerissen und geprüft werden, ob die Klappe des Umschlages unter dem Ring unbeschädigt sind. Das Siegelornament muß bis zum vollständigen Verbrauch des Schlüsselheftes erhalten bleiben ([Abb. 1](#)).
- an der Vorderseite des Schlüsselheftes jede der 2 Seitenklappen aufgerissen ([Abb. 2](#)) und die Klappe des Schlüsselheftes herausgezogen werden, wobei sie vom Schutzbügel abgerissen wird ([Abb. 3](#)).

3. Bei der **Entnahme** der Additionsreihen ist die Unversehrtheit der inneren Perforation zu prüfen (leicht zupfen). Die Blätter sind einzeln vom Rücken des Schlüsselheftes abzureißen und zu entnehmen.

4. Das Entfernen des Schutzbügels ist verboten.
Die Heftseiten mit den Additionsreihen sind zur Entnahme einzeln über den Schutzbügel zu ziehen.



11.5. Manuelles und teilmaschinelles Chiffrierverfahren DIAMANT

Chi 5187

1. 6. 1969

Geheime Verchlußsache!

ZCO 6385/69

16 Blatt Ex. Nr. 104

Blatt 1

Gebrauchsanweisung DIAMANT

1. Zweckbestimmung

Das Chiffreverfahren DIAMANT dient zur Bearbeitung von Klartexten, deren Klarelemente im ITA Nr. 2 enthalten sind oder in solche umgewandelt werden können.

Es ist für teilmaschinelle und rein manuelle Bearbeitung vorgesehen. Eine rein maschinelle Bearbeitung ist ebenfalls möglich. Die Anwendung von Codes ist möglich (vgl. Abschnitte [3.2.](#) und [4.4.](#)).

Das Verfahren DIAMANT gewährleistet bei ordnungsgemäßer Anwendung absolute Sicherheit für die chiffrierte Nachricht. Mit dem Verfahren können individuelle und zirkulare Verkehre abgewickelt werden.

1

2. Chiffriermittel

Zum Verfahren DIAMANT gehören folgende Chiffriermittel:

- Substitutions- und Additionstafel [TAXUS](#) bzw. zugewiesenes Gerät mit Bedienungsanweisung;
- Additionsreihen (Wurmtabellen bzw. Schlüssellochstreifenabschnitte) und Kenngruppentafeln;
- Gebrauchsanweisung zum Verfahren DIAMANT.

2.1. Substitutionstafel

Die zugewiesene Substitutionstafel enthält nur Klarelemente des ITA Nr. 2. Sie gewährleistet die eineindeutige Zuordnung der Klareinheiten zu den Zwischeneinheiten.

2.2. Additionstafel

2.2.1. Die **Additionstafel** dient in Verbindung mit den Wurmtabellen bei der Chiffrierung zur Umwandlung des Zwischentextes in Chiffretext und bei der Dechiffrierung zur Umwandlung des Chiffretextes in Zwischentext. Die Additionstafel enthält 26 Substitutionen, in denen die Buchstaben des Normalalphabetes in bestimmter Weise angeordnet sind. Jede Substitution besteht aus drei Komponenten. Die erste Zeile bildet jeweils die erste, die zweite Zeile die zweite und die dritte Zeile die dritte Komponente.

2.2.2. Die Additionstafel ist so aufgebaut, daß bei der Chiffrierung und bei der Dechiffrierung die Komponenten 1, 2 und 3 vertauscht werden können. Von den drei zusammengehörigen Buchstaben - Wurmbuchstabe, Zwischentextbuchstabe, Chiffretextbuchstabe - ist jeweils der dritte eindeutig bestimmt, wenn zwei bekannt sind.

In der **Kurzform der Additionstafel** sind die dreistelligen Gruppen zusammengehöriger Buchstaben aufgeführt.

Die Kurzform der Additionstafel kann eingepreßt werden und ermöglicht damit eine wesentliche Erhöhung der Chiffrier- geschwindigkeit.

2

Chi 5187
31.10. 1969

GVS - 6385/69 - Blatt 2E -

2.3. Additionsreihen und Kenngruppentafeln

2.3.1. Form und Verpackung

Die Additionsreihen, in Form von Wurmtabellen oder Schlüssel-
lochstreifenabschnitten, sind in Heften bzw. Kassetten unterge-
bracht.

Jedes Exemplar einer Serie enthält eine Kenngruppentafel, die
soviel Kenngruppen umfaßt, wie die Additionsreihe Wurmtabel-
len bzw. Schlüssellochstreifenabschnitte enthält.

Auf der Verpackung sind folgende Kennzeichnungen enthalten:

- Typ-Nummer : festgelegter Aufbau der Additionsreihen;
- I bzw. Z: Verwendung für individuellen (Auflage 2) bzw. zirku-
laren Verkehr (Auflage 3 und höher);
- Serien- und Exemplarnummer : wenn nicht anders angewiesen,
dient Exemplar 1 zum Chiffrieren, die übrigen Exemplare zum
Dechiffrieren.

2.3.2. Ungültige Additionsreihen

Als ungültig gekennzeichnete Wurmtabellen/Schlüssellochstrei-
fenabschnitte sind nicht zur Chiffrierung zu verwenden.

Bei längeren Sprüchen sind diese Wurmtabellen/Schlüsselloch-
streifenabschnitte zu überspringen, und es ist ohne Unter-
brechung die/der nächstfolgende gültige Wurmtabelle/Schlüssel-
lochstreifenabschnitt zur Chiffrierung zu verwenden.

2.3.3. Entnahme

**Die Wurmtabellen/Schlüssellochstreifenabschnitte dürfen erst
dann aus dem Heft bzw. aus der Kassette entnommen werden,
wenn sie unmittelbar zur Arbeit benötigt werden.**

Die Entnahme der Wurmtabellen/Schlüssellochstreifenabschnitte
ist in der Entnahmetabelle/Kenngruppentafel durch Datum und
Signum nachzuweisen.

2.3.4. Kontrolle der Wurmtabellen und Kenngruppentafeln

Vor Beginn der Chiffrierung bzw. Dechiffrierung sind die Kenn-

gruppentafeln und die Wurmtabellen wie folgt auf Fehler zu überprüfen:

a) Wurmtabellen und Kenngruppentafeln, **die keine oder eine falsche Seriennummer bzw. Tabellennummer aufweisen**, sind aus dem Zusammenhang mit der entsprechenden Serien bzw. Tabellennummer zu kennzeichnen.

Wurmtabellen dieser Art dürfen nicht zur Chiffrierung verwendet werden.

b) Bei der manuellen Bearbeitung in Wurmtabellen bzw. Kenngruppentafeln auftretende **Fehlzeichen** sind durch nachfolgende Substitution in Buchstaben umzusetzen:

Fehlzeichen: - ? : @ 3 ↓ * ~ 8 ■ () .
Buchstabe: a b c d e f g h i j k l m

Fehlzeichen: , 9 0 1 4 ' 5 7 = 2 / 6 +
Buchstabe: n o p q r s t u v w x y z

c) Bei der maschinellen Bearbeitung in Kenngruppentafeln auftretende **Fehlzeichen** sind entsprechend dem ITA Nr. 2 in Buchstaben umzusetzen.
Anstelle **einzelner fehlender Buchstaben** in den Fünfergruppen der Kenngruppentafel ist der Buchstabe „o“ einzusetzen.

2.4. Wechsel der Schlüsselunterlagen

Die Leitstelle des Schlüsselbereiches (verantwortliche Chiffrierstelle) ordnet den Wechsel der Schlüsselunterlagen an. Die Chiffrierstellen haben von der Leitstelle rechtzeitig neue Schlüsselunterlagen anzufordern, so daß ein kontinuierlicher Chiffrierverkehr gewährleistet wird. Die Additionstafel und die Substitutionstafel werden nicht gewechselt.

3. Herrichtung der Klartexte für teilmaschinelle Verbindungen

3.1. Falls nicht anders angewiesen, ist jedes Telegramm (zu chiffrierender Klartext) wie folgt zu gliedern (Beispiel [1](#)):

- VS-Einstufung;
- geheimzuhaltende Teile der Anschrift;
- eigentlicher Text (ggf. mit Fortsetzungsvermerken);
- geheimzuhaltende Teile des Absenders;
- Wiederholungen.

Im Verkehr der Chiffrierstellen untereinander können Empfänger und Absender weggelassen werden. Dasselbe trifft zu bei ständig wiederkehrenden Meldungen, Berichten usw., aus denen klar hervorgeht, wer Empfänger und Absender sind.

3.2. Die vom Absender angegebene **Textanordnung** ist mit zu chiffrieren (Beispiel [1](#)). Kürzungen des Klartextes sind statthaft, wenn Sinnentstellungen ausgeschlossen sind und keine buchstabengetreue Wiedergabe des Klartextes gefordert wird.

Bei gemeinsamer Anwendung der Substitutionstafel und des Codes sind die Zwischeneinheiten aus den beiden Mitteln so zu wählen, daß der kürzeste Zwischentext entsteht (Beispiel [2](#)). Der Code darf nur fünfstellige Buchstabengruppen als Codegruppen enthalten.

3.3. **Klareinheiten**, die nicht in der Substitutionstafel oder im Code enthalten sind und für die keine Festlegungen getroffen werden, sind als Wörter voll auszuschreiben (Beispiele [3](#), [4](#)).

5

3.4. Es sind die folgenden **Indikatoren** zu unterscheiden:

	Kurzbezeichnung	Symbol
- Wagenrücklauf/Zeilenvorschub	WR/Zl	∅
- Übergang zu Buchstaben	Bu	≈

- Übergang zu Ziffern und Zeichen Zi »
- Zwischenraum ZwR ≠
- folgende Gruppe ist Codegruppe Code ↑

Der jeweilige Indikator darf innerhalb von Buchstabentext **nicht mehrmals unmittelbar hintereinander** gesetzt werden (Beispiel [1](#)).

- 3.4.1. Es sind die **Textarten** „Bu“ und „Zi“ zu unterscheiden. Nach dem Indikator „Bu“ dürfen nur Buchstaben, nach dem Indikator „Zi“ dürfen nur Ziffern und Zeichen gesetzt werden (Beispiele [1](#), [2](#), [4](#), [7](#)). Jeder Spruch beginnt in Buchstabentext. Beginnt der Spruch mit Zifferntext, so ist der Indikator „Zi“ voranzustellen.
- 3.4.2. Die **Textanordnung** ist durch die Indikatoren „WR/Zl“ und „ZwR“ zu verwirklichen. Der Indikator „WR/Zl“ sowie der Indikator „ZwR“ dürfen innerhalb von Zifferntext mehrmals unmittelbar hintereinander gesetzt werden (Beispiel [1](#)). Jede Zeile soll nicht mehr als ca. 66 Anschläge enthalten.
- 3.4.3. Vor **jede** Phrase, die durch Codegruppen ersetzt werden soll, ist der Indikator „Code“ zu setzen (Beispiel [5](#)). Die Phrasen sind zu unterstreichen. Der Indikator „Code“ kann in beliebiger Textart gesetzt werden. Bei Übergang zu einer anderen Textart ist nach der Phrase der entsprechende Indikator (» oder ≈) zu setzen (Beispiel [2](#)).
- 3.5. Beginnen Wörter mit dem Buchstaben x bzw. y, so ist unmittelbar vor dem entsprechenden Wort die Indikatorenfolge „Zi-Bu“ einzusetzen, wenn das Wort mit dem Anfangsbuchstaben
 x unmittelbar am Anfang der Zeile steht,
 y vom vorhergehenden Wort durch einen Zwischenraum getrennt wird (Beispiel [6](#)).

- 3.6. Die **Schriftzeichen ä, ö, ü und ß** sind aufzulösen und als ae, oe, ue und sz zu schreiben (Beispiele [1](#), [2](#), [5](#), [6](#)).
In **Eigennamen**, bei denen eine eindeutige Rückverwandlung jedes einzelnen Buchstaben gewährleistet sein muß, sind die Umlaute als einfache Laute und ß als s zu schreiben. Diese Eigennamen müssen am Ende des Telegramms entsprechend Abschnitt [3.8.](#) wiederholt werden (Beisp. [1](#), [9](#)).
- 3.7. **Zahlen, Zeichen und Buchstaben-Ziffernfolgen** sind mit den notwendigen Indikatoren unverändert in den hergerichteten Klartext zu übernehmen (Beispiele [1](#), [2](#), [4](#), [7](#)).
Römische Zahlen sind durch die entsprechenden lateinischen Schriftzeichen zu ersetzen. In Zweifelsfällen ist „roem“ vor die Zahl zu schreiben (Beispiel [7](#)).
- 3.8. **Wiederholungen** von Wörtern, Buchstaben- und Ziffernfolgen sind vorzunehmen, wenn bei Verstümmelung einzelner Buchstaben bzw. Ziffern Sinnentstellungen auftreten können. Wiederholungen sind nach mehrmaligem Setzen des Indikators „WR/Zl“ an den Schluß des Textes in der Reihenfolge ihres Auftretens, durch den Indikator „ZwR“ voneinander getrennt, anzufügen.
Wichtige Angaben, z. B. Buchstaben- und Ziffernfolgen, sind zur Vermeidung von Rückfragen bei Verstümmelungen der 1. Wiederholung, sichtbar getrennt von dieser, nochmals anzufügen (Beispiele [1](#), [10](#)).
- 3.8.1. **Aufgelöste Schriftzeichen**, die der Originalschreibweise in Eigennamen entsprechen, sind in der Wiederholung zu verdoppeln (Beispiel [8](#)).
- 3.8.2. Eigennamen mit **Umlauten und ß** sind in der Wiederholung mit aufgelösten Schriftzeichen „ae“, „oe“, „ue“ bzw. „sz“ zu schreiben (Beispiel [9](#)).

- 3.9. **Fortsetzungen** sind zu bilden, wenn Klartexte aus praktischen Erwägungen geteilt werden. Jeder Teil ist als selbständiger Klartext zu bearbeiten.

Zur Kennzeichnung als ersten Teil erhält dieser um Ende den Buchstaben a mit nachfolgendem Fortsetzungsvermerk ff, der angibt, daß ein weiterer Teil folgt.

Jeder weitere Teil erhält zur Kennzeichnung als Fortsetzung in der Reihenfolge des Alphabets am Anfang des Textes einen der Buchstaben b, c, d ... und, außer dem letzten Teil, am Ende des Textes den Fortsetzungsvermerk ff.

Der erste Teil enthält die VS-Einstufung und den Empfänger, der letzte Teil den Absender und die 1. und 2. Wiederholung (Beispiel [10](#)).

3.10. **Bearbeitung von Telegrammen mit zirkularem und individuellem Text**

Bei zirkularen Telegrammen, in denen ein oder mehrere individuelle Textteile eingefügt sind, ist einerseits der gesamte zirkulare und andererseits der gesamte individuelle Text zusammenzuziehen und jeweils als ein zirkularer bzw. individueller Spruch zu bearbeiten.

Damit bei der Dechiffrierung der individuelle Textteil wieder eindeutig in den zirkularen eingefügt werden kann, sind bei der Chiffrierung im hergerichteten Klartext an den entsprechenden Stellen des zirkularen und individuellen Textes die gleichen Kennzeichen ia, ib ic ... nacheinander für die einzelnen Textteile einzusetzen. Die Kennzeichen sind vom eigentlichen Text durch den Indikator WR/Zl (Absatz) zu trennen.

Bei der Chiffrierung kann der Indikator WR/Zl (unter Berücksichtigung des Abschnittes [3.4.](#)) mehrmals hintereinander zwischen den einzelnen zirkularen bzw. den einzelnen individuellen Textteilen gesetzt werden, so daß die individuellen Textteile bei der maschinellen Dechiffrierung ohne manuelle Nebenarbeiten in den zirkularen Text eingefügt werden können.

4. **Herrichtung der Klartexte für rein manuelle Verbindungen**

Die Herrichtung der Klartexte erfolgt wie unter Abschnitt [3.](#) mit folgenden Einschränkungen (Beispiel [11](#)):

- 4.1. Die **Textanordnung** ist (mit Ausnahme von Absätzen) nicht mit zu chiffrieren.
- 4.2. Nachstehend aufgeführte **Indikatoren** erhalten folgende Bedeutung:
 - 4.2.1. „WR/Zl“ ist nur in der Form des Absatzes zu verwenden.
 - 4.2.2. „ZwR“ ist nur in der Form des Trennzeichens „#“ zu setzen:
 - zwischen aufeinanderfolgenden Wörtern, Zahlen usw., die als ein Ausdruck gelesen zu Sinnentstellungen führen können (Beispiel [12](#));
 - vor und nach allgemein gebräuchlichen Abkürzungen (Beispiel [13](#));
 - zwischen Namensteilen mehrteiliger fremdartiger Namen, deren Teilung nicht auf andere Art gekennzeichnet ist;
 - bei VS-Einstufung, Empfänger, Absender und den Wiederholungen, um diese Teile vom eigentlichen Text zu trennen (Beispiel [10](#));
 - bei Fortsetzungen (Beispiel [10](#));
sofern nicht bereits andere Indikatoren eine Trennung anzeigen (Beispiel [13](#)).
- 4.3. Entbehrliche **Interpunktionszeichen** sind wegzulassen.
- 4.4. **Codegruppen** müssen nicht fünfstellig sein.

5. Bildung des Zwischentextes

- 5.1. Die Buchstaben des hergerichteten Klartextes, außer j, q, x und y sind unverändert in den Zwischentext zu übernehmen. Die restlichen Klareinheiten (die Buchstaben j, q, x und y, Indikatoren, Phrasen, Ziffern und Zeichen) sind in der Reihenfolge ihres Auftretens durch die Buchstaben oder Buchstabengruppen (Zwischeneinheiten) zu ersetzen, die ihnen in der Substitutions-

tafel oder im Code zugeordnet sind (Beispiele [2](#), [5](#), [6](#), [7](#), [14](#)).

- 5.2. Der nur noch aus Buchstaben bestehende Zwischentext ist in der Regel in Fünfergruppen einzuteilen. Ist die letzte Gruppe nicht vollständig, ist sie durch beliebige Buchstaben, die den Sinn des Textes nicht entstellen, zu einer vollen Gruppe aufzufüllen (Beispiel [15](#)).

10

Chi 5187

GVS-6385/69 - Blatt 6 -

6. Chiffrierung

- 6.1. Zur **maschinellen Chiffrierung** des hergerichteten Klartextes ist als Additionsreihe der nächstfolgende noch nicht benutzte Schlüsselstreifenabschnitt (Beispiel [16](#)) zu verwenden. Die Bearbeitung hat gemäß der Bedienungsanweisung zum festgelegten Gerät zu erfolgen. Das Ergebnis der Chiffrierung ist der Chiffretext (Beispiel [17](#)).

- 6.2. Zur **manuellen Chiffrierung** des Zwischentextes ist als Additionsreihe die nächstfolgende noch nicht benutzte Wurmtabelle (Beispiel [16](#)) zu verwenden. **Jede Fünfergruppe der Wurmtabelle darf zur Chiffrierung nicht mehr als einmal benutzt werden.** Bei der Chiffrierung ist die Wurmtabelle zeilenweise so über dem Zwischentext anzulegen, daß unter jedem Buchstaben der Wurmtabelle (Wurmbuchstabe) ein Buchstabe des Zwischentextes steht. Durch den jeweiligen Wurmbuchstaben wird die zu verwendende Substitution der Additionstafel festgelegt (Komponente 1). Der unter dem Wurmbuchstaben stehende Zwischentextbuchstabe ist in der zur Substitution gehörigen Komponente 2 bzw. 3 aufzusuchen. Der in der Substitution darunter (in Komponente 3) bzw. darüber (in Komponente 2) stehende Buchstabe ist der Chiffretextbuchstabe. In dieser Weise ist der gesamte Zwischentext in Chiffretext umzusetzen (Beispiel [18](#)).

Reicht die Anzahl der Fünfergruppen einer Wurmtabelle zur Chiffrierung des Zwischentextes nicht aus, so ist die nächst-

folgende Wurmtabelle (beachte Abschnitte [2.3.2.](#) und [2.3.4.](#)) in gleicher Weise zu benutzen. Sind die Wurmtabellen eines Heftes/ einer Kassette verbraucht, so ist das/die nächstfolgende für diesen Verkehr vorgesehene Heft/Kassette zu benutzen (in der Regel das/die mit der nächsthöheren Seriennummer versehene Heft/Kassette).

Bleiben Fünfergruppen einer Wurmtabelle bei der Chiffrierung des Zwischentextes unbenutzt, so sind diese Fünfergruppen zur Bearbeitung eines anderen Spruches nicht mehr zu verwenden.

Benutzte Wurmtabellen sind nach Bearbeitung eines Spruches ungültig geworden und spätestens nach Ablauf der festgelegten Frist zu vernichten.

- 6.3. Jeder Wurmtabelle/jedem Schlüssellochstreifenabschnitt ist entsprechend der Numerierung eindeutig eine fünfstellige Buchstaben-
gruppe als Kenngruppe zugeordnet.

Die **Kenngruppen** sind aus der Kenngruppentafel (Beispiel [19](#)) spaltenweise von oben nach unten, in der Reihenfolge der Spalten von links nach rechts zu entnehmen. Die Kenngruppe, die der/dem zur Chiffrierung benutzten Wurmtabelle/Schlüssellochstreifenabschnitt zugeordnet ist, ist als erste Gruppe dem Chiffretext voranzustellen (vgl. Beispiele [16](#), [19](#) und [20](#)).

Werden zur Chiffrierung eines Zwischentextes/hergerichteten Klartextes mehrere Wurmtabellen/Schlüssellochstreifenabschnitte benutzt, so ist nur die Kenngruppe der/des ersten verwendeten Wurmtabelle/Schlüssellochstreifenabschnittes dem Chiffretext voranzustellen. Die Kenngruppen der anderen Wurmtabellen/Schlüssellochstreifenabschnitte bleiben unberücksichtigt.

Alle Kenngruppen, deren Wurmtabellen/Schlüssellochstreifenabschnitte zur Chiffrierung verwendet wurden, sind in der Kenngruppentafel zu streichen.

7. Dechiffrierung

- 7.1. Die erste Fünfergruppe im Spruch ist die **Kenngruppe** (Beispiel [20](#)). Anhand der Stellung der Kenngruppe in der gültigen Kenngruppen-
pentafel – die Kenngruppen spaltenweise von oben nach unten, in der Reihenfolge der Spalten von links nach rechts abgezählt – wird die Nummer der/des ersten für den Spruch benutzten Wurmtablette/Schlüssellochstreifenabschnittes bestimmt (vgl. Beispiele [16](#) und [19](#)). Die Kenngruppen, deren Wurmtablettens/Schlüssellochstreifenabschnitte zur Dechiffrierung des Spruches benutzt wurden, sind zu streichen.
- 7.2. Für die **maschinelle Dechiffrierung** des Chiffretextes ist als Additionsreihe der durch die Kenngruppe bestimmte Schlüssellochstreifenabschnitt zu verwenden. Die Bearbeitung hat gemäß der Bedienungsanweisung zum festgelegten Gerät zu erfolgen. Das Ergebnis der Dechiffrierung ist der Klartext (Beispiel [21](#)).
- 7.3. Für die **manuelle Dechiffrierung** des Chiffretextes ist als Additionsreihe die durch die Kenngruppe bestimmte Wurmtablette zeilenweise so über dem Chiffretext anzulegen, daß unter jedem Wurmbuchstaben ein Buchstabe des Chiffretextes steht. Durch den jeweiligen Wurmbuchstaben wird die zu verwendende Substitution der Additionstafel festgelegt (Komponente 1). Der unter dem Wurmbuchstaben stehende Chiffretextbuchstabe ist in der zur Substitution gehörigen Komponente 2 bzw. 3 aufzusuchen. Der in der Substitution darunter (in Komponente 3) bzw. darüber (in Komponente 2) stehende Buchstabe ist der Zwischentextbuchstabe. In dieser Weise ist der gesamte Chiffretext in Zwischentext umzusetzen (Beispiel [22](#)).

Reicht die Anzahl der Buchstaben der Wurmtablette zur Dechiffrierung nicht aus, so ist die nächstfolgende Wurmtablette (be-

achte Abschnitte [2.3.2.](#) und [2.3.4.](#)) in gleicher Weise zu benutzen. Sind die Wurmtabellen eines Heftes/einer Kassette verbraucht, so ist das/die nächstfolgende für diesen Verkehr vorgesehene Heft/Kassette zu benutzen (in der Regel das/die mit der nächsthöheren Seriennummer versehene Heft/Kassette).

Benutzte Wurmtabellen sind nach fehlerfreier Bearbeitung des Spruches und spätestens nach Ablauf der festgelegten Frist zu vernichten.

Anhand der im Zwischentext enthaltenen Indikatoren ist ersichtlich, welche Teile des Zwischentextes noch mittels der Substitutionstafel bzw. zusätzlich des Codes in Klartext umgewandelt werden müssen.

- 7.4. Entsprechend der Wiederholung und der Festlegungen im Abschnitt 3. sind die notwendigen **Korrekturen** im erhaltenen Klartext vorzunehmen (vgl. Beispiel [21](#) bzw. [22](#) mit [1](#)). Aus dem Textzusammenhang erkennbare Verstümmelungen sind zu berichtigen. Bei Berichtigung verstümmelter Codegruppen ist entsprechend den Hinweisen zur Berichtigung von Codegruppen des zugewiesenen Codes zu verfahren.

14

Chi 5187

GVS-6385/69 - Blatt 8 -

8. Rückfragen

Eine Rückfrage hat zu erfolgen, wenn in einem empfangenen Spruch Verstümmelungen enthalten sind, die nicht aus dem Zusammenhang oder mit Hilfe der Hinweise zur Berichtigung von Codegruppen des zugewiesenen Codes berichtigt werden können.

Die Rückfrage ist durch Angabe der Kenngruppe des Spruches und der Stellenzahlen der verstümmelten Fünfergruppen im Chiffretext durchzuführen (Beispiel [23](#)).

Eine andere Methode der Rückfrage ist nicht gestattet.

Verstümmelungen können auf zwei Arten berichtigt werden:

- a) Verwendung der/des gleichen Wurmtabelle/Schlüssellochstreifenabschnittes und bei unverändertem Klartext einfache Berichtigung der Verstümmelung;
- b) Verwendung einer/eines neuen Wurmtabelle/Schlüssellochstreifenabschnittes zur Chiffrierung desselben Textteiles.

Übermittlungsfehler und einzelne Chiffrierfehler, die bei der Berichtigung des Fehlers keine Verschiebung des Zwischentextes in Bezug auf die Additionsreihe ergeben, können nach a) oder nach b) berichtigt werden. **Andere Chiffrierfehler sind grundsätzlich nach b) zu berichtigen.**

15

9. Bearbeitung von Weiterleitungen

Weiterleitungen sind grundsätzlich nur gestattet, wenn keine direkte Chiffrierverbindung von einer Dienststelle zu einer anderen besteht bzw. die Chiffrierverbindung zeitweilig unterbrochen ist.

Der Spruch ist dann über die nächstvorgesetzte Dienststelle oder über eine andere Chiffrierstelle zu leiten. Von der absendenden Dienststelle sind der gesamte letztendliche Empfänger und der Absender zu chiffrieren. Die weiterleitende Dienststelle dechiffriert den Spruch und beginnt die Bearbeitung des Ausgangs (Weiterleitung) mit einer/einem neuen Wurmtabelle/Schlüssellochstreifenabschnitt.

Es sind der Empfänger und der gesamte ursprüngliche Absender zu chiffrieren.

16

Chi 5187

GVS-6385/65 - Blatt 9 -

10. Sicherheitsbestimmungen

<u>Vorkommnisse</u>	<u>Sofortmaßnahmen</u>
10.1. Kompromittierung von Klartext oder Zwischentext.	a) Vor Übermittlung Mitteilung an Absender der Nachricht. Weitere Bearbeitung erst nach Rücksprache mit diesem. b) Durch offene Übermittlung oder nach Übermittlung: Mitteilung an Absender und Empfänger der Nachricht.
10.2. Kompromittierung eines Exemplars einer Schlüsselserie.	a) Vor Übermittlung damit bearbeiteter Sprüche: Außerkraftsetzung aller Exemplare der betreffenden Schlüsselserie. b) Nach Übermittlung damit bearbeiteter Sprüche: Außerkraftsetzung aller Exemplare der betreffenden Schlüsselserie. Mitteilung an Absender und Empfänger übermittelte Nachrichten.
10.3. Kompromittierung von Additionsreihen (Wurmtabellen bzw. Schlüssellochstreifenabschnitte)	a) Vor Übermittlung: - Ausgangsmaterial: Betreffende Additionsreihen vernichten. Bereits bearbeitete Klartexte mit einer neuen Additionsreihe bearbeiten. - Eingangsmaterial: Mitteilung an absendende Chiffrierstelle. Additionsreihen des Eingangsexemplars in der Regel erst 48 Stunden nach Absetzen der Mitteilung vernichten. b) Nach Übermittlung: Mitteilung über Kompromittierung der betreffenden Textteile an Absender und Empfänger der Nachricht.
10.4. Wiederholte Benutzung einer Additionsreihe zur Chiffrierung.	a) Vor Übermittlung: Fehler korrigieren. b) Nach Übermittlung: - Chiffrierte Mitteilung über Kompromittierung der betreffenden Textteile an empfangende Chiffrierstelle und Mitteilung an Absender der Nachricht. - Mitteilung über Kompromittierung der betreffenden Textteile durch empfangende Chiffrierstelle an Empfänger der Nachricht.
10.5. Wiederholte Benutzung einzelner Wurmgruppen in einem Spruch.	a) Vor Übermittlung: Fehler korrigieren. b) Nach Übermittlung: Keine Sofortmaßnahme erforderlich. Bei Notwendigkeit chiffrierte Mitteilung an empfangende Chiffrierstelle.
10.6. Verschiebung des Zwischen-	a) Vor Übermittlung:

- textes bzw. des hergerichteten Klartextes (in der Folge Zwischentext) gegenüber der bereits verwendeten Additionsreihe bei Berichtigungen.
- 10.7. Verwendung des Eingangsexemplares zur Chiffrierung.
- 10.8. Verwendung der Kenngruppentafel als Additionsreihe.
- 10.9. Anwendung falscher kryptographischer Addition beim Chiffrieren (z. B. Verwendung einer anderen Additionstafel).
- 10.10. Einsetzen einer falschen Kenngruppe, Überschließung der Kenngruppe, Fehlen der Kenngruppe.
- 10.11. Kompromittierung der Additionstafel, der Substitutionstafel oder des Schlüsselcodes.
- 10.12. Kompromittierung der Kenn-
- Fehler korrigieren.
- b) **Nach Übermittlung:**
- Chiffrierte Mitteilung über Kompromittierung der betreffenden Textteile an absendende Chiffrierstelle und Mitteilung an Empfänger der Nachricht.
 - Mitteilung über Kompromittierung der betreffenden Textteile durch absendende Chiffrierstelle an Absender der Nachricht.
- a) **Vor Übermittlung:**
- Fehler korrigieren.
Mitteilung an empfangende Chiffrierstelle. Vernichtung der vorzeitig gelösten Additionsreihen des Eingangsexemplares in der Regel 48 Stunden nach Absetzen der Mitteilung.
- b) **Nach Übermittlung:**
- Bei Notwendigkeit chiffrierte Mitteilung an empfangende bzw. absendende Chiffrierstelle.
- a) **Vor Übermittlung:**
- Fehler korrigieren.
- b) **Nach Übermittlung:**
- Chiffrierte Mitteilung an Leitstelle. Leitstelle weist Außerkraftsetzung aller Exemplare der Schlüsselserie oder Verwendung einer noch nicht benutzten Wurmtabelle/Schlüssellochstreifenabschnittes als Kenngruppentafel an.
- a) **Vor Übermittlung:**
- Fehler korrigieren.
- b) **Nach Übermittlung:**
- Keine Sofortmaßnahmen erforderlich. Bei Notwendigkeit offene Mitteilung an empfangende Chiffrierstelle.
- a) **Vor Übermittlung:**
- Fehler korrigieren.
- b) **Nach Übermittlung:**
- Bei Notwendigkeit offene Mitteilung der richtigen Kenngruppe an empfangende Chiffrierstelle.
- Meldung erforderlich. Betreffende Additionstafel, Substitutionstafel oder Schlüsselcode bleiben in Kraft.
- Keine Sofortmaßnahmen erforderlich.

gruppentafel.

Anmerkung!

Ist die Mitteilung über Kompromittierung über Nachrichtenkanäle zu übermitteln, so ist sie zu chiffrieren.

21

11. Beispiele

Für die Bildung des Zwischentextes in den Beispielen wurde die Substitutionstafel TAXUS verwendet. Die Codegruppen sind frei gewählt.

Abkürzungen : KT = Klartext
hKT = hergerichteter Klartext
ZwT = Zwischentext
AdR = Additionsreihe
ChT = Chiffretext

Symbole für Indikatoren: vgl. Abschnitt 3.4.

Beispiel 1:

KT: VD 137
Deutsche Export- und Importgesellschaft
Feinmechanik-Optik m. b. H. Berlin
Gen. Müller

Nachfrage Preisverhandlung vom 24.5.
1. Preisverhandlung für Exportauftrag
124/4y/07143/66-kx 430041 fortführen
2. Vereinbarten Preis zu xxb Mikroskope akzeptieren
(Absprache mit Herrn Tien Ken Sin vom 4.3.
beachten)

Meierhoeft

hKT: vd ≠ » 137 ∅ ∅ ≈ deutsche ≠ export »-#
≈ und ≠ importgesellschaft ∅ feinmechanik »
-≈ optik ≠ m » . ≈ b » . ≈ h » . ≠ ≈ ber

lin Ø gen » . ≠ ≈ muller » Ø Ø ≈ nachfrage
≠ preisverhandlung ≠ vom ≠ » 24.5. Ø Ø 1.
Ø ≈ preisverhandlung ≠ fuer ≠ exportauftrag Ø
» 124/4 ≈ y » / 07143 / 66 - ≈ kx ≠ » 430
041 ≈ ≠ fortfuehren Ø » 2. Ø ≈ vereinbaren
≠ preis ≠ zu ≠ xxb ≠ mikroskope ≠ akzeptier
en Ø » (≈ absprache ≠ mit ≠ herrn ≠ tien ≠

22

Chi 5187

GVS-6385/69 - Blatt 12 -

ken ≠ sin ≠ vom » ≠ 4.3. ≈ ≠ beachten »)
Ø Ø ≈ meierhoeft » Ø Ø Ø Ø ≈ vd ≠ »
137 ≠ mueller ≠ » 245 ≠ 1244 ≈ y » 071
4366 ≈ kx » 430041 ≠ ≈ xxb Ø tien ≠ ken ≠
sin ≠ » 43 ≠ ≈ meierkoeoeft » Ø Ø I37 ≠
245 ≠ 12440714366 ≈ kx » 430 041 ≠ ≈ xxb
» ≠ 43

Beispiel 2:

KT: Zu 1.: Nachfrage bezüglich Exportauftrag Nr. ...
hKT: zu ≠ » 1 . ↑ nachfrage ≈ bezueglich
ZwT: zu y j e p hjw stuvw q bezueglich
hKT: ↑ exportauftrag nr »
ZwT: jw fsnae nr j P ...

Beispiel 3:

KT : ... ? ... hKT: ... fragezeichen ...
... § paragraph ...
... \$ dollar ...

Beispiel 4:

KT: ... werden 3 PKW am 14. des...
hKT: ... werden ≠ » 3 ≈ ≠ pkw ≠ am » ≠ 14.
≈ ≠ des ...
KT: ... PKW F9 IA 25-23 ...

hKT: ... pkw ≠ f » 9 ≈ ≠ ia ≠ » 25-23 ...
KT : ... ½ ... ⅓ ...
hKT: ... 1/2 ... 1/3 ...
oder: ... 0,5 ... ein ≠ drittel ...

Beispiel 5:

KT: ... ab 14.7. Alar**mbereitschaft** für ...
hKT: ... ab ↑ 14.7. ↑ alarmbereitschaft fuer ...
ZwT : ... ab jwdefgh jw klmno fuer ...

Beispiel 6:

KT: ... wurden über Xerox vervielfältigt ...
hKT: ... wurden ≠ ueber Ø » ≈ xerox ≠ ver ...
ZwT: ... wurden y ueber y j q xxeroxx y ver ...
KT: ... wohnhaft in York ...
hKT: ... wohnhaft ≠ in ≠ » ≈ york ...
ZwT: ... wohnhaft y in y j q yyork ...

Beispiel 7:

KT: ... in XVI/12. enthalten ...
hKT: ... in ≠ xvi » /12. ≈ ≠ enth ...
oder: ... in ≠ roem ≠ xvi » / 12. ≈ ≠ enth ...
ZwT: ... in y roem y xxvi j t ezp q y enth ...

Beispiel 8:

KT:	hKT:	Wdhlg :
..Fasz binderfaszbinder..	..faszszbinder..
..Saegers..	..saegers..	..saeaegers..

Beispiel 9:

KT:	hKT:	Wdhlg:
..Großenhain..	..grosenhain..	..groszenhain..
..Müller..	..muller..	..mueller..
..Bärenhof..	..barenhof..	..baerenhof..

Beispiel 10: Dreiteiliger KT:

1. Teil: VS-Einstufung Empfänger Text aff

- 2. Teil: b Text ff
- 3. Teil: c Text Absender 1. Wiederholung
 - 2. Wiederholung

24

Chi 5187

GVS-6385/69 - Blatt - 13 -

Beispiel 11: KT: Siehe Beispiel [1](#)

hKT: vd » 137 ≈ ∅ deutsche export und importges
 ellschaft ≠ feinmechanik optik ≠ mbh ≠ berlin
 ≠ gen ≠ muller ∅ nachfrage preisverhandlung
 vom » 24.5. ≠ 1. ≈ preisverhandlung fuer exp
 ortauftraq » 124/4 ≈ y » /07143/66 - ≈ kx
 ≠ » 430041 ≈ fortfuehren ≠ » 2. ≈ verein
 barten preis zu ≠ xxb ≠ mikroskope akzeptieren
 » (≈ absprahe mit herrn ≠ tien ≠ ken ≠ sin
 ≠ vom » 4.3. ≈ beachten ») ≈ ∅ meierhoeft
 ∅ vd » 137 ≈ mueller » 245 ≠ 1244 ≈ y »
 0714366 ≈ kx 430041 ≠ ≈ xxb ≠ tien ken
 sin » 43 ≈ meierhoeoeft » ∅ 137 ≠ 245 ≠
 12440714366 ≈ kx » 430041 ≈ xxb » 43

Beispiel 12:

KT: ... in Gerswalde ...
 hKT: ... in ≠ gerswalde ...

Beispiel 13: KT: Siehe Beispiel [4](#)

hKT: ... werden » 3 ≈ pkw ≠ am » 1 4. ≈ des ...

Beispiel 14: KT: Siehe Beispiel [1](#)

hKT: vd ≠ » 137 oo ≈ deutsche ≠ ex
 ZwT: vd y j edi xx q deutsche y exx

hKT: port » - ≠ ≈ und ≠ importgesell
 ZwT: port j b y q und y importgesell

hKT: schaft ∅ feinmechanik » - ≈ opt
 ZwT: schaft x feinmechanik j b q opt

hKT: ik ≠ m » . ≈ b » . ≈ h » . ≠ ≈ berlin
ZwT: ik y m j p q b j p q h j p y q berlin

hKT: Ø gen » . ≠ ≈ muller » 00 ≈ nac
ZwT: x gen j p y q muller j xx q nac

25

hKT: hfrage ≠ preisverhandlung ≠ v
ZwT: hfrage y preisverhandlung y v

hKT: om ≠ » 24.5. 00 1.0 ≈ preisve
ZwT: om y j zvpfp xx epq q preisve

hKT : rhandlung ≠ fuer ≠ exportauftr
ZwT : rhandlung y fuer y exxportauftr

hKT : ag0 » 124/4 ≈ y » /07143/66-
ZwT : agx j ezvtv q yyj toievdtsb

hKT: ≈ kx ≠ » 430041 ≈ ≠ fortfuehre
ZwT : q kxx y j vdoove q y fortfuehre

hKT: n0»2.0 ≈ vereinbarten ≠ pre
ZwT: nxjzpx q vereinbarten y pre

hKT: is ≠ zu ≠ xxb ≠ mikroskope ≠ ak
ZwT: is y zu y xxxxb y mikroskope y ak

hKT: zeptieren Ø » (≈ absprache ≠
ZwT: zeptieren x j cq absprache y

hKT: mit ≠ herrn ≠ tien ≠ ken ≠ sin ≠ v
ZwT: mit y herrn y tien y ken y sin y v

hKT: om » ≠ 4.3. ≈ ≠ beachten ») 0
ZwT: om j y vdpq q y beachten j g x

hKT: Ø ≈ meierhoeft » 0000 ≈ vd
 ZwT: x q meierhoeft j xxxx q vd

hKT: ≠ » 137 ≠ ≈ mueller ≠ » 245 ≠ 1
 ZwT: y j edi y q mueller y j zvf y e

hKT: 244 ≈ y » 0714366 ≈ kx » 43004
 ZwT: zvv q yyj oievdss q kxxj vdoov

hKT: 1 ≠ ≈ x x b Ø tien ≠ ken ≠ sin ≠
 ZwT: e y q xxxx b x tien y ken y sin y

hKT: » 43 ≠ ≈ meierhoeoeft » 00 13
 ZwT: j vd y q meierhoeoeft j xx ed

hKT: 7 ≠ 245 ≠ 12440714366 ≈ kx »
 ZwT: i y zvf y ezvvsievdss q kxxj

hKT: 430041 ≠ ≈ x x b » ≠ 43
 Zwt: vdoove y q xx xxb j y vd

26

Chi 5187

GVS-6385/69 - Blatt 14 -

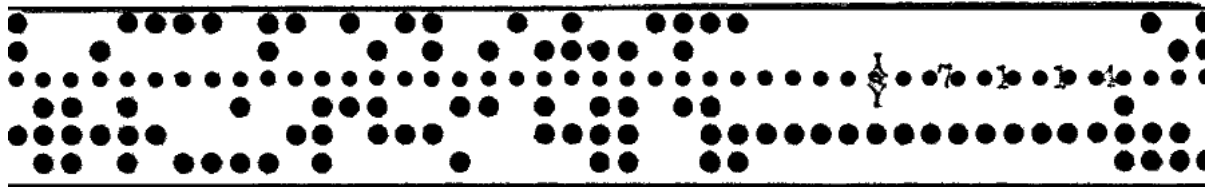
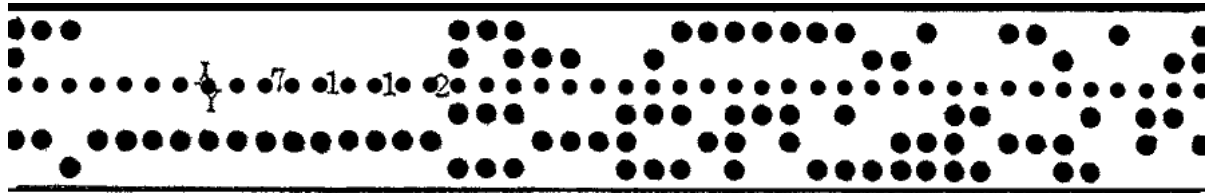
Beispiel 15: ZwT: Siehe Beispiel [14](#)
 Zwischentext in Fünfergruppen:

vdyje dixxq deuts cheye xxpor tjbyq undyi mport gesel lscha
 ftxfe inmec hanik jbqop tikym jpqbj pqhjp ypber linxg enjpy
 qnull erjxx qnach frage yprei sverh andlu ngyvo myjzv pfpxx
 epxqp reisv erhan dlung yfuer yexxp ortau ftrag xjezv tvqyy
 jtoie vdtss bqkxx yjvdo oveqy fortf uehre nxjzp xqver einba
 rteny preis yzuyx xxxby mikro skope yakze ptier enxjc qabsp
 rache ymity herrn ytien ykeny sinyv omjyv pdpqy beach tenjg
 xxqme ierho eftjx xxxqv dyjed iyqmu eller yjzvf yezvv qyyjo
 ievds sqkxx jvdoo veyqx xxxbx tieny kenys inyjv dyqme ierho
 eoeft jxxed iyzvf yezvv oievd ssqkx xjvdo oveqy xxxxb jyvdx

27

Beispiel 16:

Schlüssellochsteifenabschnitte 12 und 13 eines Schlüssellochstreifens mit je 250 Additionselementen



Wurmtabellen 12 und 13 eines Wurmtabellenheftes mit je 50 Wurmgruppen

```
qyqrr mpydx sfzyl gbmhd dghen
ijsod tyfch sticp kizdm ustuk
motty ooykt qylfy dnxsg awbbp
hwixo awqgx oxosu vwvwj zzibe
ruubi vseni tlzbh eihal vwlqs 05371
daenb zceib ubdaj gjxme gsxvh 12
yknvq cuyln zauqf Ixoln cxnhe
bsgpj sqgvn wzhej dnpvk umhpe
nkoie bdcma ihphj thspd oyweu
pppqa skffl hzcwa fepwa hbnvp
```

icrmt xlqwg fytql uroky wnlrg
ucpsv abelr xlrch jmrjp pnjbv
vcccn bkygu mzhcz sablj oqwjp
icrxq gqlqd nbaff toutb beluk
iimfo vpwpm xnmai jgaia wqkso 05371
inoyb qwpvy nxoft nkvpv vmylk 13
hvinm hdnws kdvdz ozfto domyr
slpdm hblqs lkrna ogqls rjxip
veskh lqzdm jkyjj hclrr tyvjm
mrxdz zhwdm scdjh iecjv veuxb

Beispiel 17: hKT: Siehe Beispiel [1](#)

ChT: oylze kcezm eqgiw rrj..
..... ..itz tcssc uyatd vxkzb

Beispiel 18:

ZwT: Siehe Beispiel [15](#)
AdR: qyqrr mpydx sfzyl gbmhd dgh..
ZwT: vdyje dixxq deutz cheye xxp..
ChT: oylze kcezm eqgiw rrjus zwd..

AdR: ..xdz zhwdm scdjh iecjv veuxb
ZwT : ..qkx xjvdo oveqy xxxxb jyvdx
ChT: ..mmd djitz tcssc uyatd vxkzb

Beispiel 19:

Kenngruppentafel:

kdgiz wwszv dydag yewta hrfar
uinli yewte ncmbq ajtny kljrrj
bccth igate ippys kpcau zqacr
larko exyja yuque yrsmk iecyj

zflen tdsgi hogav wyzdw clkyq 05371
tirbi omkud mwvrm hprvn rwrzs
prjts xxpii xdkmj hnqzx igqnd
ojooy acuqi itvkk rahqd qeiyh
njoue erzoz mbobm iysbn vhzxz
edkip oiliv idryc jxlcy smbjs

Beispiel 20: ChT: Siehe Beispiel [17](#) bzw. [18](#)

Kenngruppe: yewte

Spruch: yewte

oylze kcezm eqgiw rrjus zwd..
..mmd djitz tcssc uyatd vxkzb

30

Chi 5187

GVS-6385/69 - Blatt 16 -

Beispiel 21: Spruch: Siehe Beispiel [20](#)

vd 137

deutsche export- und importgesellschaft
feinmechanik-optik m.b.h. berlin
gen.muller

nachfrage preisverhandlung vom 24.5.

1.

preisverhandlung fuer exportauftrag
124/4y/07143166-kx 430041 fortfuehren

2.

vereinbarten preis zu xxb mikroskope akzeptieren
(absprache mit herrn tien ken sin vom 4.3. beachten)

meierhoeft

vd 137 mueller 245 1244y0714366kx430041 xxb
tien ken sin 43 meierhoeoft
137 245 12440714366kx430041 xxb 43

Beispiel 22: Spruch: Siehe Beispiel [20](#)

Kenngruppe: yewte

AdR: qyqrr mpydx sfzyl qbm..

ChT: oylze kcezm eggiw rrj..

ZwT: vdyje dixxq deuts che..

hKT: vd#>>1 3700~- deuts che..

KT: VD 137 Deutsche

AdR: ..wdm scdjh iecjv veuxb

ChT: ..itz tcssc uyatd vxkzb

ZwT: ..vdo ovevq xxxxb jyvdx

hKT: ..430 041#≈ x x b >># 43 0

KT: .. 430041 xxb 43

Beispiel 23:

Vom Spruch mit der Kenngruppe lbkqm sind die 14.
bis 18. und die 23. bis 26. Gruppe fehlerhaft.

Kückfrage: lbkqm a) 14-18 b) 23-26

Antwort: lbkqm a) 14-18 b) 23-26

a) pfuhd gwnbd rvwyh xgcdo edolz

b) qkcdv mrgut eexrb sjuey

A	B	C	D	E	F	G	H	I	J	K	L	M													
A	Z	A	Y	A	W	A	B	A	T	A	S	A	R	Q	P	A	O	A	N						
B	X	B	X	B	V	B	U	B	R	B	Q	B	Q	Q	P	O	N	B	M						
C	X	C	W	C	U	C	T	C	R	C	Q	C	Q	Q	P	O	N	C	M						
D	Y	D	V	D	T	D	S	D	R	D	Q	D	Q	Q	P	O	N	D	M						
E	Y	E	U	E	S	E	R	E	Q	E	Q	E	Q	Q	P	O	N	E	M						
F	T	F	S	F	R	F	Q	F	Q	F	Q	F	Q	Q	P	O	N	F	M						
G	S	G	R	G	Q	G	P	G	P	G	P	G	P	G	P	G	P	G	P						
H	R	H	Q	H	P	H	O	H	M	H	L	H	L	H	L	H	L	H	L						
I	Q	I	P	I	O	I	N	I	M	I	L	I	L	I	L	I	L	I	L						
J	P	J	O	J	N	J	M	J	L	J	K	J	K	J	K	J	K	J	K						
K	O	K	N	K	M	K	L	K	L	K	J	L	K	J	L	K	J	L	K						
L	N	L	M	L	K	L	M	L	K	L	J	M	L	K	L	J	M	L	K						
M	N	M	L	M	K	M	J	M	K	M	J	N	M	K	M	J	N	M	K						
N	O	N	K	N	O	N	J	N	O	N	J	H	N	O	N	J	H	N	O						
O	P	O	J	O	P	O	H	O	P	O	H	G	O	P	O	H	G	O	P						
P	K	P	J	P	H	P	G	P	H	P	G	F	P	H	P	G	F	P	H						
Q	J	Q	I	Q	H	Q	F	Q	H	Q	F	E	Q	H	Q	F	E	Q	H						
R	H	R	G	R	F	R	E	R	E	R	E	D	R	E	R	E	D	R	E						
S	G	S	F	S	E	S	D	S	E	S	D	C	S	E	S	D	C	S	E						
T	F	T	E	T	D	T	C	T	D	T	C	B	T	D	T	C	B	T	D						
V	W	V	D	V	C	V	B	V	A	V	Z	W	V	A	V	Z	W	V	A						
W	D	W	C	W	B	W	A	W	Z	W	Y	X	W	Z	W	Y	X	W	Z						
X	C	X	B	X	A	X	Z	X	Y	X	Y	X	Y	X	Y	X	Y	X	Y						
Y	B	Y	A	Y	Z	Y	X	Y	X	Y	X	Y	X	Y	X	Y	X	Y	X						
Z	A	Z	Z	Z	X	Z	Y	Z	X	Z	Y	Z	X	Z	Y	Z	X	Z	Y						
N	O	P	Q	R	S	T	U	V	W	X	Y	Z													
A	M	A	L	A	K	A	J	A	I	A	H	A	G	A	F	A	E	A	D	A	C	A	B	A	A
B	L	B	K	B	J	B	I	B	H	B	G	B	F	B	E	B	D	B	C	B	B	B	B	B	B
C	K	C	J	C	I	C	H	C	G	C	F	C	E	C	D	C	C	C	C	C	C	C	C	C	C
D	J	D	I	D	H	D	G	D	F	D	E	D	D	D	D	D	D	D	D	D	D	D	D	D	D
E	I	E	H	E	G	E	F	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
F	H	F	G	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
G	F	G	E	G	E	G	D	G	C	G	B	G	A	G	H	G	I	G	J	G	K	G	L	G	M
H	E	H	D	H	C	H	B	H	A	H	Z	H	Y	H	X	H	W	H	V	H	U	H	T	H	S
I	D	I	C	I	B	I	A	I	Z	I	Y	I	X	I	W	I	V	I	U	I	T	I	S	I	R
J	C	J	B	J	A	J	Z	J	Y	J	X	J	W	J	V	J	U	J	T	J	S	J	R	J	Q
K	B	K	A	K	Z	K	Y	K	X	K	W	K	V	K	U	K	T	K	S	K	R	K	Q	K	P
L	A	L	Z	L	X	L	W	L	V	L	U	L	T	L	S	L	R	L	Q	L	P	L	O	L	N
M	Z	M	Y	M	X	M	W	M	V	M	U	M	T	M	S	M	R	M	Q	M	P	M	N	M	N
N	Y	N	X	N	W	N	V	N	U	N	T	N	S	N	R	N	Q	N	P	N	O	N	N	N	N
O	X	O	W	O	V	O	U	O	T	O	S	O	R	O	Q	O	P	O	N	O	N	O	N	O	N
P	W	P	V	P	U	P	T	P	S	P	R	P	Q	P	Q	P	Q	P	N	P	M	P	L	P	L
Q	V	Q	U	Q	T	Q	R	Q	R	Q	R	Q	R	Q	R	Q	R	Q	N	Q	M	Q	K	Q	K
R	U	R	T	R	S	R	Q	R	P	R	O	R	N	R	O	R	N	R	O	R	N	R	J	R	J
S	T	S	R	S	Q	S	P	S	O	S	P	S	O	S	P	S	O	S	P	S	O	S	J	S	J
T	U	T	S	T	Q	T	U	T	P	T	O	T	N	T	U	T	N	T	U	T	N	T	I	T	I
V	R	V	Q	V	P	V	O	V	N	V	M	V	L	V	K	V	J	V	I	V	H	V	G	V	G
W	Q	W	P	W	O	W	N	W	M	W	L	W	K	W	J	W	I	W	H	W	G	W	F	W	F
X	P	X	O	X	N	X	M	X	L	X	K	X	J	X	I	X	H	X	G	X	F	X	E	X	E
Y	O	Y	N	Y	M	Y	L	Y	K	Y	J	Y	I	Y	H	Y	G	Y	F	Y	E	Y	D	Y	D
Z	N	Z	M	Z	L	Z	K	Z	J	Z	I	Z	H	Z	G	Z	F	Z	E	Z	D	Z	C	Z	C

1	SYZAH	TWUOG	KIXSH	BOBHU	TYRGO
2	GIGUA	VBFAS	HCSTR	IHKJU	CXHUB
3	ZIEZA	UFGGY	WPKY	SZBHJ	LIYAS
4	JNHBY	KCKR	DRPKJ	PHYBU	ZUKNA
5	JENHU	HVAUP	XSHXR	SGGSV	YFJXG
6	GFTGC	PVCST	PHRLY	HCEUS	YHONP
7	GQFTL	TPOZY	HKSVT	RXPJH	HSNKH
8	DRCKU	TZEZO	GNTBZ	QYQZA	JHTAH
9	TEUKS	GPPTI	PBFGE	CCQVV	KUEGR
10	QZROL	DEPEA	KFBQO	TUCRF	NBRKH

11.6. Aufbau des Chiffre IDEAL. BStU ^{*215}

E 145

Gebrauchsanweisung zur Chiffre „Ideal“

Die Chiffre „Ideal“ dient zur Überschlüsselung des Codes „Aster“.

1. Chiffriermittel

Chiffriermittel sind eine Chiffriertafel, zwei Gitter und zwei Chiffrierblocks.

Zum Chiffrieren wird das rote Gitter benutzt, zum Dechiffrieren eines Spruches von einer polnischen Stelle dient das gelbe Gitter, von einer deutschen Stelle das rote Gitter. Jedes Gitter enthält 10 Arbeitsfelder in horizontaler Richtung und 10 Arbeitsfelder in vertikaler Richtung. Benutzt werden jeweils nur die in horizontaler Richtung liegenden Arbeitsfelder. Zum Chiffrieren wird die rote, zum Dechiffrieren der blaue Chiffrierblock benutzt.

2. Chiffrierung

Der Klartext, wird nach dem Code „Aster“ in Codegruppen umgesetzt und diese in die jeweils ersten Zeilen der fünf Zeilengruppen auf dem oberen Teil eines Blattes im roten Chiffrierblock übernommen.

Das rote Gitter wird mit dem festgelegten Anlegepunkt an einer beliebigen Stelle der Chiffriertafel angelegt. Die Stelle der Chiffriertafel wird in der Kenngruppe festgehalten, die als erste Gruppe in den unteren Teil des roten Chiffrierblockes eingetragen und als erste Gruppe

Zeile von links nach rechts abgelesen und unter die Codegruppen im roten Chiffrierblock geschrieben.

Es werden nur die Arbeitsfelder benutzt, in denen genau drei Ziffern sichtbar sind.

Sind mehr Codegruppen zu überschlüsseln, als bei einer Anlage des roten Gitters Zifferngruppen aus den Arbeitsfeldern abgelesen werden können, so wird der Anlegepunkt des Gitters in der gleichen Spalte der Chiffriertafel um ein Feld nach unten verschoben. Die in den Arbeitsfeldern sichtbar werdenden 3-stelligen Zifferngruppen werden in der gleichen Weise wie vorher behandelt. So wird fortgefahren, bis unter jeder Codegruppe eine Zifferngruppe steht.

Die neuen Anlegepunkte des Gitters werden nicht durch eine besondere Kenngruppe festgelegt.

Die im roten Chiffrierblock auf dem oberen Teil des Blattes jeweils untereinander stehenden Ziffern werden kryptographisch addiert (z. B. $9 + 5 = 4$, $4 + 6 = 0$ usw.) Die einzelnen Summen werden auf den unteren Teil des Blattes übertragen. Hier werden die Ziffern automatisch in Fünfergruppen einteilt.

Der untere Teil des zur Chiffrierung im roten Chiffrierblock benutzten Blattes wird abgetrennt

des Spruches gesandt wird.

und dem Funker übergeben.

Es ist strengstens verboten, für verschiedene Sprüche das gleiche Anlegefeld in der Chiffrier-tafel zu wählen.

Die Kenngruppe besteht aus den folgenden fünf Buchstaben:

1. Buchst.: Einer der drei Zeilenbuchstaben des Großquadrates der Chiffrier-tafel, in dem sich das Anlege-feld befindet.
2. Buchst.: Einer der vier Spaltenbuchstaben des Großquadrates.
3. Buchst.: Der Zeilenbuchstabe des Anlege-feldes.
4. Buchst.: Der Spaltenbuchstabe des An-legefeldes.
5. Buchst.: Einer der drei Buchstaben, die den festgelegten Anlegepunkt des Gitters bezeichnen.

Die in den horizontalen Arbeitsfeldern sichtbar werdenden 3-stelligen Zifferngruppen werden in der Reihenfolge von oben nach unten, in der

3. Dechiffrierung

Der Geheimtext wird in die jeweils ersten Zeilen der fünf Zeilengruppen auf einem Blatt des blauen Chiffrierblocks eingetragen. An Hand der Kenngruppe wird das Anlegefeld in der Chiffrier-tafel und der Anlegepunkt des verwendeten Git-ters bestimmt. Die einzelnen Buchstaben der Kenngruppe haben die in 2 beschriebene Bedeu-tung.

Kommt der Spruch von einer deutschen Stelle, so ist zur Dechiffrierung das rote Gitter, kommt er von einer polnische Stelle, das gelbe Gitter zu verwenden. In derselben Weise wie beim Chiffrieren wird das Gitter gehandhabt und die 3-stelligen Zifferngruppen unter den Geheimtext im blauen Chiffrierblock geschrieben.

Die jeweils untereinander stehenden Ziffern wer-den kryptographisch subtrahiert (z. B. $6 - 8 = 8$, $3 - 4 = 9$ usw.) Die einzelnen Differenzen werden in die stritte Zeile geschrieben. Die dort ab-geteilten 3-stelligen Zifferngruppen sind die Codegruppen.

IDEAL		UXCE	MPGW	ARZT	KHSF	DIQV	NLOB
2		OIUAE	OUIEA	OAEUI	IAUEO	UAIQE	AEIUO
	I	3 9 6 1 0	7 5 8 2 4	8 0 1 2 7	9 5 6 4 3	8 0 7 1 5	6 2 4 9 8
D	U	1 4 8 6 3	9 0 2 7 5	2 4 6 8 0	7 9 5 3 1	5 8 2 9 6	3 7 0 4 1
P	O	9 2 7 0 8	3 5 6 1 4	0 8 1 6 5	9 4 7 2 3	0 1 9 3 8	4 7 2 6 5
Q	E	7 1 3 6 5	8 2 7 4 0	6 5 9 1 3	7 5 1 9 2	6 4 0 8 7	5 4 6 1 9
	A	4 6 8 1 3	9 5 0 7 2	1 2 3 4 5	6 7 0 8 9	4 8 6 1 3	5 9 7 0 2

N C T	E	0 3 2 8 6	1 4 7 5 9	6 2 0 1 9	8 5 4 7 6	3 8 1 3 4	6 0 2 9 5
	O	7 1 5 3 0	4 6 9 2 8	1 6 4 7 3	9 8 5 2 0	4 6 0 9 8	1 7 5 2 3
	I	2 0 6 1 9	3 8 4 7 5	0 8 2 9 5	7 3 1 4 9	8 2 3 6 7	4 5 1 0 6
	A	5 8 2 6 7	0 1 3 9 4	5 6 1 7 2	8 3 9 5 4	0 6 7 1 0	9 3 6 8 4
	U	6 1 9 7 5	4 3 8 2 0	7 3 8 1 5	9 4 0 2 6	9 4 5 7 2	8 3 0 4 1
V E U	A	8 6 4 2 1	3 0 5 7 9	8 1 9 2 0	7 3 6 4 5	2 9 7 8 6	5 4 1 3 2
	I	3 9 8 7 5	6 2 0 1 6	2 8 1 3 5	0 9 7 4 7	0 2 9 1 8	3 5 6 7 4
	O	9 5 3 8 1	7 4 6 0 2	8 3 7 4 6	1 5 0 9 2	4 5 7 6 1	0 7 4 3 9
	U	0 9 8 7 4	6 5 3 2 1	4 6 8 9 7	3 1 5 2 0	3 6 1 8 5	7 2 9 4 0
	E	1 6 4 9 3	0 2 7 8 5	3 2 7 5 9	1 8 6 0 2	4 5 2 7 0	3 8 1 9 6
W H G	E	4 7 0 8 2	6 5 1 9 3	7 5 2 2 0	3 6 9 1 7	2 8 5 6 1	9 2 3 0 4
	A	5 2 8 9 1	3 4 0 6 7	2 0 9 1 7	8 5 3 6 4	9 3 7 5 1	6 0 4 2 8
	O	7 8 9 6 5	4 0 3 2 1	8 4 9 2 6	3 7 1 0 5	7 3 4 6 8	2 9 5 1 0
	I	6 4 2 8 1	9 3 5 8 0	1 2 3 4 5	6 8 7 9 0	5 9 4 8 3	0 2 7 6 5
	U	8 1 6 3 0	7 5 4 2 9	6 5 4 1 9	3 7 2 5 4	6 8 1 0 3	7 2 9 4 7
I A F	A	0 9 3 4 8	6 7 2 1 5	8 3 6 1 0	4 5 2 7 9	1 3 5 7 9	0 8 6 4 2
	I	2 7 9 3 5	8 1 6 0 3	2 5 0 8 4	9 6 7 1 3	8 4 9 3 7	2 6 0 5 1
	U	9 6 3 8 4	2 0 5 7 1	3 8 4 7 0	2 5 6 9 1	7 2 6 5 4	0 1 8 0 9
	E	5 2 7 4 6	0 9 3 1 8	4 9 6 1 3	5 7 2 8 0	2 4 7 0 5	6 9 8 1 3
	O	1 6 3 9 2	4 5 0 8 7	2 0 8 6 5	4 1 3 7 9	5 6 9 1 4	8 0 2 7 5
S X K	A	2 9 1 8 3	7 4 6 5 0	1 3 6 8 2	4 7 0 9 5	7 1 0 8 2	9 3 4 5 6
	I	7 3 6 0 9	4 5 1 2 8	5 6 7 3 0	9 8 1 6 2	9 2 6 4 0	3 8 5 7 1
	U	3 6 7 2 5	8 0 4 1 2	8 3 5 9 6	7 0 4 2 1	0 9 1 2 8	7 4 3 6 2
	E	8 2 6 3 0	4 9 5 7 1	0 9 8 7 5	4 6 2 1 6	3 4 5 7 1	8 2 9 3 0
	O	6 9 2 7 9	1 3 0 4 5	8 1 9 2 7	3 4 6 5 0	9 2 1 5 6	4 3 0 7 8
B R L	E	0 3 9 2 4	7 5 8 1 6	2 4 6 8 0	9 7 5 3 1	2 5 3 8 1	0 9 4 6 7
	A	9 8 6 5 2	1 0 7 3 4	0 8 5 2 6	4 1 9 7 3	4 7 5 3 2	8 6 1 0 9
	O	4 7 0 9 3	6 5 2 8 1	5 9 2 8 3	6 4 7 1 0	3 5 4 2 6	0 9 7 8 1
	U	6 4 8 2 0	9 8 5 7 5	9 4 5 4 0	5 6 0 4 8	9 4 5 6 8	9 0 5 4 2
	I	4 8 5 9 4	5 9 4 8 9	5 8 4 5 6	8 5 4 6 5	6 8 6 8 2	6 4 8 6 8
O Z	E	1 3 5 7 9	0 8 6 4 2	3 0 2 8 1	4 7 5 9 6	8 1 4 7 0	5 9 2 3 6
	U	5 0 9 2 8	3 7 1 6 4	8 5 3 9 0	7 6 4 5 1	0 8 3 9 6	8 4 2 5 7

M	O	2 7 0 1 4	8 5 9 3 6	0 3 6 8 5	1 0 3 7 9	1 3 0 4 8	6 5 7 2 9
	I	9 2 8 3 7	4 6 5 0 1	4 8 6 9 8	7 4 2 8 7	2 5 8 2 0	4 6 2 3 7
	A	0 9 6 3 8	5 2 4 9 7	0 1 4 3 9	2 5 7 6 8	3 1 0 9 2	8 4 7 5 6

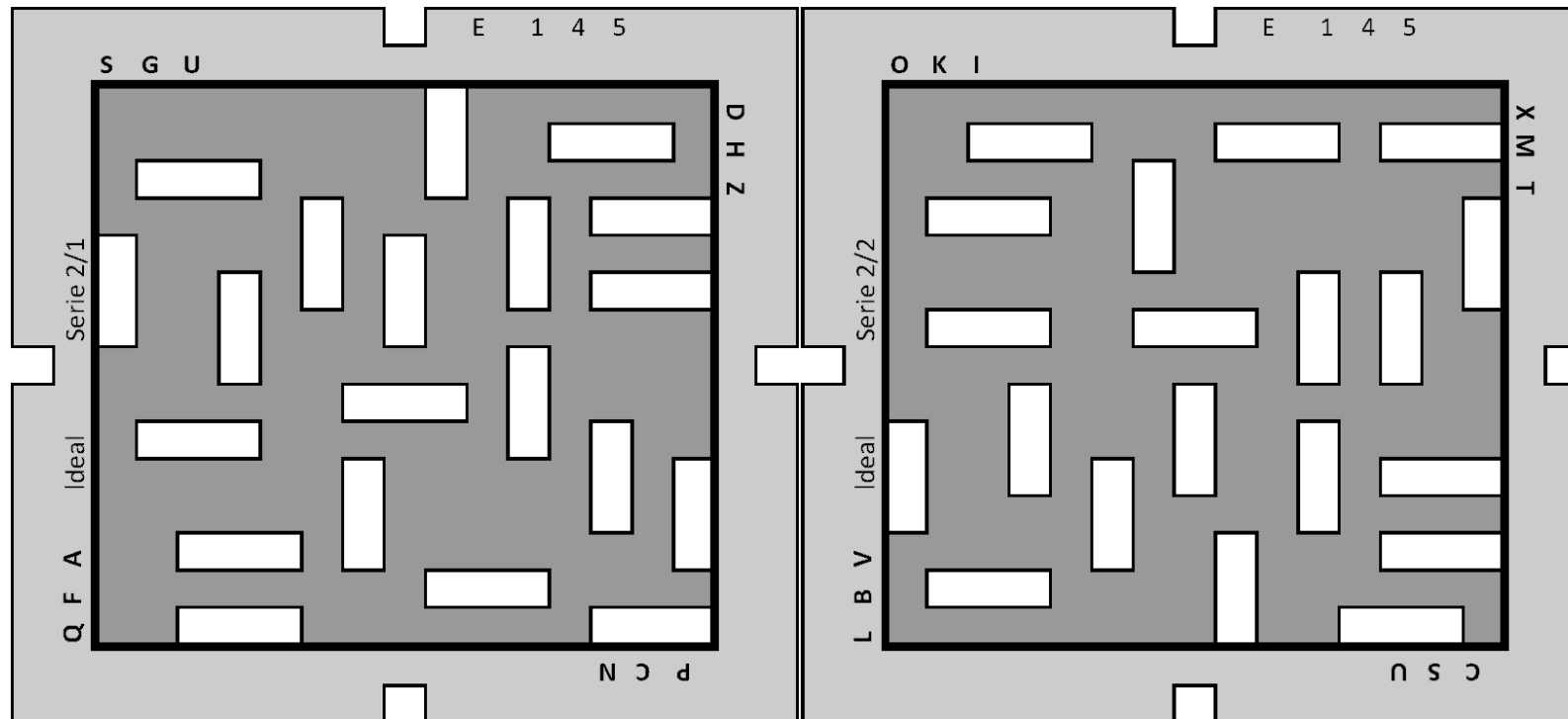


Abb.: Rotes Gitter und gelbes Gitter

11.7. Schlüssel FORMAT ^{BSTU *225}

Referat 1/E

Berlin, den 25.3.1960

Anweisung zur Herstellung der Schlüsselunterlagen für das Chiffre-
verfahren "Format"

1 Verfahren

Das Verfahren "Format" ist ein Mehrfachwurmverfahren als Ziffern-

verfahren. Es dient zur Überschlüsselung des Codes "009". Aus einer Chiffretafel wird unter Benutzung eines Gitters eine Additionsreihe abgelesen, dem Codetext zugeordnet und auf diese Weise der Chiffretext gebildet.

2 Aufbau der Schlüsselunterlagen

21 Aufzählung der Schlüsselunterlagen, die zu einer Schlüsselserie gehören

Zu einer Schlüsselserie gehören beim Verfahren "Format" als Schlüsselunterlagen eine Chiffretafel und ein Gitter, die zur Bildung von Additionsreihen dienen.

22 Aufbau der Chiffretafel

die Chiffretafel enthält 40 Zeilen und 30 Spalten, die zu 48 Quadraten mit je 5 Zeilen und 5 Spalte zusammengefaßt sind. In jedem Feld der Chiffretafel steht eine der Ziffern von 0 - 9. Die Ziffern befinden sich in zufälliger Anordnung. Die Wahrscheinlichkeit für das Auftreten einer der 10 Ziffern in einem beliebigen Feld der Chiffretafel beträgt 1/10.

Die 6 nebeneinander liegenden Quadrate in der Chiffretafel bilden eine Quadratzeile, die 8 untereinanderliegenden Quadrate eine Quadratspalte. Die 8 Quadratzeilen der Chiffretafel sind mit je drei Buchstaben, die 6 Quadratspalten der Chiffretafel mit je 4 Buchstaben des reduzierten deutschen Normalalphabetes (ohne Y und J) ohne Wiederholungen in zufälliger Reihenfolge bezeichnet.

Die 5 Zeilen einer Quadratzeile sind links von den Quadraten mit je einem der 5 Vokalen A, E, I, O, U ohne Wiederholungen in zufälliger Reihenfolge bezeichnet. Die 5 Spalten einer Quadratspalte sind oberhalb der Quadrate mit je einem der 5 Vokale A, E, I, o, U ohne Wiederholungen in zufälliger Reihenfolge bezeichnet.

Die Chiffretafel trägt in der linken oberen Ecke die Aufschrift

FORMAT

.... (Seriennummer)

23 Aufbau des Gitters

Das Gitter enthält ein Quadrat aus 15 Zeilen und 15 Spalten, in dem 10 Arbeitsfelder in horizontaler Richtung und 10 in vertikaler Richtung ausgestanzt sind. Jedes Arbeitsfeld

besteht aus 3 Gitterfeldern. Die horizontalen und die vertikalen Arbeitsfelder einer Gitterlage überschneiden sich teilweise. Arbeitsfelder, die sich nicht überschneiden, grenzen nicht direkt aneinander. Die Anordnung der Arbeitsfelder des Gitters ist unsystematisch und asymmetrisch in Bezug auf die beiden Achsen und die beiden Diagonalen des Gitters. Dadurch überdecken sich bei den 8 verschiedenen Lagen, in die ein Gitter durch Drehen um die beiden Achsen und durch Wenden gebracht werden kann, keine zwei Arbeitsfelder völlig.

An den Kanten des Gitters ist in der Mitte je ein Feld ausgestanzt, das Anlegepunkt genannt wird. Die 8 Anlagepunkte des Gitters (beiderseits) sind jeweils links von Anlegepunkt mit je drei der Buchstaben des reduzierten deutschen Normalalphabetes (ohne J und Y) ohne Wiederholung in zufälliger Reihenfolge bezeichnet.

Das Gitter trägt an je einer Gitterkante beiderseitig die Aufschrift

FORMAT Serie ... (Seriennummer)

3 Herstellung der Schlüsselunterlagen

31 Herstellung der Chiffretafeln

311 Je 150 Stück der Ziffern 0 - 9 werden in einen Karton gelegt, gemischt, willkürlich nacheinander herausgezogen und in der gezogenen Reihenfolge zur Bildung der Ziffernzeilen einer Chiffretafel benutzt, bis die für die Chiffretafel benötigten 1200 Ziffern ausgewählt sind.

Die 24 Buchstaben des reduzierten deutschen Normalalphabetes ohne J und Y werden in einen Karton gelegt, getauscht, willkürlich nacheinander herausgezogen und in der gezogenen Reihenfolge zur Bezeichnung der 8 Quadratzeilen der Chiffretafel benutzt. Zu jeder Quadratzeile gehören 3 untereinanderstehende Buchstaben.

Die 24 Buchstaben des reduzierten deutschen Normalalphabetes ohne J und Y werden in einen Karton gelegt, gemischt, willkürlich nacheinander herausgezogen und in der gezogenen Reihenfolge zur Bezeichnung der 6 Quadratspalten der Chiffretafel benutzt. Zu jeder Quadratspalte gehören 4 nebeneinanderstehende Buchstaben.

Die 5 Buchstaben A, E, I, O, U werden in jeden 14 Kartons

gelegt und in jedem Karton gemischt. Die Buchstaben aus 8 Kartons dienen zur Bezeichnung der Zeilen der Quadrate der Chiffretafel, die Buchstaben aus den übrigen 6 Kartons zur Bezeichnung der Spalten der Quadrate der Chiffretafel, indem die Buchstaben willkürlich nacheinander aus je einem Karton herausgezogen und in der gezogenen Reihenfolge eingesetzt werden.

312 der in 311 beschriebene Vorgang wird für jede herzustellende Chiffretafel wiederholt.

32 Herstellung der Gitter

321 Herstellung von vordrucken für Gittervorlagen

Zur Herstellung von Gittervorlagen, nach denen in Ref. 5 die Gitter angefertigt werden, werden Vordrucke verwendet. Die Vordrucke tragen die Aufschrift

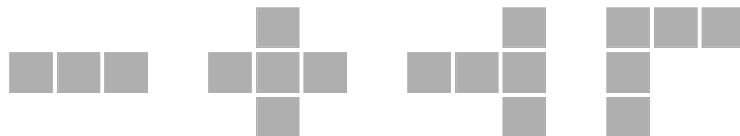
Vordruck	FORMAT
----------	--------

Sie enthalten ein Quadrat aus 15 Zeilen und 25 Spalten. die Felder der Haupt- und Nebendiagonale, der 8. Zeile und der 8. Spalte sind fett umrahmt, die übrigen Felder mager. Die Felder des Vordruckes entsprechen in ihrer Größe den Feldern des Gitters in Originalgröße. Die Größe des Vordruckes entspricht DIN A6.

Für die Vordrucke wird durchsichtiges Papier verwendet.

322 Herstellung der Gittervorlagen

Die Arbeitsfelder eines Gitters (10 in horizontaler Richtung und 10 in vertikaler Richtung) werden - bis auf die Beachtung einiger Bedingungen - unsymmetrisch unter Benutzung der Figuren

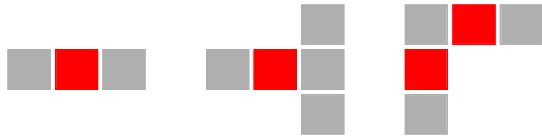


in einen Vordruck - den Gittervorlagenentwurf - eingetragen. Die zu beachtenden Bedingungen sind folgende:

1) Asymmetrie der Lage der Arbeitsfelder zu den beiden Achsen und der Haupt- und der Nebendiagonale des Quadrats.
das wird dadurch erreicht, daß

a) kein ganzes (horizontales oder vertikales) Arbeitsfeld in eine der beiden Achsen eingetragen wird,

b) keines der rot gezeichneten Felder die Figuren



in eine der beiden Achsen und keines der rot gekennzeichneten Felder der Figuren



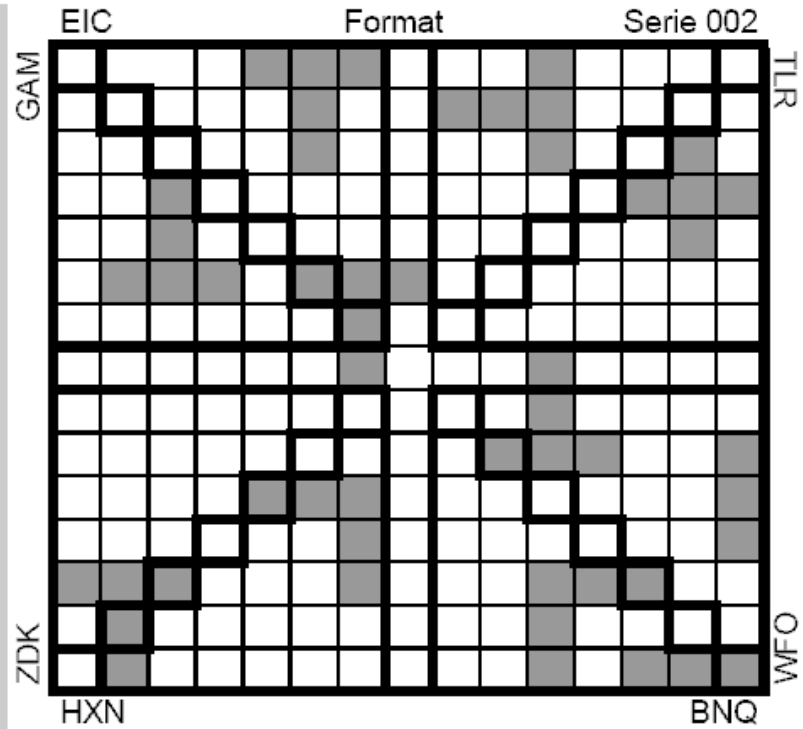
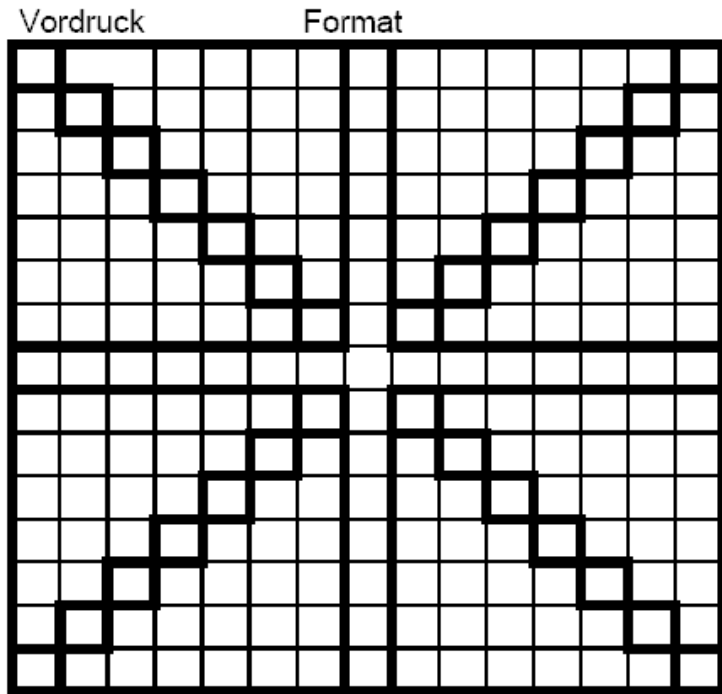
in die Haupt- oder Nebendiagonale eingetragen wird.

c) Nach Eintragung einer Figur in den Vordruck alle zu dieser Figur in Bezug auf die beiden Achsen und die Haupt- und die Nebendiagonale spiegelsymmetrischen Felder deutlich sichtbar und unterschiedlich in der Farbe zur Eintragung der Figur ausgestrichen werden und keine drei zusammenhängenden Felder, die einmal auf diese Art in einem Vordruck ausgestrichen wurden, erneut als Arbeitsfelder bei dieser Vorlage benutzt werden.

2) In einem Gitter dürfen zwei horizontale bzw. zwei vertikale Arbeitsfelder erst mit einem Abstand von mindestens 3 Zeilen bzw. 3 Spalten vollständig untereinander bzw. nebeneinander stehen.

- 3) Bei den Gittern für drei aufeinanderfolgende Schlüsselserien dürfen sich bei jeder möglichen Lage von je 2 Gittern nicht mehr als jeweils 3 Arbeitsfelder einer Richtung vollständig überdecken.
Das ist durch Aufeinanderlegen der entsprechenden Gittervorlagen zu überprüfen.
Die im Gittervorlagenentwurf eingetragenen 10 horizontalen und 10 vertikalen Arbeitsfelder und nur sie werden in einen zweiten Vordruck überragen, der als Gittervorlage an Ref. 5 weitergegeben wird.
Die 24 Buchstaben des reduzierten deutschen Normalalphabetes ohne J und Y werden in einen Karton gelegt, gemischt, willkürlich nacheinander herausgezogen und in der gezogenen Reihenfolge zur Bezeichnung der Anlegepunkte - je 3 Buchstaben pro Anlegepunkt- benutzt. Die Buchstaben werden in der Gittervorlage jeweils links von Anlegepunkt eingetragen.
Auf die Gittervorlage wird die Nummer der Serie eingetragen, für die das Gitter zu verwenden ist.

4 Beispiel einer Gittervorlage



5 Organisatorisches zur Herstellung der Schlüsselunterlagen
 51 Referat 2 ist verantwortlich für

- a) die rechtzeitige, schriftliche Auftragserstellung bei Referat 1 zur Herstellung von Gittervorlagen und zur Bestellung von Schlüsselserien zum Verfahren "Format"

Der Auftrag muß enthalten:

1. Nummer der herzustellenden Schlüsselserien,
2. Auflage jeder Schlüsselserie,
3. Termin der Fertigstellung jeder Schlüsselserie.

- b) die Aufbewahrung und Auslieferung der verpackten Schlüsselserien an die Benutzer.

52 Referat 1 ist verantwortlich für

- a) die Herstellung der Gittervorlagen.
Jede Gittervorlage ist in zwei Exemplaren herzustellen. Das erste Exemplar erhält Referat 5, das zweite bleibt in Referat 1.
Jede Gittervorlage ist durch den Hersteller und einen weiteren Mitarbeiter genau auf ihre Richtigkeit zu überprüfen. Die Überprüfung wird durch Signum auf dem zweiten Exemplar der Gittervorlage bestätigt.
- b) die schriftliche Auftragserstellung zur Herstellung der Schlüsselserien zum Verfahren "Format" im Druck bei Referat 5 und die Übergabe der Gittervorlagen an Referat 5.
- c) die Überprüfung der Chiffretafel jeder Schlüsselserie in Bezug auf die Irregularität der Ziffernanordnung in der Arbeitsgruppe 3/Arbeitsgebiet 1. Die Überprüfung ist durch Signum auf dem von Referat 5 vorgelegten Abzug zu bestätigen.
- d) die rechtzeitige Auftragserstellung zur Herstellung von Vordrucken für die Gittervorlagen in ausreichender Menge bei Referat 5.

53 Referat 5 ist verantwortlich für

- a) den termingerechten Druck der Schlüsselserien entsprechend der Herstellungsanweisung und den Gittervorlagen von Referat 1.
ein Abzug der Chiffretafel jeder Schlüsselserie ist Referat 1 (Arbeitsgruppe 3/Arbeitsgebiet 1) zur Überprüfung der Irregularität der Ziffernanordnung (vor der Verpackung der Schlüsselserie) vorzulegen.
Die Seriennummer eines Gitters muß mit der auf der entsprechenden Vorlage angegebenen Nummer übereinstimmen.
- b) das Korrekturlesen der gedruckten Schlüssel-

serien.

- c) die Verpackung der überprüften Schlüsselserien und ihre Übergabe an Referat 2.
Jedes Schlüsselunterlagenexemplar einer Schlüsselserie ist die Auslieferung an Referat 2 in einer versiegelten Tüte verpackt. Die Tüte trägt auf der Vorderseite die Aufschrift

FORMAT

Ex.-Nr. Serie (Nummer)

- 6 Schlüsselbereiche
Das Verfahren "Format" wird beim Kommando Deutsche Grenzpolizei/Grenze See in vier Schlüsselbereichen in allgemeinem Verkehr benutzt.
1. Schlüsselbereich: Brigadestab Rostock, 3 Bereitschaften, 3 Stützpunkte (7 Chiffrierstellen)
 2. Schlüsselbereich: Bootsstützpunkt Wismar, Boote (11 Chiffrierstellen)
 3. Schlüsselbereich: Bootsstützpunkt Saßnitz, Boote (9 Chiffrierstellen)
 4. Schlüsselbereich: Bootsstützpunkte Wieck, Boote (13 Chiffrierstellen)
- 7 Schlüsselwechsel und Schlüsselunterlagenwechsel
- 71 Beim Verfahren "Format" wird ein Spruchschlüssel angewendet.
- 72 Der Wechsel der Schlüsselunterlagen zum Verfahren "Format" erfolgt nach Bearbeitung von 400 Codegruppen spätestens jedoch nach einem Monat innerhalb eines Schlüsselbereichs auf Anordnung der Zentrale des jeweiligen Schlüsselbereichs.
- 73 Bei Kompromittierung oder beim Verdacht der Kompromittierung ist sofort Schlüsselwechsel durchzuführen.
- 8 Bevorratung und Anforderung von Schlüsselunterlagen und Verbleib ungültig gewordener Schlüsselunterlagen
- 81 Bevorratung

Außer der in Gebrauch befindlichen Schlüsselserien müssen für die Schlüsselbereiche die folgenden Anzahl von Reserveschlüsselserien vorhanden sein:

1. Schlüsselbereich: 6
2. - 4. Schlüsselbereich je 3

Je eine Reserve-Schlüsselserie befindet sich in der jeweiligen Zentrale des 2. - 4. Schlüsselbereichs, alle übrigen Reserve-Schlüsselserien lagern beim Brigadestab Rostock.

Bei der Abteilung XI lagern 3 Reserve-Schlüsselserien.

82 Anforderung
Die Anforderung von Schlüsselserien erfolgt quartalsweise von der Abteilung Nachrichten II des MdI.

83 Verbleib
48 Stunden nach Außerkraftsetzung einer Schlüsselserien erfolgt die Vernichtung der Schlüsselunterlagen dieser Serie durch die Zentrale des jeweiligen Schlüsselbereiches.

11.8. Codierverfahren FL-1 ^{BStU *225}

Az.: 00 15 40 Vertrauliche Verschlusssache !
 VVS-Nr.: D 272 925
 10. Ausfertigung = 05 Blatt

NATIONALE VOLKSARMEE
KOMMANDO DER VOLKSMARINE

Anordnung Nr. 17/85
des Stellvertreters des Chefs und Chef des Stabes
über
die Einführung des "Codierverfahrens FL-1"
vom 09.12.1985

Zur Einführung des "Codierverfahrens FL-1"

ORDNE ICH AN:

1. Zum Schutz der Zivilflotten der DDR im Verteidigungs-
zustand wird, auf der Grundlage der Ordnung Nr. 200/9/609
des Stellvertreters des Ministers und Chef der Volks-
marine, für die gedeckte Übermittlung von Informationen
des Zusammenwirkens zwischen Schiffen und Booten der
Volksmarine und der 6. Grenzbrigade Küste mit Schiffen
des Kombinats Seeverkehr und Hafengewirtschaft und Schiffe
des VEB Fischkombinat Rostock, das manuelle "Codierver-
fahren FL-1" eingeführt.
2. Die Einführung des "Codierverfahrens FL-1", bestehend
aus dem Kurzcode FL-1 und Überschlüsselungsmitteln Typ
542, erfolgt entsprechend Anlage 1.
3. Durch den Stellvertreter des Chefs des Stabes für opera-
tive Arbeit sind die operativen Einsatzprinzipien für
die Nutzung des Codierverfahrens festzulegen.
4. Für die Planung und Verteilung der erforderlichen Codier-
mittel sowie für die Ausbildung der Nutzer ist der Chef
Nachrichten verantwortlich.
5. Vorschläge für die weitere Vervollkommnung der genutzten
Codiermittel sind an den Chef Nachrichten im MfNV weiter-
zuleiten.

Vertrauliche Verschlusssache !

VVS-Nr.: D 272 925 10. Ausf., Bl. 2

6. Festlegungen zur Gültigkeit und zum Wechsel der Unterlagen
sind im "Plan der Gültigkeit der Codiermittel" zu treffen.
7. Nutzung des "Codierverfahrens FL-1":
 - (1) Zur Arbeit mit dem Kurzcode FL-1 sind berechtigt:
 - Offiziere der Stäbe der Volksmarine sowie Mitarbeiter
der Abt. I der Kombinate im Interesse der operativen
Führung.
 - Alle Informationen, die mit dem "Codierverfahren

(1) Verteiler für die Kurzcodes Fl-1 und Überschlüsselungs-
mittel Typ 542:

- 1. Flottille Ex. 001 bis 008
- 4. Flottille Ex. 009 bis 017
- 6. GBrK Ex. 018 bis 029
- NBB/NR-18 Ex. 030
- KSH Ex. 031 bis 041
- VEB Fischkombinat ex. 042 bis 047

(2) Kenngruppenzuweisung:

- Die Kenngruppenzuweisung ist auf den Überschlüsselungs-
komplekten Typ 542 (Deckblatt außen) einzutragen.
Durch die Nutzer sind nur diese zugewiesenen Kenngrup-
pen zum Überschlüsseln von Ausgangsinformationen zu
verwenden.

2. Einweisung der Oberoffiziere SNV der Verbände, Leiter Chif-
frierstelle NBB/NR-18, Leiter IB-Stellen der Kombinate.

- Verantwortlich: Chef Nachrichten
- Termin: 15.12.1985

3. Vorbereitung von Übungssprüchen zur Übergabe an die Komman-
danten bzw. Kapitäne der Schiffe, die für die Teilnahme an
der Erprobung vorgesehen sind.

- Verantwortlich: Stellvertreter des Chef des Stabes für
operative Arbeit / Leiter der Abt. I der
Kombinate
- Termin: 15.12.1985

(1) 10 vorbereitete Übungssprüche pro Schiff, Länge 5 bis
12 Codegruppen als Zwischentext übergeben.

(2) Achtung - es dürfen keine gleichlautenden Texte ange-
fertigt werden !

(3) Die Übungssprüche sind mit "Zur Übung" einzuleiten.

4. Austausch der Listen der teilnehmenden Schiffe (Schiffs-
name und Rufzeichen).

- Verantwortlich: Stellvertreter des Chef des Stabes für
operative Arbeit / Leiter der Abt. I der
Kombinate
- Termin: 15.12.1985

Vertrauliche Verschlusssache !

VVS-Nr.: D 272 925 10. Ausf., Bl 4

5. Einweisung und aktenkundige Belehrung der Kommandanten bzw. Kapitäne zur ordnungsgemäßen Nutzung der Codiermittel, zum Ziel des Informationsaustausches einschließlich politischer Bedeutung, Auswertung und zu den Besonderheiten der eingesetzten Codiermittel.

- Verantwortlich: Stabschef der Verbände / Leiter der Abt. I
der Kombinate

- Termin: 15.12.1985

(1) Durch die Kommandanten bzw. Kapitäne ist folgende Statistik zu führen und dem Erprobungsbericht beizufügen:

- Datum / Uhrzeit / Spruch-Nr. / Absender / Empfänger /
Gruppenanzahl / Fehler, davon nach Entstümmeln klar /
Bearbeitungszeit (ver- bzw. entschlüsseln).

6. Seewurferprobung

(1) Die Unterlagen für das "Codierverfahren FL-1" wurden für die eventuelle Vernichtung durch Seewurf entwickelt. Das soll erreicht werden

a) durch die Verwendung von wasserlöslichem Hydrasol-
Spezialpapier;

b) durch eingearbeitete Metallbeschwerung.

(2) Zur genauen Beurteilung der Verhaltensweise der zu vernichtenden Unterlagen durch Seewurf ist eine spezielle Seewurferprobung im Bereich der 4. Flottille durchzuführen (Dauer ca. 6 Stunden).

(3) Durch tauchermäßige Sicherstellung ist zu überprüfen bzw. zu gewährleisten:

a) das Sinkverhalten der Dokumente;

b) der Grad der Vernichtung durch Auflösung (Zeitabschnitte angeben);

c) die Bergung der eingesetzten Unterlagen.

Diese spezielle Erprobung wird unter Führung des Leiters der UA. Chiffrierdienst durchgeführt. Die Einweisung der Teilnehmer erfolgt vor Ort.

(4) Durch den Stabschef der 4. Flottille ist sicherzustellen

- 1 Schiff zur Aufnahme der Erprobungsgruppe, der Einsatzort wird präzisiert;

- 2-3 Taucher zur Beobachtung und Bergung der Unterlagen.

Für den Zeitraum 01.04.86 bis 15.04.86 ist ein entsprechender Terminvorschlag zu unterbreiten.

7. Nach Abschluß der Erprobung sind die Unterlagen von Bord der Schiffe der Volksmarine abzuziehen und beim Oberoffizier SNV der Verbände zu lagern.

Vertrauliche Verschlusssache !

VVS-Nr.: D 272 925 10. Ausf., Bl 5

Diese Festlegung ist auch für Schiffe der Kombinate zutreffend wenn feststeht, daß sie nicht an der Übung im Monat September teilnehmen. Die Lagerung der Unterlagen erfolgt beim Leiter der IB-Stelle.

8. Auswertung der Erprobung; Vorlage der Ergebnisse; Vorschläge für Änderungen zum Phrasenbestand, Aufbau der Codiermittel u.dgl.
- Verantwortlich: Stellvertreter des Chef Stabes für operative Arbeit
 - Termin: Beratung am 21.05.1986 im Kommando VM

2. Etappe - Erprobung während der Übung im Monat September 1986

1. Verteilung der Codiermittel an die Teilnehmer der Übung (siehe 1. Etappe, Punkt 7.).
Der Verteiler für die 1. Etappe (siehe Punkt 1.(1)) kann bei Notwendigkeit verändert werden.
- Verantwortlich: Stellvertreter des Chef des Stabes für operative Arbeit / Chef Nachrichten
 - Termin: 15.08.1986
2. Einweisung und aktenkundige Belehrung der Kommandanten und Kapitäne wie Punkt 5. der 1. Etappe.
- Verantwortlich: Stabschef der Verbände / Leiter der Abt. I der Kombinate
 - Termin: 15.08.1986
3. Austausch der Listen der teilnehmenden Schiffe (Schiffsnamen und Rufzeichen).
- Verantwortlich: Stellvertreter des Chef des Stabes für operative Arbeit / Leiter der Abt. I der Kombinate
 - Termin: 15.08.1986
4. Auswertung der Erprobung; Vorlage der Ergebnisse; Vorschläge

für Änderungen zum Phrasenbestand, Aufbau der Codiermittel
u.dgl.

- Verantwortlich: Stellvertreter des Chef des Stabes für
operative Arbeit
- Termin: wird präzisiert

3. Etappe - operative Nutzung

1. Der ständige operative Einsatz des "Codierverfahrens FL-1"
ist ab 01.01.1987 vorgesehen.

- (1) Durch den Stellvertreter des Chef des Stabes für opera-
tive Arbeit sowie den Chef Nachrichten sind für alle
Voraussetzungen zu schaffen.
- (2) Die 6. Flottille wird in den Kreis der Nutzer mit ein-
bezogen.

12.1. Vorschrift zum Verfahren 001 ^{BStU [*194](#)}

Chi 5001
30.11.65

Geheime Verschlusssache!
GVS-1674/65
3 Blatt/Ex.: 1043*
Bl. 01

Gebrauchsanweisung

zum Verfahren 001

1. Zweckbestimmung

Das Verfahren 001 dient zur Chiffrierung von Ziffernzwischen-
text. Es gewährleistet bei ordnungsgemäßer Anwendung absolute
Sicherheit für die chiffrierte Nachricht.

Mit dem Verfahren können individuelle und zirkulare Verkehre
aufrechterhalten werden.

2. Schlüsselunterlagen

Die Schlüsselunterlagen sind im Wurmtabellenheft zusammen-
gefaßt. Es werden unterschieden

- Wurmtabellenhefte für individuelle Verkehre mit der Kenn-
zeichnung "I" (Auflage 2),
- Wurmtabellenhefte für zirkulare Verkehre mit der Kennzeich-
nung "Z" (Auflage 3 und höher).

Wenn nicht anders angewiesen, dient Exemplar 1 zum Chiffrieren, die übrigen Exemplare zum Dechiffrieren. Die Wurmtabellenhefte enthalten die Kenngruppentafel und die Wurmtabellen. Die Kenngruppentafel enthält soviel Fünfergruppen wie das Wurmtabellenheft Wurmtabellen enthält. Die Wurmtabellen sind der Reihenfolge nach nummeriert.

3. Chiffrierung

3.1. Chiffrierung des Zwischentextes

Zur Chiffrierung des Zwischentextes wird als Additionsreihe die nächstfolgende noch nicht benutzte Wurmtabelle verwendet. Die Bearbeitung erfolgt gemäß "[Vorschrift für Ziffernadditionsverfahren](#)". Reicht die Anzahl der Fünfergruppen der Wurmtabelle nicht aus, so werden die nachfolgenden Wurmtabellen in gleicher Weise verwendet. Sind die Wurmtabellen eines Wurmtabellenheftes verbraucht, so wird das nächstfolgende für diesen Verkehr vorgesehene Wurmtabellenheft benutzt.

Bleiben Teile einer Wurmtabelle bei der Chiffrierung eines Zwischentextes ungenutzt, so dürfen sie zur Chiffrierung eines weiteren Zwischentextes nicht mehr verwendet werden. Die Wurmtabelle ist nach einmaliger Benutzung zur Chiffrierung ungültig geworden.

3.2. Einsetzung der Kenngruppe

Jeder Wurmtabelle des Wurmtabellenheftes ist entsprechend ihrer Nummer eine fünfstellige Zifferngruppe als Kenngruppe zugeordnet. Die Kenngruppen für die Wurmtabellen werden spaltenweise von oben nach unten, in der Reihenfolge der Spalten von links nach rechts, aus der Kenngruppentafel entnommen.

Die Kenngruppe, die der zur Chiffrierung verwendeten Wurmtabelle zugeordnet ist, wird als erste und letzte Gruppe dem Chiffretext angefügt.

Werden zur Chiffrierung eines Zwischentextes mehrere Wurm-
tabellen benutzt, so wird nur die Kenngruppe der ersten ver-
wendeten Wurmtabelle als erste und letzte Gruppe dem Chif-
fretext angefügt. Die Kenngruppen der anderen Wurmtabellen
bleiben unberücksichtigt.

Alle Kenngruppen, deren Wurmtabellen zur
Chiffrierung verwendet wurden, sind in der
Kenngruppentafel zu streichen.

2

Chi 5001

GVS-1674/65
Bl.02

4. Dechiffrierung

Anhand der Stellung der Kenngruppe in der Kenngruppentafel
wird die Wurmtabelle bestimmt, aus der die zu benutzende Addi-
tionsreihe zu entnehmen ist. Reicht die Wurmtabelle zur Dechif-
frierung nicht aus, so sind die nächstfolgenden Wurmtabellen in
gleicher Weise zu benutzen.

Alle Kenngruppen, deren Wurmtabellen zur Dechiffrierung ver-
wendet wurden, sind in der Kenngruppentafel zu streichen.

Die Dechiffrierung erfolgt gemäß der "[Vorschrift für Ziffern-
additionsverfahren](#)".

5. Registratur und Vernichtung

- 5.1. Bei zirkularen Verkehren sind nichtbenutzte Wurmtabellen
bzw. Hefte durch die Empfänger selbständig zu vernichten,
wenn sie Sprüche erhalten, die mit nachfolgenden Wurmtabel-
len bzw. Heften bearbeitet wurden.
- 5.2. Werden in Wurmtabellenheften des Empfängers versehentlich
Wurmtabellen gelöst, so sind dem Absender die Kenngruppe
bzw. Kenngruppen der zu vernichtenden Wurmtabellen wie folgt
offen mitzuteilen:
"23573 vernichten" bzw. "23573 bis 09471 vernichten".
- 5.3. Wenn nicht anders angewiesen, sind benutzte oder gelöste
unbenutzte Wurmtabellen spätestens nach 48 Stunden zu ver-
nichten. Vernichtete Wurmtabellen sind zu registrieren.

4

Chi 5001

GVS-1674/65
Bl.03**6. Beispiele**

Beispiel 1: (Vergleiche "Vorschrift für Ziffernadditionsverfahren"
Beispiele 16,17)

Kenngruppentafel: ~~03208~~ ~~32663~~ 77469 58466
~~54344~~ 81011 74825 57864
~~06036~~ 12864 95965 24940
~~49616~~ 43109 11436 10240
~~70942~~ 40270 00376 68471

Wurmtabelle 07: 61449 56442 81770 12327 17828
19804 66262 63452 86367 29083
25477 24262 35715 34194 66775 07
83271 37012 81576 38721 39666
10838 29462 109..
.....

Beispiel 2: (Vergleiche "Vorschrift für Ziffernadditionsverfahren"
Beispiele 18,19)

Kenngruppentafel: ~~08718~~ ~~10064~~ 33204 81351
~~32023~~ ~~36702~~ 86037 70367
~~31676~~ ~~73818~~ 96111 75685
~~88304~~ ~~15838~~ 03031 46629
~~67747~~ ~~98329~~ 65455 51746

Wurmtabelle 11: 75607 28694 48333 62978 13695
21319 68988 34515 97492 52365
20250 75921 73905 79110 22384 11
92420 70875 69640 65856 41026
48098 77874 246..
.....

12.2. Vorschrift für Ziffernadditionsverfahren 1965 BStU *194

Chi 4101
30.11.65

Geheime Verschlusssache!
GVS-1675/65
8 Blatt/Ex.: 1501*
Bl. 01

VORSCHRIFT**FÜR ZIFFERNADDITIVVERFAHREN**

**Wird 1975 durch eine neue
Vorschrift abgelöst.**

1. Zweckbestimmung

Diese Vorschrift enthält die allgemeingültigen Bestimmungen für die Anwendung von Ziffernadditionsverfahren. Weitere spezielle Festlegungen zu einzelnen Verfahren sind in den Gebrauchsanweisungen zu diesen Verfahren enthalten.

2. Herrichtung des Klartextes

- 2.1. Der Klartext ist so kurz wie möglich. abzufassen und den Klareinheiten der zugewiesenen Substitutionstafel bzw. des zugewiesenen Codes optimal anzupassen, Entbehrliche Textteile (Wörter, Satzzeichen usw.) werden weggelassen (Beispiel 1), falls nicht eine buchstabengetreue Wiedergabe des Klartextes gefordert wird.
- 2.2. Wenn im Einzelfall nichts anderes festgelegt ist, werden Zahlen, die nicht als Klareinheiten in der Substitutionstafel oder im Code enthalten sind, in das Zahlensignal (zs) der Substitutionstafel eingeschlossen und wie folgt behandelt:
 - a. Bei arabischen Zahlen wird jede Ziffer dreimal gesetzt. Einzelstehende Buchstaben oder Satzzeichen, die unmittelbar zur Zahl gehören, werden innerhalb des Zahlensignals geschrieben. Buchstaben sind durch Trennzeichen von der Zahl zu trennen (Beispiele 1 bis 7, 10, 11).
 - b. Dezimalbrüche werden wie arabische Zahlen behandelt.

Gemeine Brüche sind in Dezimalbrüche umzuwandeln oder als Wortfolgen auszuschreiben (Beispiel 3).

Chi 4101

GVS-1675/65

- c. Römische Zahlen werden wie arabische Zahlen hergerichtet und innerhalb des Zahlensignals in "r" eingeschlossen (Beispiel 4).
 - d. Uhrzeiten ohne Minutenangaben werden zweistellig, mit Minutenangaben vierstellig geschrieben, wie arabische Zahlen hergerichtet und ohne Satzzeichen geschrieben (Beispiel 5).
 - e. Bei Buchstaben-Ziffernausdrücken (Waren- und Typenbezeichnungen, Autonummern, chemische Formeln u. ä.) werden die Zahlen wie arabische Zahlen behandelt und die Buchstaben der Reihenfolge nach bei Notwendigkeit wiederholt (Beispiele 6, 11).
 - f. Tabellarische Aufstellungen werden zeilenweise bearbeitet. Zwischen den Spaltenbezeichnungen bzw. Spaltenwerten werden Trennzeichen, am Ende jeder Zeile wird ein Punkt gesetzt (Beispiel 7).
 - g. Bei einfachen Aufzählungen werden arabische Zahlen durch Buchstaben mit Punkt und Buchstaben durch Buchstaben mit Klammer ersetzt (Beispiel 8).
- 2.3. Sonstige Zeichen, die nicht als Klareinheiten in der Substitutionstafel oder im Code enthalten sind, werden als Wörter voll ausgeschrieben (Beispiel 9).
- 2.4. Trennzeichen (#) werden gesetzt, falls nicht bereits andere Zeichen eine Trennung anzeigen,
- a. zwischen aufeinanderfolgenden Wörtern, Zahlen usw., die als ein Ausdruck gelesen zu Sinnentstellungen führen können (Beispiele 1, 4, 7, 10, 11);
 - b. in tabellarischen Aufstellungen (siehe Abschnitt 2.2. f.);
 - c. vor und nach allgemein gebräuchlichen Abkürzungen (Beispiele 4, 6, 7);
 - d. bei Empfängern und Absender, um diese Teile vom eigentlichen Text zu trennen (siehe Abschnitt 6.);
 - e. bei Fortsetzungen (siehe Abschnitt 7.).

2.5. Das Wiederholungssignal (ws) wird vor und nach der Wiederholung wichtiger Wörter oder anderer wichtiger Textteile gesetzt, deren Verstümmelung zur Sinnentstellung führen kann (Beispiel 11).

2.6. Orts- und Familiennamen können bei wiederholtem Auftreten im gleichen Klartext durch den Anfangsbuchstaben mit Punkt ersetzt werden, falls Verwechslungen ausgeschlossen sind (Beispiel 12). Alle anderen selbstgewählten Abkürzungen die für längere, im gleichen Klartext wiederholt auftretende Ausdrücke eingesetzt werden können, sind in Klammern einzuschließen.

Das erste Mal wird der Ausdruck voll ausgeschrieben und die in Klammern eingeschlossene Abkürzung nachgestellt. Bei Wiederholung des Ausdrucks wird nur die in Klammern eingeschlossene Abkürzung geschrieben.

Die Abkürzung soll aus zwei Buchstaben bestehen. Werden in einem Klartext verschiedene Abkürzungen verwendet, so werden sie so gewählt, daß sie sich in beiden Buchstaben unterscheiden (Beispiel 13).

3. Bildung des Zwischentextes

3.1. Bei der Bildung des Zwischentextes wird der hergerichtete Klartext mit Hilfe einer Substitutionstafel oder eines Zifferncodes oder beider Mittel gemeinsam vollständig in Zifferntext umgewandelt (Beispiel 14). Dabei werden die nach Abschnitt 2.2. gebildeten Zifferngruppen unverändert übernommen, sonstige Klareinheiten (einschließlich Indikatoren) in der Reihenfolge ihres Auftretens durch die Ziffern oder Zifferngruppen (Zwischeneinheiten) ersetzt, die ihnen in der Substitutionstafel oder im Code zugeordnet sind.

3.2. Bei gemeinsamer Anwendung einer Substitutionstafel und eines

Codes sind die Zwischeneinheiten aus den beiden Mitteln so zu wählen, daß der kürzeste Zwischentext entsteht. Der Übergang von einem Mittel zum anderen ist durch Indikatoren anzuzeigen, wenn die verschiedenen Arten von Zwischeneinheiten sich nicht eindeutig voneinander unterscheiden.

Das gleiche gilt für die gemeinsame Anwendung mehrerer Substitutionstafeln oder Codes.

- 3.3. Besteht der hergerichtete Klartext ausschließlich aus Ziffern, so kann dieser ohne weitere Umwandlung als Zwischentext verwendet werden.
- 3.4. Der nur noch aus Ziffern bestehende Zwischentext wird in der Regel in Fünfergruppen eingeteilt. Ist die letzte Gruppe nicht vollständig, wird sie durch beliebige Ziffern, die den Sinn des Textes nicht entststellen, zu einer vollen Gruppe aufgefüllt (Beispiel 15).

4

Chi 4101

GVS-1675/65

Bl. 03

4. Chiffrierung

Die Chiffrierung des Zwischentextes erfolgt mit dem zugewiesenen Chiffreverfahren in der Weise, daß Additionsreihe und Zwischentext ziffernweise mod 10 (d. h. ohne Berücksichtigung der Zehner) addiert werden. Das Ergebnis der Addition ist der Chiffretext (Beispiel 16).

Besteht der Zwischentext aus vierstelligen Zifferngruppen, die Additionsreihe aus fünfstelligen Zifferngruppen, so wird die fünfte Ziffer jeder Wurmgruppe nicht zur Chiffrierung verwendet.

Die zur Chiffrierung benutzte Additionsreihe wird dem Empfänger durch die Kenngruppe mitgeteilt. Die Kenngruppe wird entsprechend der Vorschrift des zugewiesenen Chiffreverfahrens gebildet und dem Chiffretext als erste und letzte Gruppe angefügt (Beispiel 17).

5. Dechiffrierung

Anhand der Kenngruppe wird vom Empfänger, entsprechend den Bestimmungen des zugewiesenen Chiffreverfahrens, die für die Dechiffrierung zu benutzende Additionsreihe bestimmt (Beispiel 18). Die Dechiffrierung des Chiffretextes erfolgt mit dem zugewiesenen Chiffreverfahren in der Weise, daß die Additionsreihe vom Chiffretext ziffernweise mod 10 (d. h. ohne Berücksichtigung der Zehner) subtrahiert wird. Das Ergebnis der Subtraktion ist der Zwischentext, der mittels Substitutionstafel oder Code oder beider Mittel gemeinsam in Klartext umgewandelt wird (Beispiel 19).

Aus dem Textzusammenhang erkennbare Verstümmelungen werden berichtigt. Bei Berichtigung verstümmelter Codegruppen ist entsprechend den Bestimmungen der Gebrauchsanweisung des zugewiesenen Codes zu verfahren.

6. Empfänger und Absender

Wenn in der Gebrauchsanweisung des zugewiesenen Chiffreverfahrens nicht anders angewiesen, können der Empfänger am Anfang und der Absender am Ende des Textes stehen.

Im Verkehr der Chiffrierstellen untereinander können Empfänger und Absender weggelassen werden. Dasselbe trifft zu bei ständig wiederkehrenden Meldungen, Berichten usw., aus denen klar hervorgeht wer Empfänger und Absender sind.

7. Fortsetzungen

Werden Klartexte aus praktischen Erwägungen oder auf Grund der Gebrauchsanweisung für das zugewiesene Chiffreverfahren geteilt, so wird jeder Teil als selbständiger Klartext bearbeitet.

Zur Kennzeichnung als ersten Teil enthält dieser am Ende den Buchstaben a mit nachfolgendem Fortsetzungsvermerk ff, der anzeigt, daß ein weiterer Teil folgt.

Jeder weitere Teil enthält zur Kennzeichnung als Fortsetzung in der Reihenfolge des Alphabets am Anfang des Textes einen der

Buchstaben b, c, d ... und außer dem letzten Teil am Ende des Textes den Fortsetzungsvermerk.

Der erste Teil enthält den Empfänger, der letzte Teil den Absender. Fortsetzungskennzeichnungen werden durch Trennzeichen vom Text getrennt und mit chiffriert (Beispiel 20).

Sollen weitere geteilte Sprüche gleichzeitig an die gleiche Stelle übermittelt werden, so erhalten diese zur Unterscheidung andere aufeinanderfolgende Buchstaben in der Weise zugewiesen, daß jeder Buchstabe nur einmal als Fortsetzungskennzeichnung auftritt (Beispiel 21).

6

Chi 4101

GVS-1675/65

Bl. 04

8. Rückfragen

Eine Rückfrage hat zu erfolgen, wenn in einem empfangenen Spruch Verstümmelungen enthalten sind, die nicht aus dem Zusammenhang oder mit Hilfe der Bestimmungen der Gebrauchsanweisung des zugewiesenen Codes berichtigt werden können.

Die Rückfrage wird durch Angabe der Kenngruppe des Spruches und der Stellenzahlen der verstümmelten Fünfergruppen im Chiffretext durchgeführt (Beispiel 22).

Eine andere Methode der Rückfrage ist nicht gestattet.

Verstümmelungen können auf zwei Arten berichtigt werden:

- a. Verwendung der gleichen Einsatzgruppe und bei unverändertem Klartext einfache Berichtigung der Verstümmelung;
- b. Verwendung einer neuen Einsatzgruppe zur Chiffrierung desselben Textteiles. Bei nicht absolut sicheren Verfahren ist eine Umordnung und Umstilisierung des Textteiles vorzunehmen.

Übermittlungsfehler und einzelne Chiffrierfehler, die bei der Berichtigung des Fehlers keine Verschiebung des Zwischentextes in Bezug auf die Additionsreihe ergeben, können nach a. und nach b. berichtigt werden. Andere Chiffrierfehler werden grundsätzlich nach b. berichtigt.

9. Bearbeitung von Weiterleitungen

Weiterleitungen sind grundsätzlich nur gestattet, wenn keine direkte Chiffrierverbindung von einer Dienststelle zu einer anderen besteht bzw. die Chiffrierverbindung zeitweilig unterbrochen ist.

Der Spruch wird dann über die nächstvorgesezte Dienststelle oder über eine andere Chiffrierstelle geleitet. Von der absenden- den Dienststelle werden der gesamte letztendliche Empfänger und der Absender chiffriert. Die weiterleitende Dienststelle dechiffriert den Spruch und bearbeitet den Ausgang (Weiterleitung) mit einer neuen Einsatzgruppe. Es werden der Empfänger und der gesamte ursprüngliche Absender chiffriert.

10. Bearbeitung von Sprüchen mit zirkularem und individuellem Text

Bei zirkularen Sprüchen, in die mehrere individuelle Textteile eingefügt sind, ist der gesamte zirkulare Text zusammenzuziehen und als ein zirkularer Spruch zu bearbeiten.

Ebenso wird der gesamte individuelle Text zusammengezogen und als ein individueller Spruch bearbeitet.

Damit der individuelle Text eindeutig in den zirkularen Text eingefügt werden kann, sind an den entsprechenden Stellen des zirkularen und individuellen Textes, wo getrennt wird, Kennzeichen zu setzen.

Die Kennzeichen ia, ib, ic ... werden in Klammern eingeschlossen und mit chiffriert (Beispiel 23).

11. Wechsel der Schlüsselunterlagen

Die Leitstelle des Schlüsselbereiches (verantwortliche Chiffrierstelle) ordnet den Wechsel der Schlüsselunterlagen an.

Die Chiffrierstellen haben von der Leitstelle so rechtzeitig neue Schlüsselunterlagen anzufordern, daß ein kontinuierlicher Chiffrier-

verkehr gewährleistet ist.

8

Chi 4101

GVS-1675/65
Bl. 05

12. Beispiele

Für die Bildung des Zwischentextes in den Beispielen wurde die Substitutionstafel [ZEBRA-1](#) verwendet. Die in den Beispielen verwendeten Additionsreihen und Kenngruppen sind den Schulungsunterlagen der speziellen Verfahren entnommen.

Beispiel 1:

Klartext: Mit Wirkung vom 14.4. um 17,00 Uhr ist
volle Einsatzbereitschaft zu gewährleisten.

hergerichteter Klartext: ab zs 111 444 . 44 . # 111 777 zs
uhr volle einsatzbereitschaft

Beispiel 2:

Klartext: ... am 13.8. wurden ...

hergerichteter Klartext: ... am zs 111 333 . 888 . zs wurden

Klartext: ... 4c ...

hergerichteter Klartext: ... zs 444 # c zs ...

Klartext: ... im Raum 1648a sind ...

hergerichteter Klartext: ... im raum zs 111 666 444 888 # a zs
sind ...

Klartext: ... 970,- MDN ...

hergerichteter Klartext: ... zs 999 777 000 zs mdn ...

Beispiel 3:

Klartext: ... 1/2 113 ...

hergerichteter Klartext: ... zs 000 , 555 zs ...
... ein drittel ...

Chi 4101

GVS-1675/65

Beispiel 4:

Klartext: ... Abschnitt I11/12 ...
 hergerichteter Klartext: ... abschnitt zs r 333 r / 111 222 zs ...

Klartext: ... DPA-Nr. XI 0028367 ...
 hergerichteter Klartext: ... # dpa # nr. zs r 111 111 r # 000
 000 222 888 333 666 777 zs ...

Beispiel 5:

Klartext: ... um 9,00 Uhr ...
 hergerichteter Klartext: ... um zs 000 999 zs uhr ...

Klartext: ... um 13,05 Uhr ...
 hergerichteter Klartext: ... um zs 111 333 000 555 zs uhr ...

Beispiel 6:

Klartext: ... PKW F9 IA 25-23 ...
 hergerichteter Klartext: ... # pkw # f zs 999 zs ia zs 222 555
 - 222 333 zs ...

Beispiel 7:

Klartext: Einheit T-54 T-34 Fla-SFL Kfz
 PR 8 10 38 18 20
 PR 6 11 39 13 17
 PR 1 12 35 20 18

hergerichteter Klartext: reihenfolge der meldung:
 einheit # t - zs 555 444 zs # t - zs 333 444 zs # fla - sfl # kfz.
 pr zs 888 # 111 000 # 333 888 # 111 888 # 222 000 zs .
 pr zs 666 # 111 111 # 333 999 # 111 333 # 111 777 zs .
 pr zs 111 # 111 222 # 333 555 # 222 000 # 111 888 zs

Beispiel 8:

Klartext:	hergerichteter Klartext:
1.	a.
2.	b.
3.	c.
4.a.	d.a)
4.b.	d.b)
.....
26.	z.
26.a)	z.a)
26.c)	z.c)
26.d)	z.d)
.....

Beispiel 9:

Klartext:	hergerichteter Klartext:
§	paragraph
%	prozent

Beispiel 10:

Klartext:	... in Gersberg werden ...
hergerichteter Klartext:	... in # gersberg # werden ...
Klartext:	... 28 12 43 ...
hergerichteter Klartext:	... zs 222 888 # 111 222 # 444 333 ZS ...

Beispiel 11:

Klartext:	... von Mühltröff nach ...
hergerichteter Klartext:	... von mühltröff ws mühltröff ws na ch ...

Klartext: ... Tien Ken Sin ...
hergerichteter Klartext: ... # tien # ken # sin ws tienkensin ws ...

Klartext: ... 3 KS - IIb ...
hergerichteter Klartext: ... zs 333 zs ks - zs r 222 r zs b ws
ksb ws . . .

Beispiel 12:

Klartext: ... Körner, gebe ... Richter, geb. ...
wurden Körner und Richter ...
hergerichteter KlarEext: ... körner, geb. ... richter, geb. ...
wurden k. und r. ...

B e i s p i e l 13:

Klartext: ... wurden von der Untersuchungskom-
mission dem Generalstaatsanwalt ... der
Generalstaatsanwalt wird der Untersu-
chungskommission ...
hergerichteter Klartext: ... wurden von der untersuchungskomm
ission (uk) dem generalstaatsanwalt (ga)
... der (ga) wird der (uk) ...

12

Chi 4101

GVS-1675/65
Bl.07

Beispiel 14:

hergerichteter Klartext Beispiel 1:

hergerichteter Klartext: a b zs 111 444 . 444 . # 111 777 zs
Zwischentext: 042 89 111 444 80 444 8086 111 777 89

hergerichteter Klartext: u h r v o l l e e i n s a t z
Zwischentext: 71 53 62 74 58 56 56 1 1 2 3 64 0 69 78

hergerichteter Klartext: b e r e i t s c h a f t
Zwischentext: 43 63 2 69 65 0 50 69

Beispiel 15:

Zwischentext (Beispiel 14) in Fünfergruppen:

04289 11144 48044 48086 11177 78971 53627 45856
56112 36406 97843 63269 65050 69805

Beispiel 16:

Additionsreihe: 61449 56442 81770 12327 17828 19804 66262
Zwischentext: 04289 11144 48044 48086 11177 78971 53627
Chiffretext: 65628 67586 29714 50303 28995 87775 19889

Additionsreihe: 63452 86367 29083 25477 24262 35715 34194
Zwischentext: 45856 56112 36406 97843 63269 65050 69805
Chiffretext: 08208 32479 55489 12210 87421 90765 93999

Beispiel 17:

Spruch: 81011 65628 67586 29714 50303 28995 87775 19889
08208 32479 55489 12210 87421 90765 93999 81011

Beispiel 18:

Spruch: 33204 47024 56707 85123 62867 92300 57570 33204

Anhand der Kenngruppe 33204 wird die Additions-
reihe bestimmt, deren erste Gruppen lauten:
75607 28694 48333 629... ..

Chi 4101

GVS-1675/65

Beispiel 19:

Chiffretext: 47024 56707 85123 62867 92300 57570
Additionsreihe: 75607 28694 48333 62978 13695 21319
Zwischentext: 72427 38113 47890 00999 89715 36261
Klartext: Ü b un g:En de 09,00 U h r

Beispiel 20:

Dreiteiliger Klartext:
1. Teil: Empfänger # Text # a ff
2. Teil: b # Text # ff
3. Teil: c # Text f Absender

Beispiel 21:

Zwei weitere Sprüche (siehe Beispiel 20). die etwa zur gleichen Zeit an die gleiche Stelle übermittelt werden:

Vierteiliger Klartext:

1. Teil: Empfänger # Text # g ff
2. Teil: h # Text # ff
3. Teil: i # Text ff
4. Teil: j # Text # Absender

Dreiteiliger Klartext:

1. Teil: Empfänger # Text # l ff
2. Teil: m # Text f ff
3. Teil: n # Text # Absender

Beispiel 22:

Vom Spruch mit der Kenngruppe 21480 sind die 14. - 18. und die 23. - 26. Gruppe fehlerhaft.

Rückfrage: 21480 a) 14 - 18 b) 23 - 26
Antwort: 21480 a) 14 - 18 b) 23 - 26
a) 49364 67211 85398 35472
74624
b) 99113 68527 53740 73802

14

Chi 4101

GVS-1675/65
Bl. 08

Beispiel 23:

Zirkularer Text: (ia) (ib)
..... (ic)
Individueller Text: (ia) (ib) ...
..... (ic)

15

Geheime Verschlusssache!

GVS-ZCO/122/75

Ausfertigung ❁ 00064

Vorschrift
für
Ziffernadditionsverfahren
(manuell)

1976

Zentrales Chiffrierorgan der DDR

Geheime Verschlusssache!

GVS-ZCO/122/75

15 Blatt

Vorschrift
für
Ziffernadditionsverfahren
(manuell)

1976

GVS-ZCO/122/75 - Blatt 2

Die "Vorschrift für Ziffernadditionsverfahren (manuell)",
GVS-ZCO/122/75, wird erlassen und tritt mit Wirkung vom
01. 06. 1976 in Kraft.

löst die Vorschrift
aus dem Jahr 1965 ab.

Berlin, den 01. 06. 1976

Leiter ZCO

Inhaltsverzeichnis

	Seite
1. Zweckbestimmung	<u>7</u>
2. Herrichtung der Klartexte	<u>8</u>
2.1. Substitutionstafel und Code	<u>8</u>
2.2. Spruchaufbau	<u>8</u>
2.3. Festlegung zur Herrichtung der Klartexte	<u>9</u>
2.4. Spruchverkehr	<u>11</u>
2.5. Bereichsinterne Festlegungen zur Herrichtung der Klartexte	<u>12</u>
3. Bildung des Zwischentextes	<u>13</u>
4. Chiffrieren	<u>14</u>
5. Dechiffrieren	<u>15</u>
6. Rückfragen	<u>16</u>
7. Sicherheitsbestimmungen	<u>17</u>
7.1. Allgemeines	<u>17</u>
7.2. Vorkommnisse und Sofortmaßnahmen	<u>18</u>
8. Beispiele	<u>23</u>

1. Zweckbestimmung	
---------------------------	--

Diese Vorschrift enthält allgemeingültige Bestimmungen für die Anwendung von Ziffernadditionsverfahren zur manuellen Bearbeitung von Klartexten.

Weitere spezielle Festlegungen zu einzelnen Verfahren sind in den Gebrauchsanweisungen zu diesen Verfahren enthalten.

2. Herrichtung der Klartexte

2.1. Substitutionstafel und Code

- 2.1.1. Zur Herrichtung der Klartexte und zur Bildung der Zwischentext ist die zugewiesene Substitutionstafel zu verwenden. Durch die Substitutionstafel wird eine eindeutige Zuordnung der Klareinheit zu den Zwischeneinheiten gewährleistet. In der Substitutionstafel vorhandene Freistellungen können bereichsintern in eigener Zuständigkeit belegt werden.
- 2.1.2. Die Anwendung von Codes ist möglich (beachte Abschnitt 2.3.2.). Vor jeder Phrase, die durch eine Codegruppe ersetzt werden soll, ist der Indikator "Code" zu ersetzen ([Beispiel 5](#)). Die Phrasen sind beim Herrichten des Klartextes zu unterstreichen.
- 2.1.3. Bei gemeinsamer Anwendung der Substitutionstafel und des Codes sind die Zwischeneinheiten aus beiden Mitteln so zu wählen, daß ohne Sinnentstellung der kürzeste Zwischentext entsteht ([Beispiel 2](#)).
- 2.1.4. Klareinheiten, die nicht in der Substitutionstafel oder im Code enthalten sind und für die keine Festlegungen gelten werden, sind als Wörter voll auszuschreiben (Beispiel [3](#), [4](#)).

2.2. **Spruchaufbau**

- 2.2.1. Falls nicht anders angewiesen, ist jedes Telegramm (zu chiffrierende Nachricht) wie folgt zu **gliedern** ([Beispiel 1](#)):
- VS-Einstufung (VS-Nr.),
 - geheimzuhaltenden Teile der Anschrift,
 - eigentlicher Text mit Wiederholungen (ggf. mit Fortsetzungsvermerken und Signalen bei zirkularen Telegrammen mit individuellen Textteilen).
 - geheimzuhaltende Teile des Absenders.

8

GVS-ZCO/122/75 - Blatt 5

Im Verkehr der Chiffrierstellen untereinander können Empfänger und Absender weggelassen werden. Dasselbe trifft zu, bei ständig wiederkehrenden Meldungen, Berichten usw., aus denen klar hervorgeht, wer Empfänger und Absender sind.

- 2.2.2. Die vom Absender angegebene **Textanordnung** kann mitchiffriert werden. Kürzungen des Klartextes sind statthaft, wenn Sinnentstellungen ausgeschlossen sind und keine buchstabengetreue Wiedergabe des Klartextes gefordert wird ([Beispiel 1](#)).

2.3. **Festlegungen zur Herrichtung der Klartexte**

- 2.3.1. Es sind folgende Indikatoren zu unterscheiden:

WR/ZI	: Absatz (Ø),
Bu	: Übergang zu Buchstaben (≈),
Zi	: Übergang zu Ziffern und Zeichen (»),
ZwR	: Trennzeichen (≠),
Code	: Folgende Gruppe ist Codegruppe (↑),
rpt	: Wiederholungen (Δ).

- 2.3.2. Es sind die Textarten "Bu" und "Zi" zu unterscheiden. Der Buchstabentext ist durch den Indikator "Bu", der Zifferntext durch den Indikator "Zi" anzukündigen (Beispiele

[1](#), [2](#), [3](#), [4](#), [9](#)). Jeder Spruch beginnt in Buchstabentext (Beispiel [1](#)). Beginnt er in Zifferntext, so ist der Indikator "Zi" voranzustellen.

Interpunktionszeichen, das Wiederholungssignal und das Codiersignal mit Codegruppe können in beliebiger Textart stehen (Beispiele [1](#), [2](#), [8](#)).

2.3.3. **Trennzeichen** ist zu setzen:

- zwischen aufeinanderfolgenden Wörtern, Zahlen usw., die als ein Ausdruck gelesen zu Sinnstellungen führen können ([Beispiel 4](#));

9

- vor und nach allgemein gebräuchlichen Abkürzungen ([Beispiel 4](#));
- zwischen Namensteilen mehrteiliger fremdartiger Namen, deren Teilung nicht auf andere Art gekennzeichnet ist ([Beispiel 4](#));
- bei VS-Einstufung, Empfänger und Absender, um diese Teile vom eigentlichen Text zu trennen (Beispiele [10](#), [11](#));
- bei Wiederholungen (Beispiele [1](#), [9](#));
- bei Fortsetzungen (Beispiele [10](#), [11](#));

sofern nicht bereits andere Indikatoren eine Trennung anzeigen (Beispiele [1](#), [4](#)).

2.3.4. Die **Schriftzeichen ä, ö, ü und ß** sind aufzulösen und als ae, oe, ue und sz zu schreiben (Beispiele [1](#), [2](#), [5](#), [8](#)).

In Eigennamen, bei denen eine eindeutige Rückverwandlung jedes einzelnen Buchstabens gewährleistet sein muß, sind die Umlaute als einfache Laute und ß als s zu schreiben. Diese Eigennamen müssen entsprechend [Abschnitt 2.3.8.](#) wiederholt werden (Beispiel [7](#)).

2.3.5. **Zahlen, Zeichen und Buchstaben-Ziffernfolgen** sind mit den notwendigen Indikatoren unverändert in den hergerichteten Klartext zu übernehmen (Beispiele [1](#), [2](#), [4](#)).

- 2.3.6. **Römische Zahlen** sind durch die entsprechenden lateinischen Schriftzeichen zu ersetzen. In Zweifelsfällen ist "roem" vor die Zahl zu schreiben ([Beispiel 8](#)).
- 2.3.7. **Tabellarische Aufstellungen** sind zeilenweise herzurichten. Die einzelnen Positionen der Aufstellung sind so anzuordnen, daß die Zuordnung eindeutig wird ([Beispiel 9](#)).
- 2.3.8. **Wiederholungen** von Wörtern, Buchstaben- und Ziffernfolgen sind vorzunehmen, wenn bei Verstümmelung einzelner Buchstaben bzw. Ziffern Sinnentstellungen auftreten können.

10

GVS-ZCO/122/75 - Blatt 6

Wiederholungen sind im Text mit dem Indikator "prt" anzukündigen (Beispiele [1](#), [4](#), [9](#)).

- 2.3.9. **Aufgelöste Schriftzeichen**, die der Originalschreibweise in Eigennamen entsprechen, sind in der Wiederholung zu verdoppeln (Beispiel [6](#)).
- 2.3.10. Bei **Uhrzeiten** sind
- volle Stunden als zweistellige Zahlen
 - Stunden mit Minutenangaben als vierstellige Zahlen ohne Satzzeichen zu schreiben ([Beispiel 1](#)).
- 2.4. **Spruchverkehr**
- 2.4.1. **Fortsetzungen** sind zu bilden, wenn Klartexte aus praktischen Erwägungen oder auf Grund der Gebrauchsanweisungen für das zugewiesene Chiffrierverfahren geteilt werden.
- (1) Jeder Teil ist als selbständiger Klartext, d. h. unter Verwendung eines neuen Spruchschlüssels, zu bearbeiten.
 - (2) Der erste Teil muß enthalten: VS-Einstufung, Empfänger, den ersten Teil des Textes, der zur Kennzeichnung am Ende den Fortsetzungsvermerk "a ff" enthält, der angibt, daß ein weiterer Teil folgt.

- (3) Jeder weitere Teil ist in der Reihenfolge des Alphabets am Anfang des Textes mit einem der Buchstaben "b", "c", "d" ... und am Ende des Textes (außer dem letzten Teil) mit dem Fortsetzungsvermerk "ff" zu kennzeichnen.
- (4) Der letzte Teil muß den Absender enthalten.
([Beispiel 10](#))

Werden mehrere Sprüche mit Fortsetzungen gleichzeitig an einen Empfänger übermittelt, so erhalten die weiteren Sprüche zur Unterscheidung einen weiteren Buchstaben in der Reihenfolge des Alphabets zugewiesen ([Beispiel 11](#)).

- 2.4.2. **Zirkulare Telegramme mit individuellen Textteilen** sind wie folgt zu bearbeiten:
 - (1) Die Zirkularen und die individuellen Textteile sind jeweils zusammenzufassen.
 - (2) Anstelle des zirkularen Textes im individuellen Text und das individuellen Textes im zirkularen Text sind nacheinander die gleiche Kennzeichen "ia", "ib", "ic" ... einzusetzen.
 - (3) Die Kennzeichen sind vom eigentlichen Text durch Trennzeichen zu trennen.
 - (4) Die zirkularen und die individuellen Textteile sind jeweils getrennt als ein zirkularer und ein individueller Spruch für jeden Empfänger zu bearbeiten.
([Beispiel 12](#))
- 2.4.3. **Weiterleitungen** sind grundsätzlich nur gestattet, wenn keine direkte Chiffrierverbindung von einer Dienststelle zu einer anderen besteht bzw. die Chiffrierverbindung zeitweilig unterbrochen ist.
Der Spruch ist dann über die nächstvorgesetzte Dienststelle oder über eine andere Chiffrierstelle zu leiten. Von der absendenden Dienststelle sind der gesamte letztendliche Empfänger und der Absender zu chiffrieren. Die weiterleitende Dienststelle dechiffriert den Spruch und bearbeitet den Ausgang (Weiterleitung) mit neuem Spruchschlüssel. Es sind Empfänger und der gesamte ur-

sprüngliche Absender zu chiffrieren. ([Beispiel 13](#))

2.5. Bereichsinterne Festlegungen zur Herrichtung der Klartexte

Bei absolut sicheren Chiffrierverfahren kann durch den Leier des jeweiligen Chiffrierdienstes bereichsintern eine von der vorstehenden Ausführungen abweichende Herrichtung der Klartexte gestattet werden, wenn dies in den Gebrauchsanweisungen dieser Verfahren ausdrücklich zugelassen ist.

12

GVS-ZCO/122/75 - Blatt 7

3. Bildung des Zwischentextes

3.1. Bei der Bildung des Zwischentextes ist der hergerichtete Klartext mit Hilfe der zugewiesenen Substitutionstafel oder des zugewiesenen Zifferncodes oder beider Mittel gemeinsam **vollständig in Zifferntext umzuwandeln.**

Dabei sind die Klareinheiten (einschließlich Indikatoren) in der Reihenfolge ihres Auftretens durch die Ziffern oder Zifferngruppen (Zwischeneinheiten) zu ersetzen, die ihnen in der Substitutionstafel oder im Code zugeordnet sind (Beispiele [2](#), [5](#), [14](#)).

3.2. Der nur noch aus Ziffern bestehende Zwischentext ist in der Regel in **Fünfergruppen einzuteilen.** Ist die letzte Gruppe nicht vollständig, ist sie durch beliebige Ziffern, die den Sinn des Klartextes nicht entstellen, zu einer vollen Gruppe aufzufüllen ([Beispiel 15](#)).

13

4. Chiffrieren

Das Chiffrieren des Zwischentextes hat **mit dem zugewiesenen Chiffreverfahren** in der Weise zu erfolgen, daß

Additionsreihe und Zwischentexte ziffernweise mod 10 (d. h. ohne Berücksichtigung der Zehner) addiert werden. Das Ergebnis der Addition ist der Chiffretext ([Beispiel 16](#)). Die zum Chiffrieren benutzte Additionsreihe wird dem Empfänger durch die Kenngruppe mitgeteilt. Die Kenngruppe ist entsprechend der Vorschrift des zugewiesenen Chiffrierverfahrens zu bilden und dem Chiffretext als erste und letzte Gruppe anzufügen ([Beispiel 17](#)).

14

GVS-ZCO/122/75 - Blatt 8

5. **Dechiffrieren**

Die erste und die letzte Fünfergruppe im Spruch sind die Kenngruppen. Sie sind auf Übereinstimmung zu prüfen. Anhand der Kenngruppe ist vom Empfänger, entsprechend den Bestimmungen des zugewiesenen Chiffrierverfahrens, die für das Dechiffrieren zu benutzende Additionsreihe zu bestimmen.

Das Dechiffrieren des Chiffretextes hat mit dem zugewiesenen Chiffrierverfahren in der Weise zu erfolgen, daß die Additionsreihe vom Chiffretext ziffernweise mod 10 (d. h. ohne Berücksichtigung der Zehner) subtrahiert wird. Das Ergebnis der Subtraktion ist der Zwischentext, der mittels zugewiesener Substitutionstafel oder zugewiesener Code oder beider Mittel gemeinsam in Klartext umzuwandeln ist (Beispiele [1](#), [18](#)).

Entsprechend den Festlegungen im Abschnitt 2, sind die notwendigen Korrekturen im erhaltenen Klartext vorzunehmen (Beispiele [1](#), [18](#)).

Aus dem Textzusammenhang erkennbare Verstümmelungen sind zu berichtigen. Bei Berichtigung verstümmelter Codegruppen ist entsprechend den Hinweisen zu Berichtigung von Codegruppen des zugewiesenen Codes zu verfahren.

6. Rückfragen

Eine Rückfrage kann erfolgen, wenn in einem empfangenen Spruch Verstümmelungen enthalten sind, die nicht aus dem Zusammenhang oder mit Hilfe der Hinweise zur Berichtigung von Codegruppen des zugewiesenen Codes berichtigt werden können. Die Rückfrage ist durch Angabe der Kenngruppe des Spruches und der Stellenzahlen der verstümmelten Fünfergruppen im Chiffretext durchzuführen (Beispiel [19](#)).

Eine andere **Methode der Rückfrage ist nicht gestattet**. Verstümmelungen können auf zwei Arten berichtigt werden:

- a) Verwendung der gleichen Einsatzgruppe und bei unverändertem Klartext einfache Berichtigung der Verstümmelung;
- b) Verwendung einer neuen Einsatzgruppe zum Chiffrieren desselben Textteiles. Bei nicht absolut sicheren Verfahren ist eine Umordnung und Umstilisierung des Textteiles vorzunehmen.

Übermittlungsfehler und einzelne Chiffrierfehler, die bei der Berichtigung des Fehlers keine Verschiebung des Zwischentextes in Bezug auf die Additionsreihe ergeben, können nach a) oder b) berichtigt werden. **Andere Chiffrierfehler sind grundsätzlich nach b) zu berichtigen.**

Ist eine Rückfrage aus technischen Gründen nicht möglich, so muß der Empfänger der Nachricht auf die unklare Textstelle aufmerksam gemacht werden.

16

7. Sicherheitsbestimmungen

7.1. Allgemeines

- (1) Chiffrierunterlagen sind nach den entsprechenden grundsätzlichen Weisungen zu behandeln.
- (2) Bei besonderen Vorkommnissen ist vor Einleitung weiterer Sofortmaßnahmen entsprechend den bestehenden Bestimmungen Meldungen zu erstatten.
- (3) **Mitteilungen über Kompromittierung sind** bei Übertragung über Nachrichtenkanälen unter Verwendung der folgenden für diesen Verkehr vorgesehenen, nichtkompromittierten Schlüsselunterlagen **zu chiffrieren.**

7.2 Vorkommnisse und Sofortmaßnahmen

V o r k o m m n i s s e	S o f o r t m a ß n a h m e
(1) Einsetzen einer falschen Kenngruppe, Chiffrieren der Kenngruppe, Fehlen der Kenngruppe	
a) ohne Übermittlung des Spruches:	Fehler korrigieren.
b) und Übermittlung des Spruches:	Bei Notwendigkeit Mitteilung der richtigen Kenngruppe an empfangende Chiffrierstelle.
(2) Kompromittierung von Klartext oder Zwischentext	
a) vor Übermittlung:	Mitteilung über Kompromittierung an Absender der Nachricht. Weitere Bearbeitung erst nach Rücksprache mit diesem.
b) durch offene Übermittlung oder nach Übermittlung:	Mitteilung über Kompromittierung an Absender und Empfänger der Nachricht.

V o r k o m m n i s s e	S o f o r t m a ß n a h m e
(3) Kompromittierung eines Exemplars einer Schlüsselserie	

a) vor Übermittlung damit bearbeiteter Sprüche:	Außerkraftsetzung aller Exemplare der betreffenden Schlüsselserie. Bereits damit bearbeitete Klartexte mit den nächsten für diesen Verkehr vorgesehenen nicht kompromittierten Schlüsselunterlagen neu chiffrieren.
b) nach Übermittlung damit bearbeiteter Sprüche:	Außerkraftsetzung aller Exemplare der betreffenden Schlüsselserie. Mitteilung über Kompromittierung an Absender und Empfänger damit übermittelter Nachrichten.
(4) Kompromittierung von Additionsreihen	
a) vor Übermittlung damit bearbeiteter Sprüche	- Bereits bearbeitete Klartexte mit den nächsten für diesen Verkehr vorgesehenen nichtkompromittierten Additionsreihen neu chiffrieren.

19

<u>V o r k o m m n i s s e</u>	<u>S o f o r t m a ß n a h m e</u>
b) nach Übermittlung damit bearbeiteter Sprüche:	- Bearbeiter des Empfangsheftes Mitteilung über Kompromittierung an absendende Chiffrierstelle(n) desselben Schlüsselbereiches. - Kompromittierte Additionsreihe, falls nicht anders angewiesen, innerhalb 48 Stunden Vernichten. Mitteilung über Kompromittierung der betreffenden Textteile <u>an Absender und Empfänger der Nachricht.</u>
(5) Kompromittierung der Substitutionstafel oder des Schlüsselcodes	- Meldung erforderlich. - Betreffende Substitutionstafel oder betreffender Schlüsselcode bleiben in Kraft.
(6) Wiederholtes Benutzen von mehreren aufeinander folgenden Additions- elementen zum Chiffrieren in einem Spruch:	
a) ohne Übermittlung des Spruches:	Fehler korrigieren.

20

<u>V o r k o m m n i s s e</u>	<u>S o f o r t m a ß n a h m e</u>
b) und Übermittlung des so bearbeiteten Spruches:	Mitteilung über Kompromittierung der betreffenden Textteile an absendende bzw. empfangende Chiffrierstelle und Mitteilung an Absender und Empfänger der Nachricht.
(7) Anwendung falscher kryptologischer Addition beim Chiffrieren (z. B. Subtraktion statt Addition)	
a) vor Übermittlung des so bearbeiteten Spruches:	Fehler korrigieren.
b) nach Übermittlung des so bearbeiteten Spruches:	Keine Sofortmaßnahme erforderlich. Bei Notwendigkeit offene Mitteilung über Art des Fehlers an empfangende Chiffrierstelle.

<u>V o r k o m m n i s s e</u>	<u>S o f o r t m a ß n a h m e</u>
(8) Verschiebung des Zwischentextes gegenüber der bereits verwendeten Additionsreihe bei Berichtigungen	
a) vor Übermittlung des so bearbeiteten Spruches:	Fehler korrigieren.
b) nach Übermittlung des so bearbeiteten Spruches:	Mitteilung kompromittierter Klartextteile an Absender und Empfänger der Nachricht.
(9) Verwendung von Schlüsselunterlagen eines verfahrensfremden Typs	
a) ohne Übermittlung des Spruches:	Klartexte mit den für den Verkehr vorgesehenen Schlüsselunterlagen des zugewiesenen Typs neu bearbeiten.

- b) und Übermittlung des Spruches: | - Sofortmeldung erforderlich.
| - Ursachen ermitteln und die sich daraus ergebenden Sofort-
| maßnahmen durchführen.
-

22

GVS-ZCO/122/75 - Blatt 12

5. Beispiele

Für die Bildung des Zwischentextes in den Beispielen wurde die Substitutionstafel [TAPIR](#) verwendet. Die Codegruppen sind frei gewählt. Als Abkürzungen wurden verwendet:

KT = Klartext
hKT = hergerichteter Klartext
ZwT = Zwischentext
CT = Chiffretext
AR = Additionsreihe
KG = Kenngruppe

Kenngruppen und Additionsreihen für die Beispiele [16-18](#) sind aus der Kenngruppentafel und den Additionsreihen der Beispiele in der "[Gebrauchsanweisung zum Verfahren PYTHON \(manuell\)](#)", [GVS-ZCO/123/75](#), entnommen.

Beispiel 1:

KT: VVS 120/69
An Einsatzgruppe R
Einsatzbereitschaft

Mit Wirkung vom 14.4. um 17.00 Uhr ist die volle Einsatzbereitschaft zu gewährleisten.

Leiter des Einsatzstabes
Mauerhöft

hKT: vvs » 120/69 $\hat{=}$ 120/69 \approx einsatzgruppe = r $\hat{=}$ r \emptyset
ab » 14.4. 1700 $\hat{=}$ 14.4 1700 \approx uhr volle einsatz

Beispiel 2:

KT: zu 1.: Nachfrage bezüglich Exportauftrag Nr. ...

hKT: z u » 1 : ↑ nachfrage ≈ be z u

ZwT: 79 72 82 11 90 84 24584 81 51 79 72

hKT: e g l i ch ↑ exportauftrag n r » ...

ZwT: 1 57 62 2 53 84 36527 3 4 82 ...

Beispiel 3:

KT: ... ? \$ \$...

hKT: ...fragezeichen paragraph dollar ...

Beispiel 4:

KT: ...Werden 3 PKW am 14. des...

hKT: ...werden » 3 ≈ pkw ≠ am » 14. ≈ des...

KT: ... PKW F9 IA 25-23...

hKT: ...pkw ≠ f»9≈ia»25-23...

KT: ...1/2...1/3...

hKT: ...1/2...1/3...

oder: ...0,5...ein≠drittel

KT: ...in Gerswalde...

hKT: ...in#gerswalde...

KT: ...Herrn Tien Ken Sin wurden die...

hKT: ...herrn#tien#ken#sinØtienkensin#
wurden die...

Beispiel 5:

KT: ...ab 14.7. Alarmbereitschaft für Großenhof...

hKT: ...a b ↑ 14.7. ↑ alarmbereitschaft

ZwT: ...0 50 84 53587 84 32941

hKT: f u e r g r o s z e

ZwT: 56 72 1 4 57 4 64 69 79 1

hKT: n h o f...

ZwT: 3 59 64 56...

Beispiel 6:

KT: ...Fasz binder... ...Saegers...

hKT: ...faszbinder... ...saegers...

rpt: ...faszszbinder... ...saeegers...

Beispiel 7:

KT: ...Großenhain... ...Müller...

hKT: ...grosenhain... ...muller...

rpt: ...groszenhain... ...mueller...

Beispiel 8:

KT: ...sind in XVI/12. enthalten...

hKT: ...sind#in#xvi»/12.~enthalten...

oder: ...sind#in#roem#xvi#/12.~enthalten...
lten...

Beispiel 9:

KT:	<u>Positions-Nr.</u>	<u>Benennung</u>	<u>Nr. des Teiles</u>
	16	Schneckenrad	16.374.001
	17	Kegelrad	18.440.003
	18	Zwischenwelle	18.464.000

hKT:

lies » 3 ≈ spalten Ø

pos.nr.#benennung#nr.desteilø

» 16 ≈ schneckenrad » 16 374 001 Δ 16374001Ø

17 ≈ kegelrad » 18 440 003 Δ 18440003Ø

18 ≈ zwischenwelle » 18 464 000 Δ 18464000

Beispiel 10:

Dreiteiliger Klartext:

1. Teil: VS-Einstufung (VS-Nr.) Empfänger Text a ff
2. Teil: b Text ff
3. Teil c Text Absender

Beispiel 11:

1. Spruch: Vierteiliger Klartext:

1. Teil: VS-Einstufung (VS-Nr.) Empfänger
Text aa ff
2. Teil: ab Text ff
3. Teil: ac Text ff
4. Teil: ad Text Absender

2. Spruch: Dreiteiliger Klartext:

1. Teil: VS-Einstufung (VS-Nr.) Empfänger
Text ba ff
2. Teil: bb Text ff
3. Teil: bc Text Absender

Beispiel 12:

KT: VS-Einstufung (VS-Nr.) Empfänger X, Y, Z,
1. zirkularer Textteil
1. individueller Textteil für X
1. individueller Textteil für Y
1. individueller Textteil für Z
2. zirkularer Textteil
2. individueller Textteil für X
2. individueller Textteil für Y
2. individueller Textteil für Z
3. zirkularer Textteil Absender

hKT:

Zirkularer Text: VS-Einstufung (VS-Nr.) Empfänger
(für X, Y, Z) (allgemein)

1. zirk. Textteil ia 2. zirk Textteil ib
3. zirk. Textteil Absender

Individueller Text: VS-Einstufung (VS-Nr.) ia 1. ind. Text-
(für X) teil für X ib 2. ind. Textteil für X

Individueller Text: VS-Einstufung (VS-Nr.) ia 1. ind. Text-
(für Y) teil für Y ib 2. ind. Textteil für Y

Individueller Text: VS-Einstufung (VS-Nr.) ia 1. ind. Text-
(für Z) teil für Z ib 2. ind. Textteil für Z

Beispiel 13:

Schema der Übermittlung

A ---> B ---> C

Zu chiffrierender Klartext durch Stelle A:

VS-Einstufung (VS-Nr.) Empfänger C Text Absender A

Zu chiffrierender Klartext durch Stelle B:

VS-Einstufung (VS-Nr.) Empfänger C Text Absender A

Beispiel 14:

KT: Siehe [Beispiel 1](#):
 hKT: v v s » 1 2 0 / 6 9 ∆ 1 2
 ZwT: 74 74 69 82 11 22 00 93 66 99 85 11 22

 hKT: 0 / 6 9 ≈ e i n s a t z g
 ZwT: 00 93 66 99 81 1 2 3 69 0 70 79 57

 hKT: r u p p e ≠ r ∆ r ∅ a b »
 ZwT: 4 72 67 67 1 83 4 85 4 80 0 50 82

 hKT: 1 4 . 4 . 1 7 0 0 ∆ 1 4 .
 ZwT: 11 44 89 44 89 11 77 00 00 85 11 44 89

 hKT: 4 . 1 7 0 0 ≈ u h r v o l
 ZwT: 44 89 11 77 00 00 81 72 59 4 74 64 62

 hKT: l e e i n s a t z b e r e i
 ZwT: 62 1 1 2 3 69 0 70 79 51 4 1 2

hKT: t s c h a f t g e w a e h r l
 ZwT: 70 69 53 0 56 70 58 76 0 1 59 4 62

 hKT: e i s t e n ∅ e i n s a t z
 ZwT: 1 2 69 71 3 80 1 2 3 69 0 70 79

 hKT: s t a b m e y e r h o e f t
 ZwT: 60 70 0 50 63 1 78 1 4 59 64 1 56 70

Beispiel 15:

ZwT: Siehe [Beispiel 14](#)

Zwischentext in Fünfergruppen:
 74746 98211 22009 36699 85112 20093
 66998 11236 90707 95747 26767 18348
 54800 50821 14489 44891 17700 00851
 14489 44891 17700 00817 25947 46462

62112 36907 07951 41270 69530 56705
87601 59462 12697 13801 23690 70796
07005 06317 81459 64156 70838

Beispiel 16:

ZwT: Siehe [Beispiel 15](#)

AR: 11194 30270 81029 97833 96055 23380 962...
ZwT: 74746 98211 22009 36699 85112 20093 669...
CT: 85830 28481 03028 23422 71167 43373 521...

AR: ..773 89765 29674 25982 71326 46518
ZwT: ..796 07005 06317 81459 64156 70838
CT: ..469 76760 25981 06331 35472 16346

Beispiel 17:

CT: Siehe [Beispiel 16](#):

KG: 08494

Spruch:

08949 85830 28481 03028 23422 71167 43373 521...
..469 76760 25981 06331 35472 16346 08949

Beispiel 18:

Spruch: Siehe [Beispiel 17](#)

CT:

08949 85830 28481 03028 23422 71167 43373 521...

AR: 11194 30270 81029 97833 96055 23380 962...

ZwT: 74746 98211 22009 36699 85112 20093 669...

hKT: v v s » 1 2 0 / 6 ...

CT: ..469 76760 25981 06331 35472 16346 08949

AR: ..773 89765 29674 25982 71326 46518

ZwT: ..796 07005 06317 81459 64156 70838

hKT: z s t a bme yer h oe f t ≠

Beispiel 19:

Vom Spruch mit der Kenngruppe 59215 sind die 14. bis 18. und die 23. bis 26 Gruppe fehlerhaft.

Rückfrage: 59125 a) 14-18 b) 23-26

Antwort: 59215 a) 14-18 b) 23-26
a) 49364 67211 85398 35172 74624
b) 99113 86527 53740 73802

30

13.1. Spruch eines HV A Agenten. Sammler*12

Der dargestellte Spruch wurde bei der Festnahme eines HV A Agenten gefunden.
Zur Substitution des Klartextes wurde die Tabelle HV A (1970) genutzt.
Zur Verkürzung des Spruches desweiteren ein kleines Codebuch.
Soweit alles noch in Ordnung. Am 6.4. Funkempfang
Störung gehabt falls gesendet bitte wiederholen.
Dokumente Übergabe: beachten, fahren 14. Juni in Urlaub.

88362/38

58196 12860 79791 53817 27623

42869 98874 84423 21773 32478

90955 00634 53114 74580 69091

**dem Agenten ist hier ein Fehler
unterlaufen, dieser ist beab-
sichtigt und kennzeichnet den
Agenten als "Unentdeckt"**

81473 38737 59008 08966 68990

80143 86588 17364 01633 07805

61516 14215 66362 09599 65795

89444 89906 40663 16586 82487

90015 14822 80909 50227 22531

79459 93728 20562 66703 04918

37575 17607 18690 74079 79575
41771 56993 94896 90871 12469
78246 63590 02486 64840 81934

15137 31867 12868 61696 59062
06404 25073 87915 69317 68015
11531 56830 99773 20903 17077

62683 99371 10727 68613 92740
86273 22145 20427 76952 98449
48856 11416 30144 34565 80189

76413 89111 44489 90778 73223
55388 19901 00856 07393 53545
21791 98012 44235 97061 26768

87479 08771 90909
09366 26570 50716
86735 24241 40615

Darstellung des kodierten Textes anhand des o.g. Spruches:

58196 12860 79791 53817 27623
S O W EI TA L LE SN O C HIN

81473 38737 59008 08966 68990
OR D N UN G .A Mzi 6zi .

89444 89906 40663 16586 82487
zi 4 zi .cod cod S T ÖR U
Funk

Empfang

37575 17607 18690 74079 79575
N G G E HA B T . FA L LS G

15137 31867 12868 61696 59062
ESEN DE T BI T TEcod .cod
Wiederholen

62683 99371 10727 68613 92740
cod : B EA C H TEN - FA

Dokument
Übergabe

76413 89111 44489 90778 73223
HREN zi 1 4zi . J UNIIN

87479 08771 90909
UR L A U B . .

Das Setzen des Signal Zahl "89" nach den Zahlen bzw. vor den Satzzeichen ist notwendig denn die Spüche werden durch die empfangene Chiffrierstelle mit dem Chiffriergerät [T-305](#) bzw. [T-307/3](#) automatisch dechiffriert und dazu ist es notwendig das die entsprechende Registerumschaltung, in dem Fall Code "89", vorhanden ist. Fehlt diese muß der Chiffreur den Spruch entstümmeln.

13.2. Ein in der BStU gefundener Spruch an Kurras. BStU*285

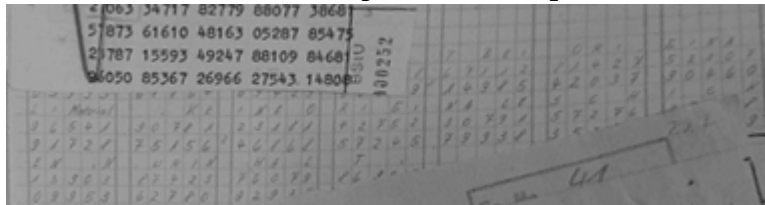


Abb.: Spruchunterlagen des MfS HVA an Kurras.
Beachtenswert ist, das die Unterlagen **vollständig** erhalten sind.
Im Normalfall wird nur der Klartext und evtl. der kontrollde-
chiffrierte Text in den Akten aufbewahrt. Das die Wurmreihen
mit den hergestellten Klartexten noch vorhanden sind entspricht
nicht den in allen Chiffrierorganen festgelegten Normen!
Das ZCO hat solche Handhabungen immer [kritisiert](#).

Die folgende Darstellung entspricht dem Foto das die BStU
zum Fall Kurras [veröffentlicht](#) hat.

Die Buchstabensubstitution ist das o. g. [HVA Verfahren](#) JUPITER.
Software JUPITER für Windows auf der [Freeware](#) Seite.
Die verwendeten Codes entsprechend der [HVA Codetabelle](#).

BITTE VORSICHT BEI ORIGINAL Material.

KEINE ORIGINALE SCHICKEN. NUR INHALT.

									Material code
KT: Kgr.	BIT	TE V	O RSI	C H	T BEI	ORI	GINA	L	
hKT: xxxxx	71286	86195	81452	72768	67112	81427	52307	96541	
OTP: 27063	34717	82779	88077	38681	57873	61610	48163	05287	
GTX: 27063	05993	68866	69429	00349	14985	42037	90460	91728	
KT: . KE	INE O	RI GI	NA LE	S C H	I C K	EN .N	URIN	HA L	T .
hKT: 90781	23181	42752	30791	57276	27278	13903	87423	76079	86900
OTP: 85475	23787	15593	49247	88109	84681	96050	85367	26966	27543
GTX: 75156	46868	57245	79938	35375	03859	09953	62780	92935	03443

Die abgebildete Wurmtabelle:

27063	34717	82779	88077	38681
57873	61610	48163	05287	85475
23787	15593	49247	88109	84681
96050	85367	26966	27543	14808

Zusätzlich sind noch weitere, nicht verwendete, Wurmtabellen vorhanden.



Abb.: Wurmtabellen, zum Vorgang Kurras. BStU

14. Funk- und Chiffrierunterlagen aus einem verschlossenem ^{Sammler*12}
Stahlbehälter mit dem Funkgerät SP-15, das in der DDR gefunden wurde.
Das ZCO versuchte mittels des Programmes [P-674](#) die BND Sprüche zu dechiffrieren.



Abb.: Sender SP-15 Sammler^{*12}
Anleitung zum Verschlüsseln

Zum Verschlüsseln muß der Klartext (KT) zunächst so vorbereitet werden, daß in ihm nur die 26 Buchstaben des Alphabetes und die Satzzeichen "Punkt" und "Komma" vorkommen. Zu diesem Zweck werden ä, ö, ü und ß in ae, oe, ue, ss umgewandelt.

Bei Zahlen werden die einzelnen Ziffern dreimal hintereinander gesetzt und als Ganzes durch Einschließen in "y" hervorgehoben.

Beispiel: 11 = y 1 1 1 1 1 1 y (siehe Seite 7)

Die Satzzeichen werden, soweit nicht besondere Abkürzungen vorgesehen sind, durch die ihnen entsprechenden Wörter ersetzt.

(Siehe Seite 7)

Bekannte Abkürzungen werden in "y" gesetzt und wiederholt.

Beispiel: km = y km y km y

Ein- und zweistellige Abkürzungen die weniger bekannt sind, werden durch die entsprechenden Buchstabierwörter ausgedrückt, jedoch nicht in "y" gesetzt (sonst Verwechslung mit Namen).

Beispiel: T54 = tango y 5 5 5 4 4 4 y [\(Siehe Seite 7\)](#)

Buchstabieralphabet

A = ALPHA	J = JULIET	S = SIERRA
B = BRAVO	K = KILO	T = TANGO
C = CHARLIE	L = LIMA	U = UNIFORM
D = DELTA	M = MIKE	V = VICTOR
E = ECHO	N = NOVEMBER	W = WHISKY
F = FOXTOTT	O = OSKAR	X = XRAY
G = GOLF	P = PAPA	Y = YANKEE
H = HOTEL	Q = QUEBEC	Z = ZULU
I = INDIA	R = ROMEO	

Beispiel: Der zu verschlüsselnde Klartext sei:

Am 2.8., 1800 Uhr, hinter Tor II keine Kfz mehr.
auf dem Hof 5 T 54 verschmutzt.

Der zu verschlüsseln vorbereitete Klartext lautet dann:

a m 2 . 8 . , 1 8 0 0 u h r , h i n t e r
t o r r o e m 2 k e i n e k f z m e h r .
a u f d e m h o f 5 t a n g o 5 4 v e r
s c h m u t z t .

Die Buchstaben und Satzzeichen dieses vorbereiteten Klartextes werden nun mit Hilfe der Umsetztabelle "dein star" in den Zwischentext (ZwT) verwandelt.

Umsetztabelle

	0	1	2	3	4	5	6	7	8	9
	D	E	I	N			S	T	A	R
4	B	C	F	G	H	J	K	L	M	O
5	P	Q	U	V	W	X	Y	Z	.	,

In dieser Tabelle sind den 8 häufigsten Buchstaben der deutschen Schriftsprache - dies sind die Buchstaben, die z. B. in "dein star" vorkommen - die Einzelziffern von 0 bis 3 und von 6 bis 9. den restlichen 18 Buchstaben in alphabetischer Reihenfolge und den Satzzeichen "Punkt" und "Komma" die Ziffernpaare von 40 bis 59 zugeordnet.

Es ist also

a = 8 g = 43 m = 48 s = 6 y = 56
 b = 40 h = 44 n = 3 t = 7 z = 57
 c = 41 i = 2 o = 49 u = 52 . = 58
 d = 0 j = 45 p = 50 v = 53 , = 59
 e = 1 k = 46 Q = 51 w = 54
 f = 42 l = 47 r = 9 x = 55

Die Umsetzung des Beispiel-Klartextes in den Zwischentext ergibt:

KT: a m y 2 2 2 y 8 8 8 y ,
 ZwT: 8 48 56 2 2 2 56 8 8 8 56 59

KT: y 1 1 1 8 8 8 y u h r
 ZwT: 56 1 1 1 8 8 8 56 52 44 9

KT: , h i n t e r t o r r o
 ZwT: 59 44 2 3 7 1 9 7 49 9 9 49

KT: e m y 2 2 2 y k e i n e
 ZwT: 1 48 56 2 2 2 56 46 1 2 3 1

KT: y k f z y k f z y m e h
 ZwT: 56 46 42 57 56 46 42 57 56 48 1 44

KT: r . a u f d e m h o f y
 ZwT: 9 58 8 52 42 0 1 48 44 49 42 56

KT: 5 5 5 y t a n g o y 5 5
 ZwT: 5 5 5 56 7 8 3 43 49 56 5 5

KT: 5 4 4 4 y v e r s c h m

ZwT: 5 4 4 4 56 53 1 9 6 41 44 48

KT: u t z t .
ZwT: 52 7 57 7 58

Das Beispiel zeigt, daß verschiedene Buchstaben und Satzzeichen durch Ziffernpaare ausgedrückt werden. Zur besseren Übersicht des Zwischentextes empfiehlt es sich, zwischen den einzelnen Buchstaben und Satzzeichen einen genügend großen Abstand zu halten.

Dieser nur noch aus Zahlen bestehende Zwischentext (ZwT) wird nur mit Hilfe der gekennzeichneten Schlüsselrolle (Zahlwurm = iW) " B R I E F " überschlüsselt. Hierzu werden die benötigten 5er-Gruppen von der Schlüsselrolle zeilenweise auf einen Blatt Papier übertragen. Von Zeile zu Zeile ist ein so großer Abstand zu lassen, daß später unter jede Zeile noch 2 weitere Zahlenreihen geschrieben werden können. (Kariertes Papier erleichtert anfangs das Verschlüsseln)

Achtung:

Bevor der Zwischentext unter die übertragenen 5er-Gruppen des Zahlenwurms geschrieben wird, überprüfen, ob auch alle Zahlengruppen fehlerfrei herausgeschrieben worden sind.

Beispiel:

Die erste Zeile der Schlüsselrolle seien:

53437 49502 63216 75486 53582 54420 58783 87207 88832 26363

55104 32277 29424 36944 67916 28104 27035 62894 52111 16121

11774 84421 35035 21388 24646 68669 23663 87164 79677 69138

40265 36835 07388 57838 27823 80079 30474 48305 21427 53598

Der in Ziffern umgewandelte Zwischentext wird nun - beginnend

bei der 2. Gruppe - unter den Zahlenwurm gesetzt.

Beispiel:

iW: 53437 49502 63216 75486 53582 54420 58783 87207 88832 26363
ZwT: ----- 84856 22256 88856 59561 11568 88565 24495 94423 71974

iW: 55104 32277 29424 36944 67916 28104 27035 62894 52111 16121
ZwT: 99949 14856 22256 46123 15646 42575 64642 57564 81449 58852

Jetzt wird immer die untere Ziffer von der oberen Ziffer abgezogen, und zwar erfolgt die Subtraktion modulo 10, d.h. ohne Zehnerübertragung.

Beispiel:

4	-	8	=	6	(=14 - 8)
9	-	4	=	5	
5	-	8	=	7	(=15 - 8)
0	-	5	=	5	(=10 - 5)
2	-	6	=	6	(=12 - 6)

Das Ergebnis der Subtraktion stellt den Geheimtext (GT) dar, der übermittelt wird. Am Anfang steht unverändert die erste 5er-Gruppe des Zahlenwurmes als Kenngruppe (hier: 5 3 4 3 7) zur Kennzeichnung des Schlüsselwurmes.

Siehe dazu das folgende Beispiel auf Seite 6:

Unser Beispiel:

iW: 53437 49502 63216 75486 53582 54420 58783 87207 88832 26363
ZwT: ----- 84856 22256 88856 59561 11568 88565 24495 94423 71974
GT: 53437 65756 41060 97630 04021 43962 70228 63812 94419 55499

iW: 55104 32277 29424 36944 67916 28104 27035 62894 52111 16121
ZwT: 99949 14856 22256 46123 15646 42575 64642 57564 81449 58852
GT: 66265 28421 07278 90821 52370 86639 63493 15330 71772 68379

Der Anfang des zu übermittelnden Beispiel-Geheimtextes lautet:

53437 65756 41060 97630 04021 43962 70228 63812 94419 55499

Sollte die letzte 5er-Gruppe des Zahlenwurmes vom Zwischentext nicht vollständig ausgenutzt sein, werden die restlichen Ziffern der 5er-Gruppe des Zahlenwurmes mit übermittelt.

Jede 5er-Gruppe des Zahlenwurmes darf nur einmal benutzt werden.

Nach dem Verschlüsseln sind die verbrauchten Zeilen des Schlüsselwurmes abzuschneiden und zu verbrennen. Auch eine nur teilweise verbrauchte Zeile wird mitvernichtet.

Die Verschlüsselung der nächsten Mitteilung beginnt mit der nächsten Zeile des Zahlenwurmes, wobei wieder die erste Gruppe der ersten Zeile unverändert als Kenngruppe am Anfang des G-Textes steht.

<u>K l a r t e x t</u>	<u>Z w i s c h e n t e x t</u>
Punkt	58 (nach Umsetz-Tabelle)
Doppelpunkt	58 58 (= 2 Punkte nach Umsetz-Tabelle)
Komma	59 (nach Umsetz-Tabelle)
Fragezeichen	f r a g e
Bine- Gedanken- oder	
Schrägstrich	q q
Bruchstrich	b r u c h
Klammer(.....)	k k kk.....kk
Absatz	s t o p
Magdeburg	y magdeburg y
Koethen	y koethen y koethen y
Grollmann-Kaserne	y grollmann y grollmann y qq kaserne
1	y 111 y
11	y 111 111 y
1000	y 111 000 000 000 y
1 000 000	y 1 y million
0100 Uhr	y 111 y uhr

1300 Uhr	y 111 333 y uhr
2245 Uhr	y 222 222 444 555 y uhr
3. 12. (Datum)	y 333 y 111 222 y
bekannte 2- und mehr- stellige Abkürzungen	y y y
km	y km y km y
Lkw	y lkw y lkw y
3,5 kg	y 333 , 555 yy kg yy kg yy
1-stellige und unbekannte Abkürzungen	nach Buchstabiertafel bzw. ausschreiben
V 2	victor y 222 y
4 m	y 444 y meter
2 3/4 t	y 222 y 333 bruch 444 y tonnen
JS-II	julius siegfried qq roem y 222 y
07 (Beispiel f. lfd. Spruch-Nr.)	y 000 777 y

TAFEL F

CODE - TAFEL

ZNA = ORANIENBURG	LMN = sowj. Luftwaffe
XOB = GRANSEE	HIK = sowj. Truppe
WPC = BERNAU	EFG = Nationale Volksarmee
VRD = BERLIN	BCD = NVA/Luftstreitkräfte
USE = KREMMEN	
TZF = NEURUPPIN	UVW = Julius-Fucik-Kaserne
DEF = LEEGEBRUCH	RST = Sachsenhausen-Kaserne (KZ)
ABC = ANNAHOF	NOP = Heinkel-Siedlung
STG = WUPPERTAL	KLM = Übungsgelände bei
	GHI = Fla-Raketen-Stellung (SO VEHIEFANZ)
RUH = Flugplatz	
PVI = STARTBAHN	OPR = Bahnhof
OWK = Rollbahn	STU = Bahntransport
NXL = Gleisanschluß	VWX = Fahrzeigkolonne
MAZ = Treibstofflager	
XZA = Radarstellung	CDE = Auslagerung
	ZAB = Ablageort
LBX = Flugbetrieb	PRS = Norden

KCW = kein Flugbetrieb	MNO = Süden
IDV = Start	IKL = Westen
HEU = Landung	PGH = Osten
GFT = Einzelstart	= in Richtung
FGS = Gruppenstart	
EHR = Platzrunde (n)	
DIP = Einzelflug	
CKO = Formationsflug	
BLN = Belegung	
AMN = Räumung	
WXZ = Neubelegung	
TUV = Flugzeug-Nummer	

Hinweise zur Anwendung der Funkunterlage

Hinter jeder Planzeit der Funkunterlage sind 3 Frequenzkennner angegeben, bestehend aus je einer Zahl und einem Buchstaben.

Bis auf Widerruf dürfen nur die Frequenzkennner der mittleren Kolonne (Farbkennzeichnung grün) verwendet werden.

Dem Buchstaben entsprechend wird der Kristall für die betreffende Planzeit gewählt. Jeder Kristall kann für die 2 Frequenzen verwendet werden (Grundfrequenz und Frequenzverdoppelung). Beide Frequenzwerte sind auf dem Kristall untereinander angegeben. Bei Angabe der Zahl 1 vor dem Buchstaben muß die Grundfrequenz, d.h. der niedrigere Frequenzwert (obere Stanzung) am Gerät eingestellt und abgestimmt werden. Steht die Zahl 2 vor dem Buchstaben, so muß der doppelte Frequenzwert (untere Stanzung) auf der Abstimmtable aufgesucht und das Gerät entsprechend eingestellt werden.

(Kristall = Steck-Quarz)

Wenn wegen veränderter Ausbreitungsbedingungen die Frequenzkennner aus einer anderen Kolonne (andere farbige Kennzeichnung!) gewählt werden müssen, erhalten Sie eine Mitteilung etwa folgenden Inhalts: "Ab (Datum) Frequenzkennner (Farbe) verwenden. Erbitten Bestätigung."

Die Bestätigung des Überganges auf eine andere Frequenzkennnerfarbe von einem bestimmten Zeitpunkt an ist äußerst wichtig, weil Sie bei nicht vorhandener Bestätigung weiterhin nach den

zuletzt gültigen Frequenzkennern überwacht werden und dabei Gefahr laufen, daß Ihre Sendungen nicht gehört werden.

Wird die Bestätigung durch ein Kurzsignal gegeben (Tafel 9), so ist dieses Kurzsignal mit der bisher gültigen Frequenzkennerkolonnie zu verschiedenen Planzeiten je einmal innerhalb von 3 aufeinander folgenden Wochen zu senden. Eine zusätzliche Bestätigung auf einem anderen Meldeweg ist empfehlenswert.

Auszug aus dem Frequenztabelle des BND Schweigefunkers:

JANUAR

E 158/I

010I	00I2	IE	ID	IA	III5	2H	IN	IK	072I	IB	IB	IB
	I409	I5	IN	2A	I7I5	IN	2A	ID	2036	IF	IB	IA
020I	0448	ID	IB	IB	0627	IC	IA	IA	0845	II	II	IE

...

usw. usf.

Bedienungsanweisung für KSG

I. Verschlüsselung und Vorbereitung

1) Schlüsselbeispiel

	evtl.Füll- ziffern	Schlüssel- Kennziffern			
Wurmtext:	---	63725	38013	80804	72471
minus					
Zwischentext:		---	11327	36501	24390
gleich					
Signaltext:		63725	27796	54303	58181
		ii			

Den Wurmtext liefert jeweils eine Zeile (20 Ziffern) der

Schlüsselrolle.

Der Zwischentext ist die gemäß Signaltafel, Pos. 1 bis 15, umgesetzte Meldung (15 Ziffern).

Der Signaltext setzt sich zusammen aus: eventuell Füllziffern, den Schlüsselkennziffern, "ii" und 15 Ziffern Geheimtext (Subtraktionsergebnis von Wurmtext minus Zwischentext modulo 10).

- 2) Alle Schlüsselvorgänge auf Richtigkeit prüfen (sehr wichtig), dann Wurm- und Zwischentext streichen.
- 3) Heraussuchen der einzelnen Segmente des Signaltextes und Anordnung in gleicher Reihenfolge.
- 4) Lückenloses Einlegen der Segmente in die Geberscheibe, jedoch in umgekehrter Reihenfolge des Signaltextes, also mit "181--" beginnen und mit den Kennziffern, abschließend. Um eine sichere Arretierung des zuletzt eingelegten Segments durch die Blattfeder zu gewährleisten, kann es notwendig werden, dieses Segment, auch wenn es eine Kennziffer ist, gegen ein passendes auszutauschen.
- 5) Benutzte Wurmzeile der Schlüsselrolle abschneiden und zusammen mit Meldungstext und Zwischenmaterial vernichten.

II. Bedienungsanleitung für G e b e r

- 1) Kurbel eindrehen und Geberscheibe so weit drehen, daß die beiden blauen Punkte einander gegenüberstehen.
- 2) Geberscheibe zum Einlegen der Segmente nach Entfernung der Rändelmutter abnehmen.
- 3) Lückenlos gefüllte Geberscheibe einsetzen (Mitnehmerscheibe roter Punkt bei rotem Punkt!), dann mit Rändelmutter festschrauben.
- 4) Bei angeschlossenem und abgestimmtem Sender Kurbel möglichst gleichmäßig, 2 mal pro Sekunde (1 Scheibenum-

drehung in 5 sec.), drehen.

- 5) Beachten, daß Abtastfeder nicht berührt oder gar verbogen wird.

III. Bedienungsanleitung für den S e n d e r

Achtung! Netzteil nur für Wechselspannung!

(Bei 220 V : Sicherung 0,4 A, bei 110 V : Sicherung 0,8 A.)

A. Grundabstimmung aller Frequenzen zwecks Eintragung der erzielten Werte in die Tabelle für Abstimmwerte unter Verwendung der für die Sendungen vorgesehenen Antennenanlage.

- 1) Sender und Netzgerät zusammenstecken, weiß markierten Schalter auf "Aus", Leistungsschalter in Stellung (*), grün markierten Schalter auf "0" stellen
- 2) Geber mit Sender verbinden, Antenne in rote Buchse, Erdleitung oder Gegengewicht in schwarze Buchse stecken. Netzschnur an Netzteil und Steckdose anschließen.
- 3) Frequenzwert 1 (obere Stanzung) vom Quarz A ablesen und notieren, Quarz in Quarzbuchse stecken (kleine Öffnung),
- 4) Auf der Abstimmtablette des Senders unter "f" diejenige fettgedruckte Frequenzzahl aufsuchen, die der Sendefrequenz am nächsten liegt (beachte: Frequenz am Quarz in kHz, auf der Tabelle in MHz, 1 MHz = 1000 kHz). Bedienknöpfe "blau", "rot" und "gelb" entsprechend den Farben auf die neben der Frequenzzahl stehenden Werte stellen.
- 5) "Weißen" Schalter über 235 auf 220 schalten, dabei das darüberliegende Instrument beobachten. Der Zeiger muß möglichst auf der Marke im schwarzen Sektor stehen. Bei Überspannung auf 235 bleiben, bei Unterspannung auf 205, notfalls nach Entfernung der Sicherheitsschraube auf 190 schalten (Vorsicht! Bei wiederansteigender Spannung zurückschalten!).

- 6) "Blauen" Knopf bei gedrückter Taste etwas hin und her drehen, bis darüberliegende Glimmlampe am hellsten leuchtet.
- 7) "Roten" Knopf bei gedrückter Taste nachstellen, bis darüberliegende Glimmlampe am hellsten leuchtet (eingestellter Wert darf nicht sehr weit entfernt vom Tabellenwert liegen, z. B. nicht 1 statt 8).
- 8) "Grünen" Knopf Stufe um Stufe nach rechts drehen. Bei jeder Stufe "roten" Knopf auf jeweils hellstes Leuchten der Glimmlampe nachregeln (s. Ziff. 7 !). Vorgang solange durchführen, bis größter Ausschlag am Antenneninstrument erreicht ist.
- 9) Leistungsschalter auf volle Leistung (●) stellen. Abstimmvorgang gemäß Ziff. 8 weiterführen, bis größter Ausschlag am Antenneninstrument erreicht ist. Ändert sich der Ausschlag in der Stellung vor dem Maximum nur wenig, ist unbedingt die niedrigere Stufe vorzuziehen. Nochmaliges Nachstimmen mit "blauem" Knopf auf hellstes Leuchten der darüberliegenden Glimmlampe.
- 10) Notieren der endgültigen Einstellwerte des "blauen", "gelben", "roten" und "grünen" Knopfes in die Tabelle für Abstimmwerte bei 1 A.
- 11) Wiederholung des Abstimmvorganges 4) - 9) für alle Frequenzen (Grundfrequenz und Frequenzverdoppelungen) und Eintragen der erzielten Abstimmwerte hinter den entsprechenden Frequenzkennern der Tabelle.

B. Verkürzter Abstimmvorgang vor den einzelnen Sendungen
(nur anwendbar, wenn gleiche Antennenanlage wie bei der Grundabstimmung benutzt wird)

- 1) Geräteaufbau entsprechend A. 1) und 2)
- 2) Quarz gemäß Funkunterlagen auswählen und in Quarzbuchse stecken. Frequenzkennern gemäß Funkunterlage in der Tabelle für Abstimmwerte aufsuchen und die zugehörige Abstimmwerte

am Sender einstellen. Leistungsschalter auf volle Leistung (0) stellen. Dieser Vorgang soll etwa 5 Min. vor der festgelegten Sendezeit beendet sein.

- 3) 1 Minute vor der Sendezeit ist das Gerät einzuschalten (siehe A. 5)
- 4) Pünktlich zur festgelegten Sendezeit wird der Sender durch Nachstellen des "blauen" und "roten" Knopfes bei gedrückter Taste auf hellstes Leuchten der darüberliegenden Glimmlampe abgestimmt und unmittelbar danach wird mit dem Drehen begonnen.

Dauer des Abstimmvorganges: höchstens 15 Sekunden
Dauer der Sendung: 45 Sekunden (keinesfalls länger!)

IV. Fehlersuchanleitung

1. Instrument am Netzteil zeigt keine Netzspannung an:
 - a) Kontrolle, ob Steckdose Strom führt (Netzspannungsprüfer oder Tischlampe)
 - b) Kontrolle der Sicherung am Gerät
 - c) Netzschnur mit dazugehörigen Steckern auf Unterbrechung prüfen.
2. Dauerndes Durchbrennen der Sicherung:
 - a) Spannungswähler auf richtiger Netzspannung ?
 - b) Röhren wechseln
 - c) Schluß im Gerät. Neues Gerät anfordern.
3. Lämpchen am blauen Knopf wird beim Durchdrehen nicht heller:

- a) Stimmt Frequenzbereich ? (Bereichsfarbe beachten!)
 - b) Quarz schwingt nicht; zur Kontrolle mit anderem Quarz versuchen!
 - c) Schwingt kein Quarz, Röhre EL95 wechseln.
4. Kein Ausschlag am Antenneninstrument zu erzielen, obwohl Glimmlampe "blau" Resonanz anzeigt:
- a) Knopf "grün" zu weit rechts?
 - b) Antennenunterbrechung? (Stecker und Zuleitung kontrollieren)
 - c) Abstimmtaste defekt, Kontaktfeder auf Zahlensegment stellen.
 - d) Röhre EL81 wechseln.

Tafelkennziffer 1 0 Tafelkennziffer 2 (Wiederholung) 0 <u>Persönliche- und Spannungstafel</u> IV/60		Zeitangaben 3 0 = entfällt 1 = heute 2 = gestern 3 = in den letzten 3 Tagen 4 = seit letzter Sendung 5 = morgen 6 = in den nächst. 3 Tagen 7 = in den nächst. 14 Tagen 8 = für die Dauer von 1 Monat 9 = für die Dauer von 3 Monaten		Persönliche Verhältnisse 4 0 = entfällt 1 = bin erkrankt (zu Hause) 2 = bin erkrankt (auß in Krankenhaus) 3 = gehe in Urlaub (am Ort) 4 = gehe in Urlaub (nach auswärts) 5 = Verwandtenbesuch 6 = Einweisung von Untermietern 7 = ziehe um im Ort 8 = ziehe um nach auswärts 9 = alles wieder normal		Sicherheitslage 5 0 = entfällt 1 = Schwierigkeiten aufgrund polit. Differenzen 2 = fühle mich überwacht 3 = wurde kontrolliert 4 = mußte zur Vernehmung 5 = rechte mit Hausdurchsuchung 6 = Verhaftung in nächster Umgebung 7 = soll mich als Spitzel verpflichten 8 = fühle mich enttarnt 9 = alles wieder normal			
Aufklärungsmöglichkeiten 6 0 = entfällt 1 = beruflich stark angespannt 2 = auf Geschäftsreise 3 = muß zu einem Lehrgang 4 = wurde dienstverpflichtet 5 = werde eingezogen 6 = Aufklärung eingeschränkt 7 = Aufklärung nicht mehr möglich 8 = Aufklärung verbessert 9 = alles wieder normal		Führung und Meldung 7 0 = entfällt 1 = Anweisung verstanden 2 = Anweisung undurchführbar 3 = Anweisung nicht verstanden 4 = GT-Brief abgeschickt 5 = TBK geleert 6 = schreibe nicht mehr an DA 7 = auß Sendetätigkeit eingeschränkt (Stromsperr) 8 = vernichte Gerät, melde an DA 9 = vernichte Gerät, setze mich nach Westen ab		Führung und Meldung 8 0 = entfällt 1 = am Meldein verhindert 2 = Tätigkeit wieder aufgenommen, komme laufend 3 = komme in 3 Tz.z. Treffort 4 = komme in 6 Tz.z. Treffort 5 = kann nicht z. Treff kommen 6 = TBK anlaufen 7 = TBK nicht anlaufen 8 = TBK-Philung fehlt 9 = GT-Mittel für Postweg erbeten		Milit. Verbände u. Organe 9 0 = entfällt 1 = SOA 2 = NVA 3 = Bereitschaftspolizei 4 = Grenzpolizei 5 = Transportpolizei 6 = Kampfgruppen 7 = GSt 8 = örtl. Parteileitung SED 9 = Betriebsparteileitung SED		Maßnahmen 10 0 = entfällt 1 = Alarmbereitschaft, Verbringung d. abbl. Sachen 2 = Bewachung öfftl. Gebäude u. Verkehrsanlagen 3 = Errichtung v. Straßensperren 4 = Vorbereitung v. Luftschutzmäßen 5 = Zusammenschließung im Standort od. St.O.-Nähe 6 = Eintreffen v. Verstärkern 7 = Beschlagnahmungen 8 = Ausnahmesperre, Ausgangssperre 9 = Deportationen	
Maßnahmen 11 0 = entfällt 1 = Straßensperren u. verschärfte Kontrollen 2 = verschärfte Bahnkontrollen 3 = verschärfte Spitzelsystem, Verhaftungen u. Vernehmungen 4 = Anwendung v. Waffengewalt 5 = Postverkehr nach außerhalb d. DDR unter Vorlage von Ausweis 6 = Postverkehr nur noch innerhalb d. DDR 7 = Reiseperr nach Ost-Bln. und BRD 8 = Reisebeschränkung innerhalb d. DDR 9 = alles wieder normal		Bevölkerung u. Betriebe 12 0 = entfällt 1 = Bevölkerung allgemein 2 = Bevölkerung kommunitätlich eingestellt 3 = Bevölkerung pro West eingestellt 4 = eigener Betrieb 5 = andere Betriebe 6 = Jugend und Studenten 7 = Arbeiter 8 = Funktionäre 9 = Behörden		Verhalten 13 0 = entfällt 1 = normal 2 = Demonstrationen u. Aufmärsche 3 = Streik 4 = Bildung oppositioneller Gruppen 5 = Sabotage 6 = Flugblätter, Vandalen 7 = Aufstand 8 = Verstärkte Republikflucht 9 = Gefangenenerbefreiung		Ursachen 14 0 = entfällt 1 = allgem. Unzufriedenheit 2 = Lohnforderungen 3 = Hormenerhöhungen 4 = Rationierungsmaßnahmen 5 = Soziale Einschränkungen 6 = Verschärfung der polit. Lage 7 = Wirksamkeit westlicher Propaganda 8 = Übergriffe von Truppe oder Polizei 9 = Reaktion auf westl. Maßnahmen		Auswirkung 15 0 = entfällt 1 = Lebensmittelknappheit 2 = Brennstoff- und Brennstoffknappheit 3 = Stilllegung von Betrieben 4 = Zerstörungen, Brände 5 = Menschenverluste 6 = Zusammenbruch der Versorgung 7 = Einlenken 8 = Aufhebung von Maßnahmen 9 = alles wieder normal	

Abb.: Tafel 0, Persönliche und Spannungstafel. Sammler*12

Anmerkung zur Substitutionstabelle DEIN STAR

In der "Cryptologia 31" Artikel von Jan Bury "The U.S. and West German Agent Radio Ciphers" wird dargestellt das durch die polnischen Sicherheitskräfte von 1959 an bis 1970 zwölf Agenten ergriffen wurden die für den U.S. Geheimdienst bzw. den BND gearbeitet haben. Seit 1959 verwendeten die BND Agenten die Substitutionstabelle "DEIN STAR". Diese Substitutionstabelle wurde bis 1989 nie geändert. Der U.S. Geheimdienst verwendete eine andere Substitution und Chiffrierung,

diese ist unter [Punkt 9.2](#) dargestellt.

Erwähnenswert ist das im ["Spektrum der Wissenschaft Kryptologie"](#) in dem Sammler [*86](#)
 Artikel: "Handverfahren" von Otto Leiberich auf Seite 22f die Substitutionstabelle
 "STEIN RAD" und "EI STRAND" dargestellt wird.
 Hierzu auch der Vergleich zu "DEIN STAR".

STEIN RAD	EI STRAND	DEIN STAR
\ 0 1 2 3 4 5 6 7 8 9 - S T E I N R A D 5 B C F G H J L M N O 6 P Q U V W X Y Z	\ 0 1 2 3 4 5 6 7 8 9 - E I S T R A N D 2 B C F G H J L M N O 3 P Q U V W X Y Z	\ 0 1 2 3 4 5 6 7 8 9 - D E I N S T A R 5 B C F G H J L M N O 6 P Q U V W X Y Z . ,

15. Sprechtafeln des MfS zur Verschleierung des UKW-Funk ^{BStU*29}

Weitere [Tarntafeln](#) des MfS,

für Personen- Objektüberwachungen.

Tafel				103			
72							
Üb1	Greifswalder Straße	Lichtenberg	Prenzlauer Allee	A	I	P	X
Alex	Üb2	Marzahn	Prenzlauer Berg	B	3	Q	8
Bernau	Grünau	Üb3	Schöneeweide	C	J	R	Y
Buch	Buch	Mitte	Üb4	1	K	6	Z
Erkner	K-Marx-Allee	Üb5	Schönhauser Allee	D	L	S	Ä
Frankfurter Allee	Karlshorst	Ostbahnhof	Stralauer Allee	E	4	T	9
Üb7	Üb6	Ostkreuz	Treptow	F	M	U	Ö
Friedrichshain	Köpenick	Pankow	Weisensee	2	N	7	Ü
Friedrich- straße	Üb8	Üb9	U.d.L.	G	O	V	-
Palast der Republik	Leninallee	Parkplatz	Üb10	H	5	W	0

Mitropa	Kaufhaus	Bahnhof	Richtung	Rückfrage bei Üb
Haus des Lesens	Centrum Warenhaus	Hotel		Verzögerung um ... Min.
	Weltzeituhr	Hotel Newa		

Tafel 72 für Personenschutz und Personenüberwachung / Kontrollen.

	H / S / F	D / O / I	A _{/J}	N _{/B}	C _{/M}	C _{/R}	L _{/K}	P _{/E}
F/K	passiert	Kind	A	F	K	6	8	Ä
P/E	Leitz	Wartburg	1	G	L	Q	V	Ö
A/M	Schloß	Trabant Schloß	B	3	M	R	W	O
R/G	Zahn	Trabant Zahn	C	H	5	S	X	Ü
B/N	Kreuz	Lada K	D	I	N	/	Y	-
O/J	männl. P	Schnalle	2	J	O	T	9	?
D/S	weibl. P	✘	E	4	P	U	Z	verlassen

Tafel 63 für Personenschutz und Personenüberwachung / Kontrollen.

Tafel 72	O/M	Q/W	B/S	T/X	V	I	U	L
A	läufer 1		blockierung	PP8867	A	H	P	W
K	läufer 2	abgeparkt	Festnahme	D6706	1	I	6	X
G	Person	zu Fuß		Richtung	B	J	Q	Y
B	personen				C	4	R	9
K	männl.	zurück	Lada weiß CU 91 - 09	Lada weiß CU 65 -	D	K	S	Z

Z	weibl.	passiert	Daccia beige BY 69 - 57	Moskwitsch gelb CU 55 - 56	2	L	7	Ä
E	Kind	Wotanstr. 19a	Moskwitsch rot CN 60 - 21	Wartburg blau CU 65 - 67	E	M	T	Ö
F	D	Kunzstraße 22	Wartburg braun CLA 5 - 14	Wartburg beige CU 63 - 99	F	5	U	0
D	Y	Brixener Str. 21	Lada blau CV 71 - 36	Wartburg/ Tau weiß CN 53 - 53	Y	N	V	Ü
C	Q	Koppenstr. 48			3	0	8	-
R	grünes Kennz.		Fahrer	Kofferraum	steigt ein			
H	5000		Pkw verlassen	Fond	versteckt			
P	5000 vermutlich			zugestiegen				

Tafel 72 genutzt, für einen Einsatz.

Vorschrift für die Nutzung der o. dargestellten Sprechtafel 72
Mischalphabete für die Sprechtafel 72

Dieses Blatt verbleibt auf
der Dienststelle!

Blatt 02 Exemplar

Der Wechsel der Mischalphabete erfolgt wöchentlich, montags ab 08,00 Uhr
bzw. mit Dienstbeginn.

Die ersten 13 Buchstaben des Mischalphabets werden links senkrecht ein-
getragen. In jede Zeile ein Buchstabe.

Die restlichen 12 Buchstaben werden oben waagerecht von links nach rechts
eingetragen. In die ersten 4 Spalten jeweils 2 Buchstaben und in die ande-
ren 4 Spalten jeweils 1 Buchstabe.





Woche:

31. N D T O A J Z B R K V W X U I G N H L E Y P C Q S






32. T N W L C F D E P R X M Y C A U J S B O Q I Z X V

33. usw. usf.

Dieses Blatt verbleibt auf der Dienststelle, es wird nur zur Einweisung verwendet.
Bedeutung der Phrasen und Symbole bei der Sprechtafel 53

2261	= TJ 1662	Signal	
7386	= LT 6837	ausgel.	= Signal ausgelöst
5921	= LW 1295	Position2	= Botschaft der USA
5958	= NM 8595	Variant.	= variabler Stützpunkt wird benötigt
100	= männliche Person	ben.	
verl. m. 10	= verlassen mit weibliche P.	 pp	=Parkhaus Keibelstraße
verl. o. 10	= verlassen ohne weibliche P.	 pp	= Parkhaus Hotel ""Stadt Berlin"
10	= weibliche Person	 pp	= Parkhaus Hotel"Metropol"
W-stand	= leistet Widerstand	✖	= Treff
SO wird verlangt	= ein sowjetischer Offizier wird verlangt		= blockieren

Tafel
53

	V/H	M/C	E/Y	R/Z	N/A	G/S	K/P	D/U	L
H/E	Ein -	Aus -		BSU 000166 -	Richtung	A	H	P	W
F/G			100	10	Position 2	1	1	6	X
L/N	2661	7386		passiert	PP	B	J	Q	Y
T/K	5921	5958	abge- stellt	Sicht		C	4	R	9
V/M			achten auf	W-stand	Variante A	D	K	S	Z
R/O	braun	grün	Aufgabe	SO wird verlangt	Variante B	2	L	7	Ä
C/W	schwarz	weiß	beginnen/ begonnen	Übergang	Variante C	E	M	T	Ö
J/P	blau	beige		verlassen	Variante D	F	5	U	0
B/X	rot	gelb	beenden/ beendet	Variante ben.	Variante E	G	N	V	Ü
D/U		verl. m. 10		 PP		3	0	8	-
A/Y	zu Fuß	verl. o. 10	Gegenmaß- nahme	 PP					
S/Z	Signal ausgel.		fahren ab	 PP	Pkw aus- gefallen	S	A	S	B

Beispiel einer angewendeten Sprechtafel No. 53

Chi 4401
1. 11. 1968

Vertrauliche Verschlusssache!
MfS - 020 Nr. 3758/68

14 Blatt Ex. Nr. 0021

Blatt 1

Instruktion über Formularcodes

1. Zweck
- 2.
3. Begriff
- 4.
5. Vorteile
- 6.
7. Nachteile
- 8.
9. Formulartypen
- 10.
11. Einsatzmöglichkeiten
- 12.
13. Chiffrierung
- 14.

Chi 4401

MfS - 020 Nr. 3758/68 -Blatt 2-

1. Zweck

Diese Instruktion enthält die allgemeinen Prinzipien, die bei der Einführung und Anwendung von Formularcodes im geheimen Nachrichtenverkehr zu beachten sind. Sie soll zugleich dazu anregen, stärker als bisher von Formularcodes Gebrauch zu machen, da diese sowohl in ökonomischer Hinsicht als auch hinsichtlich präziser und schneller Nachrichtenübermittlung erhebliche Vorzüge aufweisen.

Diese Instruktion ist keine Arbeitsrichtlinie für die Entwicklung von Formularcodes.

2. Begriff

Der Formularcode stellte eine bestimmte Kategorie der Phrasencodes (Gegensatz: Blankcode) dar, die sich vom einfachen Phrasencode wie folgt unterscheidet: Der einfache Phrasencode enthält als Phrasen einzelne Elemente, Polygramme, Wörter, Wortfolgen, Sätze und der gleichen, die in beliebiger Reihenfolge zu Nachrichtentexten zusammengefügt werden können. Dagegen enthält der Formularcode als Phrasen vollständige oder durch Einfügung bestimmter variabler Angaben zu vollständigen ergänzbare Nachrichtentexte. Reihenfolge der Angaben, Wortlaut der Nachricht evtl. auch die äußere Form (Schriftbild, Format usw.) sind dabei von vornherein festgelegt. Diese Texte können zu einem Code zusammengefaßt werden; sie können aber auch zusätzlich als einzelne Formulare ausgedruckt und dem Empfänger in dieser einheitlichen Originalform ausgehändigt werden. Bei Benutzung technischer Nachrichtenmittel wird nicht der vorgedruckte Text, sondern nur die Bezeichnung des entsprechenden Formulars übermittelt.

Chi 4401

MfS - 020 Nr. 3758/68 -Blatt 3-

3. Vorteile

Formularcodes bieten gegenüber einfachen Phrasencodes folgende Vorteile:

- 3.1. Sie ermöglichen besonders starke Textkürzungen mit allen damit verbundenen weiteren Vorteilen wie:
 - a) Verkürzung und damit Beschleunigung der Schreibarbeit beim Aufsetzen der Nachricht durch den Absender und bei der Niederschrift des Klartextes durch den Empfänger;
 - b) Erhöhung der Chiffrier- und Dechiffriergeschwindigkeit;
 - c) Verkürzung der Übermittlungszeit (bei Benutzung von Fernmeldemitteln);
 - d) Einsparung von Schlüsselunterlagen;
 - e) Einschränkung der Fehlermöglichkeiten (der beim Empfänger wie beim Absender vorgedruckt vorliegende Text bleibt in jedem Fall fehlerfrei), durch weniger Rückfragen und Verzögerungen.

Insgesamt ergibt sich daraus eine Beschleunigung des Spruchdurchlaufes vom Absender bis zum Empfänger. Die aufgezählten Vorteile, insbesondere die Einsparung von Schlüsselunter-

lagen, können die Anwendung von Formularcodes auch in Verbindung mit maschinellen Chiffrierverfahren und bei der Datenübertragung lohnend machen.

Anmerkung: Es ist notwendig diesen Gesichtspunkt zu betonen, da bei der Einschätzung der Zweckmäßigkeit der Anwendung eines Codes oft einseitig aus der Sicht des Chiffreurs geurteilt wird, für den die Anwendung eines Codes in der Regel eine zusätzliche Mühe bedeutet, und dabei die Einsparungen an Arbeitszeit, material und Kosten bei der Produktion von Schlüsselunterlagen und der Nachrichtenübermittlung unberücksichtigt bleiben.

Chi 4401

MfS - 020 Nr. 3758/68 -Blatt 4-

- 3.2. Die Anwendung von Formularcodes erhöht im allgemeinen die Sicherheit bei Anwendung nicht absoluter sicherer Verfahren, wenn das verwendete Formular nicht bekannt ist, da erstens ein zusammenhängender Text leichter zu dekryptieren ist als einzelne isolierte Angaben und zweitens diese selbst nach Dekryptierung für sich noch keinen sinnvollen Text ergeben.
- 3.3. Durch die Standardisierung der Texte und ihre gleichbleibende Anordnung wird die Auswertung der Nachrichten durch den Empfänger erleichtert und beschleunigt. Es ist dadurch auch möglich, bestimmte Angaben, da sie immer an gleicher Stelle stehen, schnell herauszugreifen, ohne erst den gesamten vorangehenden text dechiffrieren zu müssen.
- 3.4. Ein gut aufgebautes Formular zwingt den Absender zu klarer und logischer Abfassung der Nachricht und hilft ihm, keine wichtigen Angaben zu vergessen und überflüssige Angaben wegzulassen.
- 3.5. Liegen die Formulare als zusätzliche Einzeldrucke vor, so können die Nachrichten dem Empfänger in einer Form ausgehändigt werden, die weitgehend der Originalform beim Absender entspricht.
- 3.6. Im mehrsprachigen Nachrichtenverkehr mit Hilfe von Codes weisen Formularcodes gegenüber einfachen Phrasencodes ganz

entscheidende Vorteile auf.

Es gibt zwei Hauptschwierigkeiten bei der wortweisen Übersetzung mittels einfacher Phrasencodes: Die Inkongruenz der verschiedenen Bedeutungen mehrdeutiger Wörter und die grammatikalischen Besonderheiten in beiden Sprachen. Diese Schwierigkeiten spielen bei der satzweisen Übersetzung, wie sie für Formularcodes charakteristisch ist, kaum noch eine Rolle.

Chi 4401 MFS - 020 Nr. 3758/68 -Blatt 5-

Das gilt auch für ein- oder anzufügende variable Angaben, da es sich dabei in der Regel um Begriffe handelt, deren Inhalt in beiden Sprachen voll übereinstimmt, z. B. Zeitangaben, Kartenpunkte, Eigennamen.

Die Anwendung von Formularcodes in mehrsprachigen Nachrichtenverkehren hat demnach eine besonders günstige Perspektive.

Chi 4401 MFS - 020 Nr. 3758/68 -Blatt 6-

4. Nachteile

4.1. Geringe Anpassungsfähigkeit an variable Texte.

Nachrichtentexte, für die kein passendes Formular vorliegt, oder die auch nur einzelne Angaben enthalten, die in den Formularen nicht vorgesehen sind, können mit diesen allein nicht bearbeitet werden. Doch läßt sich dieser Nachteil durch zusätzliche Hilfsmittel wie Substitutionstabellen oder Hilfscode ausgleichen.

4.2. Die Hauptschwierigkeit liegt bei der Entwicklung. Für die Erarbeitung eines Formularcodes genügt es nicht, die im jeweiligen Nachrichtenverkehr häufiger vorkommenden Einzelphrasen zu erfassen und zu einem Code zu verarbeiten, sondern es ist eine durchgreifende Regulierung des Sprachgebrauchs im Nachrichtenverkehr des jeweiligen Anwendungsbereiches erforderlich. Diese Aufgabe kann nicht von dem zuständigen Chiffrierorgan allein gelöst werden. In der Regel ist die Mitarbeit anderer Spezialisten und der Leitung des jeweiligen Bereiches erforderlich.

Chi 4401 MFS - 020 Nr. 3758/68 -Blatt 7-

5. Formulartypen

Bei den Nachrichtentextformularen können u.a. folgende Typen unterschieden werden:

5.1. Typ V (abgeleitet von "vollständig")

Vollständige Nachrichtentexte, die lediglich mit Spruchkopf (Empfänger) und Spruchende (Absender) zu verstehen sind.
Beispiel zu Typ V: Glückwunschtelegramme der Deutschen Post

5.2. Typ U (abgeleitet von "unterbrochen")

Unterbrochene Nachrichtentexte, wobei an den (durch Auslassungspunkte gekennzeichneten) Unterbrechungsstellen variable Angaben eingesetzt werden können. Die variablen Angaben bzw. die ihnen zugeordneten Codegruppen werden vor Chiffrierung und Übermittlung in festgelegter Reihenfolge an die Formularbezeichnung angefügt; der Empfänger fügt die Angaben nach Dechiffrierung und Decodierung an den entsprechenden Stellen des Formulars ein.

Beispiel zu Typ U: Gegnerischer Kernwaffenschlag... (1)
im Raum... (2)
Detonationsstärke... (3) Kilotonnen.
Radioaktive Wolke breitet sich aus in
Richtung... (4)

Dieses Beispiel enthält vier Unterbrechungsstellen für folgende variable Angaben:

(1)Uhrzeit, (2)Kartenkoordinaten, (3)Zahl, (4)Himmelsrichtung.

5.3. Typ W (abgeleitet von Anfangsbuchstaben der Fragewörter)

Fragebogenform. Zu einem bestimmten Fragenkomplex wird, in der Regel zeilenweise untereinander, der Reihe von Einzelfragen vorgedruckt, die zu beantworten sind. Die Fragen sind nummeriert, so daß ein den Fällen, wo aus einem umfangreichen

Fragen angegeben werden müssen, zu denen Antworten gegeben werden. Im umgekehrten Fall, wenn aus einem umfangreichen Fragenkomplex nur wenige Fragen unbeantwortet bleiben, kann auch so verfahren werden, daß auf die Angabe der Frage- bzw. Zeilennummern verzichtet wird und an den Stellen, wo keine Beantwortung erfolgt, Blendgruppen oder die Phrase "Keine Angabe" eingesetzt werden.

Da bei dieser Variante die Antworten in der Regel verschieden lang sind, ist es zur Vermeidung von Mißverständnissen ratsam, den Beginn einer neuen Antwort zu markieren, sei es durch Angabe der Fragenummer oder durch Trennzeichen bzw. doppeltes Trennzeichen (wenn das einfache Trennzeichen auch anderweitig benutzt wird) oder ein anderes für diesen Zweck festgelegtes Symbol.

Beispiel zu Typ W: Transportbefehl (vereinfacht)

01	Einheit	...
02	Verladebahnhof	...
03	Zugnummer	...
04	Wagenbestand der Kategorie I, II, III	...
05	Verladezeit	...
06	Abfahrtszeit	...
07	Entladebahnhof	...
08	Ankunftszeit	...
09	Entladezeit	...
10	Marschroutenach Entladung	...

In der linken Spalte stehen die Frage- bzw. Zeilennummern, in der zweiten Spalte die Fragen, und in die dritte Spalte können die Antworten eingetragen werden. Frage- und Antwortteil können auch getrennt ausgedruckt werden, wobei die Fragennummern auch im Antwortteil vorgedruckt werden müssen.

5.4. Typ T (abgeleitet von "Tabelle")

Tabellenform. Sie beruht auf dem gleichen Prinzip wie die Fragebogenform, doch sind die Fragen nicht zeilenweise, sondern spaltenweise angeordnet. Die Antworten werden ebenfalls spal-

tenweise unter der jeweiligen Frage eingetragen.

Vorzüge der Variante:

- a) Bei Chiffrierung mit einer Additionstabelle kann diese unmittelbar an den Grundtext angelegt und ohne weitere Zwischenschreibarbeit in Geheimtext umgewandelt werden, wenn die Abstände der Grundeinheiten den Abständen der Additionseinheiten angepaßt sind.
- b) mehrere zeitliche aufeinanderfolgende Nachrichten des gleichen Absenders zum gleichen Fragenkomplex können auf einem Formular zeilenweise untereinander geschrieben werden, so daß ein rascher Überblick über Veränderungen, Entwicklungstendenzen, Schwankungen u.dgl. möglich ist.
- c) Mehrere gleichzeitige Nachrichten verschiedener Absender zum gleichen Fragenkomplex können beim Empfänger ebenfalls auf einem Formular zeilenweise untereinander geschrieben werden, so daß ein sofortiger Vergleich, Summierung usw. möglich sind.

Beispiel zu Typ T: Stärkemeldung

Datum	Offiziere	Uffz.	Soldaten	Summe
0 1 1 1	0 0 4 3	0 1 3 4	1 0 5 0	1 2 2 7
0 2 1 1	0 0 4 1	0 1 2 9	1 0 6 7	1 2 3 7

In diesem Beispiel besteht der Grundtext aus vierstelligen Zifferngruppen, die durch geringfügige Herrichtung des Klartextes entstehen, indem das Datum als vierstellige Zahl geschrieben wird und die übrigen Zahlen bei Notwendigkeit durch vorangesetzte Nullen zu vierstelligen Zifferngruppen ergänzt werden. Eine aus vier- oder fünfstelligen Gruppen

bestehende Ziffernadditionsreihe läßt sich bei Anpassung der Ziffern- und Spaltenabstände des Formulars an die Ziffern- und Gruppenabstände der Additionsreihe ohne weiteres anlegen.

Wird eine fünfstellige Additionsreihe benutzt, so sind folgen-

de Regelungen möglich:

- 1) die erste oder letzte Ziffer jeder Fünfergruppe der Additionsreihe wird weggelassen,
- 2) die vierstellige Zifferngruppe des Grundtextes werden durch vorangestellte Nullen zu Fünfergruppen ergänzt.

Chi 4401

MfS - 020 Nr. 3758/68 -Blatt 11-

6. Einsatzmöglichkeiten

6.1. Allgemeine Voraussetzungen

Die Vorteile der Formularcodes können nur dann voll wirksam werden, wenn für den jeweiligen Anwendungsbereich folgende Voraussetzungen gegeben sind:

1. Anfall von stereotypen oder synonymen Nachrichtentexten in größerer Zahl,
2. Standardisierung dieser Nachrichtentexte nach Inhalt u. Form,
3. Durchsetzung der Anwendung dieser Standards.

Die erste Voraussetzung ist in vielen Fällen gegeben. Die zweite und dritte Voraussetzung können nur mit Unterstützung des Leiters der jeweiligen Bereiche erfüllt werden.

- 6.2. Typ V wird weniger zur Anwendung kommen als die anderen Typen, da in den meisten Fällen eine Variationsmöglichkeit gegeben sein muß, um einen unökonomischen Aufwand bei der Vorbereitung kompletter Nachrichtentexte zu vermeiden. Es gibt aber typische, immer wiederkehrende Situationen, bei denen mit einer geringen Anzahl von Textvarianten auskommt, wofür sich dieser Typ anbietet. Ein alltägliches Beispiel sind Glückwunsch- und Beileidsadressen zu bestimmten Anlässen. Ein weiteres Beispiel ist die Auslösung einer bestimmten Alarmstufe mit allen damit verbundenen Maßnahmen in einem bestimmten Bereich; diese Maßnahmen sind gewöhnlich in einem besonderen Dokument zusammengefaßt, das in diesem Fall die Rolle des Formulars spielt, während die Formularbezeichnung durch das entsprechende Alarmsignal übermittelt wird. Die gleiche Regelung ist auch für typische Lagemeldungen und anderes denkbar.

- 6.3. Die Typen U und W sind breit einsetzbar und für alle Situationen geeignet, wo ein öfter wiederkehrender konstanter Nach-

richtenteil durch variable Angaben ergänzt werden muß. Typ U

Chi 4401 MfS - 020 Nr. 3758/68 -Blatt 12-

wird dann benutzt, wenn es sich um eine geringe Anzahl variabler Angaben handelt. Typ W ist aus Gründen der Eindeutigkeit und Übersichtlichkeit vorzuziehen, wenn eine größere Anzahl variabler Angaben übermittelt werden muß.

Als variable Angaben kommen vorwiegend in Betracht: Zeitangaben (Uhrzeiten, Daten, Jahreszahlen u.a.), Maß- und Gewichtsangaben, reine Zahlen, Ortsangaben (Kartenkoordinaten, Ortsnamen, Richtungen u.a.), sonstige Eigennamen (Personennamen, Warenbezeichnungen, Bezeichnungen von Dienststellen, Bereichen, Einheiten u.a.)

- 6.4. Typ T eignet sich besonders für statistische Aufstellungen und sonstige Meldungen, bei denen eine begrenzte Anzahl von Angaben in feststehender Reihenfolge unmittelbar oder mittels eines Hilfscodes als Zifferngruppen dargestellt werden kann, z. B. Stärke-, Bestands-, Bedarfs-, Transportmeldungen.
-

Chi 4401 MfS - 020 Nr. 3758/68 -Blatt 13-

7. Chiffrierung

7.1. Grundsätze

An- oder einzufügende variable Angaben, die der Geheimhaltung unterliegen, sind vor der Übermittlung über technische Nachrichtennetze zu chiffrieren. Die Einsetzung fest zugeordneter Codegruppen für diese Angaben mittels eines Hilfscodes) gilt nicht als Chiffrierung.

Die Formularbezeichnung ist zu chiffrieren, wenn dem Gegner schon die Erkennung des allgemeinen Inhalts der Nachricht von Nutzen sein kann, z. B. die Tatsache, daß es sich um einen Marschbefehl handelt.

Das gleiche gilt für die Zeilen- oder Spaltenbezeichnung der Typen T und W, wenn dem Gegner schon die Tatsache, daß zu bestimmten Fragen Angaben gemacht werden oder keine Angaben gemacht werden, Nutzen bringen kann.

Teilchiffrierung ist zulässig, wenn die offen übermittelten Angaben keine Rückschlüsse auf den konkreten Inhalt der chiffrier-

ten Angaben zulassen.

7.2. Wahl des Chiffrierverfahrens

Die Fachleute, die mit der Entwicklung eines Formularcodes beauftragt sind, müssen bereits im Frühstadium der Entwicklung mit den Stellen in Verbindung treten, die für die Festlegung und Bereitstellung der dafür benötigten Chiffriermittel zuständig sind. Das ist notwendig, weil Typ Form, Aufbau, Textarten der variablen Angaben, Geheimhaltungsgrad und andere Eigenschaften des Formularcodes sowie die Anwendungsbedingungen mit Art des Chiffrierverfahrens sowie Beschaffenheit der Chiffriermittel abgestimmt werden müssen und begrenzte Möglichkeiten hinsichtlich der Chiffriermittel Rückwirkungen auf die weitere Entwicklung des Formularcodes haben können.

Chi 4401

MfS - 020 Nr. 3758/68 -Blatt 14-

7.3. Grundtext

Die Anwendung eines manuellen Schlüsselverfahrens setzt in der Regel voraus, daß ein homogener, nur aus Ziffern oder Buchstaben bestehender Grundtext vorliegt. Liegt der Klartext als homogener Text vor, wie in dem Beispiel unter 4.4., so kann er ohne weiteres der Chiffrierung zugrundegelegt werden; andernfalls ist die Bildung eines homogenen Zwischentextes mittels Hilfscode oder Substitutionstabellen oder beider Mittel erforderlich. Ist nur Tarnung oder Verschleierung erforderlich, so kann die Chiffrierung auch direkt, ohne vorherige Bildung eines Zwischentextes, durch Anwendung einer Tarntafel, einer Sprechtafel, einer Buchstabier- und Zahlentafel, eines Mittels der Kartencodierung oder eines anderen Tarn- oder Verschleierungsmittels erfolgen, vorausgesetzt, daß alle zu chiffrierenden Textteile als Klareinheiten (Phrasen) in diesem Mittel erfaßt sind.

ULTRA-Code

Ausgabe : ALPHA - MIKE

Numeral Code

	A	X	S	W	U	R	Y	I	D	G	E	L	F
V	0	1	2	3	4	5	6	7	8	9	A	B	C
Z	D	0	1	2	3	4	5	6	7	8	9	E	F
J	G	H	0	1	2	3	4	5	6	7	8	9	I
K	J	K	L	0	1	2	3	4	5	6	7	8	9
H	9	M	N	O	0	1	2	3	4	5	6	7	8
O	8	9	P	Q	R	0	1	2	3	4	5	6	7
M	7	8	9	S	T	U	0	1	2	3	4	5	6
C	6	7	8	9	V	W	X	0	1	2	3	4	5
T	5	6	7	8	9	Y	Z	A	0	1	2	3	4
Q	4	5	6	7	8	9	D	E	G	0	1	2	3
B	3	4	5	6	7	8	9	H	I	L	0	1	2
N	2	3	4	5	6	7	8	9	N	O	R	0	1
P	1	2	3	4	5	6	7	8	9	S	T	U	0

Einheiten	Kennwörter	Einheiten	Kennwörter
6840th Tank Batallion	BUMKIN	6837th Air Defense Btl	LAGDUSH
6841th Tank Batallion	BRUNCE	2nd Fighter Squadron	MUZGASH
6843nd Rocket Batallion	CHUBB	6848th Fighter Squadron	NOB
6843rd Motor Rifle Btl	COTMAN	6851th Fighter Squadron	ORCS
6844th Enginee Btl	ELDER	6854th Fighter Squadron	POSTMASTER
6845th Motor Rifle Btl	FALLOHIDE	6860th AWACS Squadron	SHADOWFAX
HQ 1. Luftflotte	FIREFOOT	6863rd Airlift Squadron	SLINKER
6838th HQ Batallion	GOBLIN	6888th Attack Squadron	TOOK
3839th HQ Batallion	GREENHAND	6867th Attack Squadron	WIZARD
1st Air Defense Btl	GRUBB	3rd HQ Batallion	WOSES
6838th Air Defense Btl	LAGDUF	6869th Frigat Task Force	GOLLUM

Deckwörter (Air Base, Stadt)

Pathos	BREE
Maritsa	THAL
Leros	TIRION
Cigli	ARNOR
Kos	VALINOR
Zypern	ROHAN
Samos	NAZGUL
Paradisi	SIRIOR
Limassol	ISEN
Antalya	AINUR
Bodrum	MORIA
Izmir	ENDORAS
Istanbul	GONDORA

Authent. Code

	V	W	X	Y	Z
A	52	15	25	31	02
D	85	35	26	89	33
E	05	58	47	32	39
G	49	81	17	23	37
H	84	08	92	91	73
I	56	12	43	80	88
L	69	74	35	54	53
N	67	34	71	62	76
O	42	29	63	27	16
R	99	10	09	06	30
S	78	97	46	82	68
T	90	14	59	48	21
U	65	44	86	07	20

	D	Z	K	F	G
10	Abgabe	Frequenz	Meldung	Überwachen	Zuweisung
6	Anholung	GefStd	Nebel	Übernehmen	BtrbSt
3	Eintreffen	Grenze	Panzer	Verluste	Ankunft
9	Angriff	Koppeln	Über	Verpflegung	Begleitschutz
2	Auffangen	Luftlandung	Raum	Verwundete	MiG-29SM
4	Ausfall	Lösen	Sendeverbot	VZL	Datum
11	Bedarf	Minen	Sicherung	VRV	AN-72
5	Bergung	Marsch	nach	zerschlagen	später
8	Brücke	Munition	Stellung	zerstören	Abflug
1	Erkundung	Inspizierung	Transport	vorbereiten	folgt

<u>Geronimo</u>	<u>Dull Knife</u>	<u>Lone Wolf</u>	<u>Little Turtle</u>	<u>Woman Chief</u>
Mullah Mansur Mehsud	Maulawi Roshan	Abdul Salaam	Mohamed Omar	Mulfah Baradar