Notizen zum Kurs KRYPTOGRAFIE, fbi, h-da, 2008

Quellen:

Whitfield Diffie: The First Ten Years of Public-Key Cryptography, Proceedings of the IEEE Band 76 (Heft 5), 1988, S.560-577
Grundlegender Artikel, eine Art *BigBang* der modernen Kryptografie.

Albrecht Beutelspacher: Kryptologie, Vieweg-Verlag
Einführender Text, vielfach neu aufgelegt. Viele Inhalte dieser Notizen orientieren sich am *Beutelspacher*.

Bruce Schneier: Applied Cryptography, 2. Auflage, Wiley, 1996
Standardwerk der modernen Kryptologie (Kompendium)

AJ Menezes, PC van Oorschot und SA Vanstone: Handbook of Applied Cryptography.
Weiteres Standardwerk, online verfügbar unter:
http://www.cacr.math.uwaterloo.ca/hac/

J.Buchmann: Einführung in die Kryptographie, Springer-Lehrbuch, 1999
Weiterführendes Standardwerk, inzwischen in der 3. Auflage. Es beschreibt (mathematisch anspruchsvoll) den aktuellen Stand des Fachs. Enthält die Mathematik der modularen Arithmetik und der Gruppentheorie.

PGP (Pretty Good Privacy)
Software, populäres Kryptosystem. Ursprünglich entwickelt von Phil Zimmermann, dann kommerziell weiterentwickelt von Network Associates, seit langem Open Source (GPG).

Cryptool
Reichhaltiges und anwenderfreundliches Paket mit Demos aller Art zur Kryptografie. Ursprünglich entwickelt von der Deutschen Bank, inzwischen in Händen der TU Darmstadt.

Teil 1 Historisches

Kryptografie (also die Lehre, Texte für fremde Augen unlesbar zu machen) gibt es seit Menschengedenken. Und immer hatte Kryptografie Ähnlichkeiten mit der Geschichte vom Hasen und dem Igel: Ständig erfanden die Kryptografen neue todsichere Chiffren und nie dauerte es lange, bis die Codebrecher (die Kryptoanalytiker) die Chiffre gebrochen hatten. Stationen dieser langen Geschichte sind die *Cäsar-Chiffrierung* (siehe unten) und die *Enigma* (siehe Ergänzungen) aus dem letzten Weltkrieg.
Seit kurzem (genauer seit Erscheinen des oben zitierten Artikels von Whitfield Diffie) hat sich Grundlegendes geändert. Es scheint, als hätten die Chiffrierer derzeit einen Vorsprung vor den Codebrechern, der schwer einholbar ist.

Außerdem: In früheren Zeiten war Kryptografie eifersüchtig gehütetes Herrschaftswissen. Jetzt dagegen ist starke Kryptografie gratis für jedermann im Internet verfügbar, die Kryptografie hat sich *demokratisiert*. Bezeichnend sind die ebenso hartnäckigen wie vergeblichen Versuche, starke Kryptografie zu verbieten.

Cäsar-Chiffrierung
Caesar sprach: S B K F S F A F S F Z F .
Was sprach Caesar?

Nachdem Sie die Cäsar-Chiffre gebrochen haben, gehen wir gleich zu einer etwas besseren Chiffre über:

Schlüsselwortchiffre:
Ein **Schlüssel** besteht aus einem *Schlüsselwort* und einem *Schlüsselbuchstaben*.

Beispiel: Schlüsselwort = SCHRIFT
Schlüsselbuchstabe = e

Man notiert nun das Klartextalphabet in die erste Zeile und schreibt das Schlüsselwort darunter und zwar beim Schlüsselbuchstaben beginnend:

Klarbuchstabe: 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 C H R I F T

Zur kompletten Chiffriertabelle kommt man nun, indem man in der zweiten Zeile und hinter dem Schlüsselwort beginnend die noch fehlenden Geheimbuchstaben (angefangen bei A) einträgt.

Im Beispiel resultiert die folgende **Chiffrier-Dechiffrier-Tabelle**:

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

Beispiel (mit Schlüsselwort/-buchstabe: SCHRIFT/e)
Klartext: peterchensmondfahrt
Geheimtext: GS...

Bei der Schlüsselwortchiffre wird jeder Klarbuchstabe einem festen Geheimbuchstaben zugeordnet. Die Buchstaben werden permutiert, die Schlüsselwortchiffre ist also eine **Permutations-Chiffre.**

Man erkennt, daß Verschlüsseln und Entschlüsseln bei der Schlüsselwortchiffre fast identisch ablaufen, die Chiffre ist insofern **symmetrisch**. Die Verschlüsslerin (traditionell **Alice** genannt) benutzt die Chiffriertabelle von oben nach unten.

Der Entschlüssler (**Bob** genannt) benutzt sie von unten nach oben.

Selbstverständlich muß beiden, Alice und Bob, der benutzte Schlüssel (im Beispiel *SCHRIFT/e*) bekannt sein. Insbesondere bedeutet das, daß Alice und Bob den Schlüssel irgendwann vorher auf sicherem Wege ausgetauscht haben müssen.

Permutationschiffren gibt es soviele, wie es Permutationen der 26 deutschen Buchstaben gibt, also 26! (26 *Fakultät*). Letzteres ist eine astronomisch große Zahl, woraus man schließen könnte, daß Kryptografie auf Basis von Permutationschiffren eine sichere Sache ist.

Die Permutationschiffre ist gewiß sicherer als die Cäsarchiffre. Das Problem ist nur, daß feste Klarbuchstaben immer auf dieselben Geheimbuchstaben abgebildet werden, und das wiederum bedeutet, daß man die statistischen Buchstabenhäufigkeiten der deutschen Sprache ausnutzen kann: Der häufigste Buchstabe im Geheimtext entspricht sehr wahrscheinlich einem e !

Die folgende Tabelle gibt die **statistischen Häufigkeiten von Buchstaben** in Texten deutscher Sprache wieder:

a	6,51 %	k	1,21 %	u	4,35
b	1,89	l	3,44	v	0,67
c	3,06	m	2,53	w	1,89
d	5,08	n	9,78	x	0,03
e	17.40	o	2,51	y	0,04
f	1,66	p	0,79	z	1,13
g	3,01	q	0,02		
h	4,76	r	7,00		
i	7,55	s	7,27		
j	0,27	t	6,15		

Der mit Abstand häufigste Buchstabe ist e (17,4%).
Der ebenfalls deutlich zweithäufigste Buchstabe ist n (9,78%).
Also wird man, wenn der Text nur genügend lang ist (>= 500 Buchstaben), die Äquivalente zu e und n mit großer Sicherheit identifizieren.

Hinter e und n wird eine deutlich abgehobene Gruppe gebildet von den Buchstaben

i , s , r , a , t (Prozentzahlen zwischen 7,55 und 6,15)

die als Gruppe identifiziert werden können. Jedoch wird man noch nicht sagen können, welcher Buchstabe innerhalb dieser Gruppe welches Äquivalent hat.

Um hier weiterzukommen, werden Buchstabenpaare abgezählt, deren Häufigkeiten im Deutschen ebenfalls gut bekannt sind.

Häufigkeiten einiger Bigramme in Texten deutscher Sprache:

en	3,88%	nd	1,99%
er	3,75	ei	1,88
ch	2,75	ie	1,79
te	2,26	in	1,67
de	2,00	es	1,52

Das statistisch häufigste Buchstabenpaar ist *en* (3,88%), also das Paar aus den bereits identifizierten Buchstaben e und n.
(Damit hat man eine Möglichkeit, die Zuordnungen für e und n zu kontrollieren.)
Wir prüfen e in Zweierverbindung mit Buchstaben aus der Gruppe {i,s,r,a,t} nach Häufigkeit. Das häufige Paar ist *er* (3,75%), womit es also möglich ist, den Buchstaben r in der Gruppe {i,s,r,a,t} zu identifizieren. Die nächsthäufige Kombination mit e ist das Paar *te*, welches zusätzlich dadurch charakterisiert wird, daß das umgekehrte Paar *et* sehr selten auftritt.
Der Buchstabe i wird dadurch herausgehoben, daß die Kombination *ei* und *ie* fast gleich häufig sind.
Bleiben s und a innerhalb der Gruppe {i,s,r,a,t}. Diese beiden können dadurch unterschieden werden, daß e in Kombination mit s signifikant häufiger ist als e in Kombination mit a.
Ferner ist es möglich, die Buchstaben c und h zu identifizieren, die in der Kombination *ch* sehr häufig, einzeln aber eher selten auftreten.

Damit sind also die Äquivalente der Buchstaben e,n,i,s,r,a,t,h,c bekannt, die zusammen schon mehr als zwei Drittel eines Textes aus machen.
Damit kann der Angreifer den Geheimtext vom Rechner teilübersetzen lassen (die unbekannten Zeichen läßt er als Leerzeichen stehen) und kann den Text vermutlich schon verstehen.

Der hier vorgeführte Angriff auf die Permutationschiffre nimmt an, daß der Angreifer *weiß*, mit welcher Art Chiffre verschlüsselt wurde. Also, meint man, sollten Alice und Bob einfach geheim halten, mit welcher Chiffre sie arbeiten!
Aber das ist überhaupt keine gute Idee. In der Praxis wird ein relativ großer Personenkreis ein und denselben Chiffrieralgorithmus benutzen, welcher auch relativ aufwendig entworfen sein muß, um gewissen Mindestanforderungen an Geheimhaltung zu genügen.
Was man allenfalls (für eine Weile) wird geheimhalten können, ist der jeweils benutzte *Schlüssel*. Die Hoffnung, den ganzen Algorithmus auf Dauer geheimhalten zu können, ist illusorisch.

Prinzip von Kerckhoff
Die Sicherheit eines Kryptosystems darf sich nur auf die Geheimhaltung des aktuellen *Schlüssels* gründen. Der benutzte Chiffrier-*Algorithmus* sollte so gut wie eben möglich der öffentlichen Kritik unterzogen sein.
Der Chiffrieralgorithmus bleibt auf Dauer der gleiche, der aktuelle Schlüssel ist in regelmäßigen Abständen zu erneuern.

Einen Verstoß gegen das Kerkhoff'sche Prinzip erlebte man vor einiger Zeit beim Versuch der Hollywood-Filmbranche, den Verschlüsselungs-Algorithmus ihrer DVD's geheimgehalten.
Der Algorithmus wurde bald bekannt und dann umgehend gebrochen, denn er war schlecht entworfen, und er war nicht ausreichend getestet und der öffentlichen Kritik unterzogen worden.

Das Problem bei der Permutations-Chiffre war, daß feste Klar-buchstaben immer demselbem Geheimbuchstaben zugeordnet wurden.
Bei **polyalphabetischen** Chiffren wird das anders gemacht.
Die Idee ist, verschiedene monoalphabetische Chiffrierungen im Wechsel zu benutzen.
Es gibt viele Möglichkeiten zur Realisierung dieses Gedankens, vorstellen wollen wir die **Vigenere-Chiffre** (Blaise de Vigenere, 1523-1596), bei der der Wechsel durch ein Schlüsselwort gesteuert wird. Der Chiffre liegt das folgende **Vigenere-Quadrat** zu Grunde:

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Das Quadrat enthält untereinander geschrieben und zwar jeweils um eine Position verschoben die 26 möglichen Verschiebechiffren.
Angenommen, Alice will eine Nachricht an Bob schicken und die beiden haben sich über ein Schlüsselwort geeinigt, beispielsweise

Alice schreibt nun das Schlüsselwort in ständiger Wiederholung unter ihren Klartext:

Klartext:	p	o	l	y	a	l	p	h	a	b	e	t	i	s	c	h
	15	14	11	24	0	11	15	7	0	1	4	19	8	18	2	7
Schlüssel:	V	E	N	U	S	V	E	N	U	S	V	E	N	U	S	V
	21	4	13	20	18	21	4	13	20	18	21	4	13	20	18	21
Geheimtext:	K	S	Y	S	S	G	T	U	U	T	Z	X	V	M	U	C
	10	18	24	18	18	6	19	20	20	19	25	23	21	12	20	2

Zum Verschlüsseln des ersten Buchstaben p findet Alice den zugehörigen Schlüsselbuchstaben V. Sie geht damit in die Zeile V des Vigenere-Quadrats und findet in der Spalte p den Buchstaben K . Also p wird mittels V zu K.
Alice sucht dann in Zeile E den zu o gehörenden Geheimbuchstaben und findet S. Insgesamt erhält sie den oben angegebenen Geheimtext.

Beim Entschlüsseln kann Bob ganz entsprechend vorgehen: Der erste Buchstabe wurde mittels V zu K verschlüsselt. Also sucht Bob in Zeile V den Buchstaben K und findet in der ersten Zeile über K den zugehörigen Klartextbuchstaben p.

Man beachte: Wenn wir die Buchstaben mit Zahlen codieren, also

Buchstabe:	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
Code:	0	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

dann gilt

Geheimtext ≡ Klartext + Schlüssel modulo 26

Die *poly*alphabetische Vigenere-Chiffrierung benutzt *mono*alphabetische Verschiebechiffren (die Zeilen des Vigenere-Quadrats) im Wechsel. Der jedem Klartextbuchstaben zugeordnete Schlüsselbuchstabe gibt an, welche Verschiebechiffre jeweils benutzt wird.

Ein Hauptvorteil solcher polyalphabetischer Chiffren ist, daß die unterschiedlichen Buchstabenhäufigkeiten natürlicher Sprachen eingeebnet werden und dies umso wirksamer, je länger das Schlüsselwort ist. - Im ersten Praktikum soll gezeigt werden, daß die Vigenere-Chiffre dennoch, und zwar auf recht einfache Weise, gebrochen werden kann.

[CrypTool-Demo zur Vigenere-Chiffre]

Ergänzungen zur Kryptologie, Teil 1

1) Die bisher betrachteten Kryptosysteme waren *Substitutions*-Algorithmen. Es war stets so, daß sich bei den Buchstaben änderte, *was* sie waren, nicht aber, *wo* sie waren.
Bei einer schon den Griechen bekannten Chiffrierung, der *Skytale*, ist dies genau andersherum: Die Buchstaben bleiben, was sie sind, aber ihre Position ändert sich (*Transpositions*-Algorithmus).
Die Skytale funktioniert folgendermaßen: Alice wickelt einen schmalen Papierstreifen spiralförmig um einen Stab einer gewissen Dicke.
Dann schreibt sie den Klartext von links nach rechts auf den umwickelten Stab. Wenn eine Zeile voll ist, so bekommt sie eine neue Leerzeile durch Drehen des Stabes, schreibt die neue Zeile voll, dreht den Stab wieder und so weiter.
Den vom Stab wieder abgewickelten Papierstreifen schickt sie an Bob.
Der kann den Text lesen, wenn er weiß, wie dick der Stab von Alice war. - Der folgende Text wurde mit einer Skytale verschlüsselt:

ISADTPIHEHNNCSDIROOILTAIHTAEASNFEZCSWESSNISFIUKTUJSESTCRCKE!

Man rekonstruiere den benutzten Schlüssel, d.h. man bestimme den Umfang des benutzten Stabes.

2) Die folgende Transpositions-Chiffre setzt voraus, daß Alice und Bob identische Schablonen haben:

Die Schablone	Alice schreibt den Klartext in die Schablone	und füllt den Rest beliebig auf
`  *   *`	`d * a * s i`	`D V A B S I`
`* * * *   *`	`* * * * s *`	`E H E E S E`
`*     * * *`	`* t e * * *`	`Y T E H O T`
`*   * * *`	`* i * * * n`	`E I Y T S N`
`*   *     *`	`* g * e h *`	`I G A E H Y`
`* * * *`	`* * * * e i`	`D O Y U E I`
`  *   * * *`	`m * n * * *`	`M A N B B L`
`* *   * *`	`* * i * * s`	`O T I O D S`

Bob legt seine Schablone über das Kryptogramm und liest den Text.
Diese Methode hat den zusätzlichen Vorteil, daß die Restschablone mit (zufällig verteilten) Buchstaben echter Texte aufgefüllt werden kann, so daß die Häufigkeiten *stimmen* und Attacken des Angreifers wie oben beschrieben ins Leere gehen.

3) Monoalphabetische Chiffrierungen wurden in der Vorlesung durch Klartext-Geheimtext-Tabellen dargestellt:

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

Die Alternative zu einer solchen Tabelle ist die Zyklenschreibweise:

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

In der Tabelle erkennt man: a geht über in C, c geht über in I und i geht wieder über in A, womit der erste Dreierzyklus komplett ist.

Man notiere die beiden folgenden Tabellen in Zyklenschreibweise. Was fällt auf?

Klarbuchstabe: 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
Geheimbuchst.: 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

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

5) Einer Attacke des Angreifers können Alice und Bob leicht die Grundlagen entziehen: Derjenigen, die auf reinem Abzählen der Buchstabenhäufigkeit in Texten natürlicher Sprachen beruht.
Alice und Bob brauchen jeden Klartextbuchstaben nur öfter im Geheimalphabet zu repräsentieren, und zwar mit einer Häufigkeit, die dem statistischen Vorkommen des Buchstaben in der betreffenden Sprache entspricht.
Beim Verschlüsseln wählt Alice aus den Geheimrepräsentanten eines Klartextbuchstaben jedesmal zufällig einen aus. Alle Buchstaben des Geheimalphabets erscheinen dann im Geheimtext durchschnittlich gleich oft. - Eine Chiffre mit dieser Eigenschaft wird **homophon** genannt.

Beispiel

a: 10 21 52 59 71
b: 20 34
c: 28 06 80
d: 04 19 70 81 87
e: 09 18 33 38 40 42 53 54 55 60 66 75 85 86 92 93 99
f: 00 41
g: 08 12 97
h: 07 24 47 89
i: 14 39 46 50 65 76 88 94
j: 57
k: 23
l: 03 16 84
m: 11 27 49
n: 30 35 43 62 63 67 68 72 77 79
o: 02 05 82
p: 31
q: 25
r: 17 36 51 69 74 78 83
s: 15 26 45 56 61 73 96

t: 13 32 90 91 95 98
u: 01 29 58
v: 37
w: 22
x: 44
y: 48
z: 64

Der Angreifer ist aber auch gegenüber einer homophonen Chiffre nicht völlig hilflos. Alle Geheimbuchstaben sind zwar etwa gleich häufig, aber er kann weiterkommen, indem er Buchstabenpaare betrachtet.
Angenommen, er weiß bereits, daß 99 ein Repräsentant von e ist. Dann sucht er sich die Zahlen heraus, die als Vorgänger und Nachfolger von 99 etwa gleich häufig sind. Das sollten dann die Vertreter von i sein!
Nachbarn von c sind vorwiegend h und k. Also kann er die Repräsentanten der Gruppe {h,k} bekommen, wenn er einen Vertreter von c bereits hat.
Man entschlüssele das mit der obigen homophonen Chiffre verschlüsselte Kryptogramm:

23520127 6429 97845929346663 04597396 9945 5682 86886200712847 141513

6) **ALBERTI-CHIFFRE (1466)**
Bei polyalphabetischen Chiffren werden verschiedene monoalphabetische Chiffren im Wechsel benutzt. Bei der Vigenere-Chiffre hat man die 26 möglichen Verschiebechiffren des Standardalphabets zur Auswahl.
Eine Verallgemeinerung ist die Alberti-Chiffre: Sie benutzt eine feste monoalphabetische Chiffrierung des Standardalphabets und deren 26 mögliche Verschiebungen.
Die Alberti-Chiffre kann mechanisch nachgebildet werden: Auf einem von zwei konzentrischen Ringen ist das Standardalphabet notiert und auf dem anderen die monoalphabetische Chiffrierung.
Die Verschiebungen werden realisiert durch Drehung der Ringe gegeneinander.
In algebraischer Sichtweise sind die Alphabete einer Alberti-Chiffre von der Form

$$\{ \ \delta^i * P \ , \ i=0,...,25 \ \}$$

wobei P für die feste monoalphabetische Chiffrierung steht und δ^i für die vorgeschaltete Verschiebung um i Stellen.

7) **ENIGMA-CHIFFRE**
Bei dieser von deutschen Militärs im letzten Krieg benutzten Chiffrierung sind die Alphabete von der Form

$$\{ \ \delta^i * P * \delta^{-i} \ , \ i=0,...,25 \ \}$$

Also: Verschiebung, monoalphabetische Chiffrierung und nochmalige gegensinnige Verschiebung (und das ganze bis zu fünfmal iteriert). Diese Art Chiffrierung läßt sich elektromechanisch nachbilden durch *Rotoren*. Diese Rotoren enthalten an der einen Flanke 26 elektrische Eingänge, gegenüberliegend an der anderen Flanke 26 elektrische Ausgänge, und intern ist die monoalphabetische Chiffrierung mittels Verdrahtung realisiert. Eine Drehung des Rotors zwischen den elektrischen Außenkontakten realisiert die vor- und nachgeschaltete Verschiebung.