I. GRUNDPRINZIPIEN DER CHIFFRIERUNG VON NACHRICHTEN

Der Nachrichtenkontakt vor allem auf dem Funkweg zwischen z.B. einer inn- und einer ausländischen Stelle kann jederzeit von der gegnerischen Abwehr abgehört, oder, sollte es sich um Kurierpost handeln, abgefangen werden.
Da Funkverkehr auf jeden Fall vom Gegner abgehört wird, müssen die übermittelten Nachrichten so verschlüsselt sein, daß sie nur für den Eingeweihten dechiffrierbar sind.
Um ein Höchstmaß an Sicherheit im Nachrichtenverkehr zu gewährleisten, müssen beim Chiffrieren folgende Grundsätze beachtet werden:

1. Die Nachricht muß kurz (Telegrammstil) formuliert sein.
   Damit wird:
   a) das Chiffrieren erleichtert und
   b) wird es der gegnerischen Abwehr aufgrund der Kürze des Funkspruches erschwert, die Funkstelle anzupeilen.

2. Nachdem die Nachricht in einen BUCHSTABEN- oder ZAHLEN-CODE verwandelt worden ist, muß sie noch einmal mit einem besonderen Code überschlüsselt werden, um auftretende Häufigkeitsverteilungen zu vermeiden. Denn in jeder Sprache kommen bestimmte Buchstaben in einem Text häufiger vor als andere. Diese Häufigkeit spiegelt sich natürlich im verschlüsselten Text wieder, wodurch es für die gegnerische Abwehr leicht wird, die Nachricht zu entschlüsseln.

3. Die chiffrierte Nachricht muß in Fünfergruppen unterteilt werden, um Übermittlung und Empfang einfacher zu gestalten und eventuelle Fehler besser korrigieren zu können.

II. METHODEN DES CHIFFRIERENS

1. Der ZAHLENCODE

Bei dieser Chiffriermethode werden die Buchstaben eines Textes in Zahlen verwandelt, die immer zweistellig sind. Die Buchstaben des Alphabets werden in bestimmter Reihenfolge unter- und nebeneinander geschrieben. In der Horizontalen und Vertikalen werden dann Zahlen von 1 bis 0 in natürlicher oder gemischter Reihen folge eingesetzt; eine Ziffer der Vertikalen und eine der Horizontalen ergeben immer die Dechzahl eines bestimmten Buchstaben.

Einfaches Beispiel:

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

Bei diesem einfachen System ergeben sich die Deckzahlen aus der Vertikalen und Horizontalen:
a = 11; g = 22; s = 43; .... etc.
Dieses System ist in der Praxis untauglich, da es spielend zu entschlüsseln ist.
Im Folgenden soll daher ausführlich ein ausgesprochen sicheres System dargestellt werden, das vornehmlich von antifaschistischen Widerstandsgruppen im zweiten Weltkrieg verwandt wurde.

a)
Aus einem SCHLÜSSELBUCH (das Sender und Empfänger besitzen) wird ein CODEWORT ausgesucht, das aus zehn Buchstaben besteht. Sollten sich Buchstaben in dem Wort wiederholen, so wird die Wiederholung gestrichen; es müssen allerdings zehn Buchstaben übrigbleiben.
Wir verwenden in unserem Beispiel das Buch "Der kleine Lord". Das Schlüsselwort heißt FAUNTLEROY und ist das zweite Wort der 45. Zeile auf Seite 58.
Unter das Schlüsselwort werden jetzt die fehlenden Buchstaben des Alphabets in ihrer alphabetischen Reihenfolge gesetzt.

Beispiel:
F A U N T L E R O Y
B C D G H I J K M P
Q S V W X Z . (als einzige Interpunktion erscheint ein Punkt)

b)
Nun erfolgt die Umwandlung dieser Buchstabenkombination in Zahlen. Dazu werden die Buchstaben des Schlüsselwortes in der Reihenfolge des Alphabets mit 1 - 10 (10 = 0) numeriert

Also A = 1; E = 2; etc.

Beispiel:

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

c)
Um die Buchstaben jetzt in Zahlen ausdrücken zu können, wird links vor die drei Buchstabenreihen je eine vorher ausgemachte Zahl aus der oberen Zahlenreihe eingesetzt. Angenommen es wären die zweite, d.h. 1, die fünfte, d.h. 8, und die siebte, d.h. 2 gewesen. Das ergibt folgendes Bild:

Beispiel:

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

d)
Das Alphabet läßt sich nun durch zweistellige Zahlen ersetzen. Diese Zahlen erreicht man folgendermaßen:
A liegt senkrecht unter der Zahl 1 und auf waagerechter Linie mit 1, das ergibt: A = 11; B liegt senkrecht unter der Zahl 3 und waagerecht auf einer Linie mit der Zahl 8, das ergibt für B = 38; etc.etc.

Beispiel:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
11	38	18	98	21	31	58	88	48	28	78	41	68	51	61	o8

Q	R	S	T	U	V	W	X	Y	Z	.
32	71	12	81	91	92	52	82	o1	42	22

e)
Der Nachrichtentext kann jetzt chiffriert werden.
Folgende Nachricht soll übermittelt werden: 'Es werden starke Truppenbewegungen an der Südküste beobachtet'.
Der Text wird in 'Telegrammstil' übersetzt: 'STARKE TRUPPENBEWEGUNGEN AN SUEDKUESTE'
Die Buchstaben dieses Satzes werden nun durch die Zahlen aus Beispiel d) ersetzt:

Beispiel:

S	T	A	R	K	E	T	R	U	P	P	E	N	B	E	W
12	81	11	71	78	21	81	71	91	o8	o8	21	51	38	21	52

E	G	U	N	G	E	N	A	N	S	U	E	D	K	U	E
21	58	91	51	58	21	51	11	51	12	91	21	98	78	91	21

S	T	E
12	81	21

Das ergibt folgende Zahlenreihe:
1281117178218171910o8o8215138215221589151582151115112912198789121128121

f)
In dieser Form ist die Zahlenreihe überhaupt nicht übermittelbar, die Fehlerquelle ist zu groß. Die Reihe wird daher in Fünfergruppen unterteilt.

Beispiel:

12811	17178	21817	191o8	o8215	13821
52215	89151	58215	11151	12912	19878
91211	28121				

g)
Die Zahlenreihe die wir erhalten haben reicht noch nicht aus. Denn in ihr treten bestimmte Zahlen mit gleicher Frequenz auf, wie bestimmte Buchstaben in der Sprache.
Daher muß der Code noch einmal überschlüsselt werden, um die Frequenzen zu verwischen.
Um das zu erreichen, ordnen wir dem Alphabet Zahlen zu wie in Beispiel d), allerdings nur die erste Stelle jeder Zahl.

Beispiel:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	3	1	9	2	3	5	8	4	2	7	4	6	5	6	o	3	7	1	8

U	V	W	X	Y	Z	.
9	9	5	8	o	4	2

h)
Die Überschlüsselung geht nun folgendermaßen vor sich:
Wir nehmen den Schlüsselsatz der mit dem Schlüsselwort beginnt und ersetzen seine Buchstaben durch die in Beispiel g) erhaltenen Zahlen und ordnen es gleich in Fünfergruppen.

Beispiel:

FAUNT	LEROY	RUTSC	HTEUN	BEHAG	LICHA	UFSEI
31958	4276o	79811	88295	32815	44181	93124

NEMST	UHLHI	NUNDH	EBFAU	NTLER	OYRUT	SCHTE
52618	98484	59598	27349	58427	6o798	11882

(Reicht der Decksatz in der Länge nicht aus, wird er von vorn ohne Unterbrechung weitergeschrieben)

i)
Nun werden die Zahlengruppen aus f) und h) addiert.
Dabei ist darauf zu achten, daß die Zehnerstellen nicht mitgeschrieben werden: also 5+8=13 schreibe aber 3 .

Beispiel:

Zahlengruppen der Nachricht (f)	12811	17178	21817	191o8	o8215
Zahlengruppen des Schlüsseltextes (h)	31958	4276o	79811	88295	32815
Endgültig verschlüsselter Text	43769	59838	9o628	97393	3oo2o
Fortsetz.	13821	52215	89151	58215	11151
	44181	93124	52618	98484	59598
	579o2	45339	31769	46699	6o649
	12912	19878	91211	28121	
	27319	58427	6o798	11882	
	39221	67295	519o9	399o3	

j)
Um die Nachricht endgültig sendefertig zu machem, muß ihr eine Information beigegeben werden, die dem Empfänger die Stelle im Schlüsselbuch bezeichnet, an der er Schlüsselwort und -satz finden kann. Zu diesem Zweck bildet man eine Zahlengruppe, die Seite, Zeile und Wort umfaßt. In unserem Falle würde das heißen: Seite 58, Zeile 45, Wort 2 = 58452

Diese Zahlengruppe wird am Ende der Nachricht durchgegeben. Die sendefertige, verschlüsselte Nachricht lautet also:

43769 59838 9o628 97393 3oo2o 579o2 45339 31769
46699 6o649 39221 67295 519o9 399o3 58452

k)
Um den in j) aufgestellten Funkspruch zu dechiffrieren, muß der Empfänger folgendermaßen vorgehen:

1. gemäß den Angaben der letzten Zahlengruppe sucht er im Schlüsselbuch das Schlüsselwort und den Schlüsseltext.
2. Mit dem Schlüsselwort erstellt er nun ein Zahlenalphabet gemäß Beispiel c) und d).
3. Danach subtrahiert er die sich aus dem Schlüsseltext ergebende Zahlenreihe (Beispiel h) von den ihm übermittelten Zahlen. Es verbleiben Zahlengruppen gemäß Beispiel f).
4. Die Zahlenreihe wird in Zweiergruppen unterteilt und wird gemäß Beispiel d) in Buchstaben umgesetzt, womit das Telegramm lesbar wird.

Beispiel:

Funkspruch	43769	59838	9o628	97393	3oo2o	579o2
- Schlüsseltext	31958	4276o	79811	88295	32815	44181
Verbleiben	12811	17178	21817	191o8	o8215	13821
Klartext	S T	A R K	E T	R U P	P E	N B E
	45339	31769	46699	6o649	39221	67295
	93124	52618	98484	59598	27319	58427
	52215	89151	58215	11151	12912	19878
	W E	G U N	G E	N A N	S U	E D K
	519o9	399o3				
	6o798	11882				
	91211	28121				
	U E	S T E				

Dieser Zahlencode ist nur für den entschlüsselbar, der das Schlüsselbuch hat und den jeweiligen Schlüsselsatz kennt.
Für den Funker ist er leicht durchzugeben und zu empfangen, da er sich auf zehn Zeichen beschränken kann. Der Funker braucht notfalls nur die Zahlen zu beherrschen.
Der Nachteil dieses Verfahrens liegt darin, daß

a. die Verschlüsselte Nachricht doppelt so lang ist wie der Klartext (A = 11; etc.) und

b) die Verschlüsselung nach diesem Code für den Codierer eine langwierige und komplizierte Präzisionsarbeit ist, die viele Fehlerquellen in sich birgt.

2. Der BUCHSTABENCODE

Diesem Code liegt folgendes Prinzip zugrunde:
die Buchstaben des Klartextes werden durch andere Buchstaben, die sich im Zusammenhang mit dem Schlüsseltext ergeben, ersetzt.
Das Grundprinzip sieht folgendermaßen aus:

Nachricht →

Schlüsseltext ↓

	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	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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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. Horizontal und vertikal wird das Alphabet aufgetragen, wobei das vertikale eine Zeile unter dem horizontale und eine Stelle nach links verschoben beginnt.

Dieser Buchstabencode hat dem Zahlencode gegenüber einige Vorteile:

a) Man bedarf keiner zusätzlichen Überschlüsselung. Durch die Anordnung der Tabelle treten keine Frequenzen auf. Aus Beispiel 2. ist z.B. zu ersehen, daß für den dreimal auftretenden Buchstaben 'T' in unserer Nachricht drei verschiedene Codebuchstaben erscheinen, nämlich B,Y und Z.

b) Der Code ist leicht zu handhaben; sowohl das Chiffrieren wie das Dechiffrieren geht schnell und relativ mühelos.

c) Die Buchstabenanzahl im Code ist identisch mit der des Klartextes. Beim Buchstabencode behält der Text also seine Länge und wird nicht verdoppelt wie beim Zahlencode.

Nachteile liegen eventuell in folgenden Punkten:

a) Die Funker müssen das gesamte Alphabet perfekt beherrschen und darüberhinaus die Zahlen, da die Stellenangabe von Schlüsselwort und -text nur in Zahlenform möglich ist.

b) Der Buchstabencode verführt in Grenzfällen möglicherweise beim Abhören zu Assoziationen des Funkers (Silben etc.), die zu Fehlern führen können. Diese Gefahr ist allerdings gering.

Verwendet wird normalerweise ein Buchstabencode des dargestellten Systems, allerdings mit einer wesentlichen Erschwerung:

> In der Horizontalen wird ein SCHLÜSSELWORT eingetragen und zwar von vorn an. Die in diesem Wort nicht enthaltenen Buchstaben werden in ihrer alphabetischen Reihenfolge hinter dem Schlüsselwort aufgetragen.

Das Chiffrieren und Dechiffrieren findet nach dem Gleichen System statt wie in 1. - 4. geschildert.
Die einzige Erschwerung besteht darin, daß mit jedem neuen Schlüsselwort eine neue Tabelle nötig wird.
Ein geübter Schreibmaschinenschreiber benötigt dazu ca. 15 - 2o Minuten.
Beispiel siehe nächste Seite!

Wir nehmen dasselbe Beispiel wie beim Zahlencode.
Schlüsselwort: F A U N T L E R O Y
Schlüsselsatz: FAUNTLEROY RUTSCHTE UNBEHAGLICH AUF SEINEM STUHL HIN UND HER
Nachricht: STARKE TRUPPENBEWEGUNGEN AN SUEDKUESTE

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

Chiffrierung der Nachricht:

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

Fortsetz.

S U E D K U E S T E
L I C H H I N U N D
R C Y Q Z C Q J M B

Sendefertig heißt der Code also:

ALVSC MYZKM YAWNY LFMWK ICCUB RCYQZ CQJMB 58452