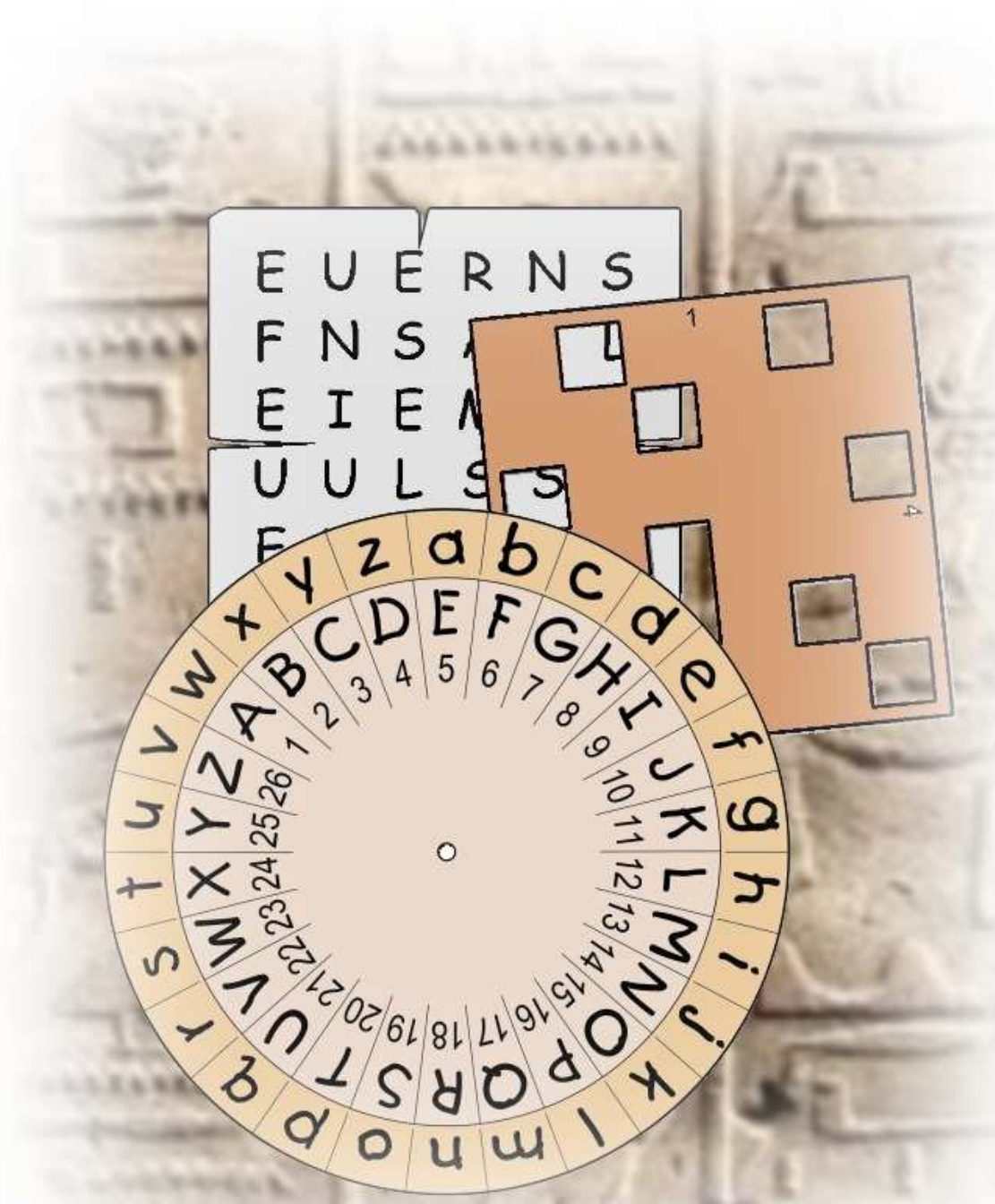


Geheimschriften

Das Geheimschreiben, Chiffrieren oder die Kryptographie genannt, ist vermutlich älter als die Kunst des Schreibens selber. Wenn wir uns Gedanken darüber machen, welche Bedeutung die Schrift für unser kulturelles und wirtschaftliches Leben hat, so muss uns Ehrfurcht vor den einfachen Buchstaben erfassen. Ob Hieroglyphen, Keilschrift chinesische Schriftzeichen oder unsere Buchstaben, sie alle wurden erfunden, um Gedanken festzuhalten oder zu vermitteln.

Zu den Vorstufen der Schrift gehören Gedächtnishilfen aller Art, z.B. der Knoten im Taschentuch. Dieser soll an eine bestimmte Sache erinnern. Wenn wir uns aber vieles merken wollen, ist das ganze Tuch voller Knoten und er nützt uns nichts mehr.

Botenstäbe sind eine weitere Art der Merkzeichen. Sie wurden bei den australischen Eingeborenen als Mitteilungsschreiben verwendet. Zu den Kerben und eingebrannten Linien merkten sich die Boten' bestimmte Sätze. Noch eine solche Gedächtnis-»Schrift«-Hilfe aus früherer Zeit ist bekannt: Anstatt eine Quittung zu geben, werden Kerben in ein Stäbchen geschnitzt. Dann wurde das Stäbchen in zwei Hälften gespalten, die eine behielt der Verkäufer, die andere bekam der Käufer. Wenn die Schuld bezahlt werden sollte, wurden die beiden Hälften zusammengelegt. Ein Betrug war unmöglich. Daher stammt wohl auch die Redensart »etwas auf dem Kerbholz haben«.

Zu allen Zeiten und bei allen Völkern hat die Chiffre eine große Rolle gespielt. Sie diente von jeher hauptsächlich diplomatischen Zwecken, dem Verbrechen (Gaunerzinken) und der Liebe. Von dem griechischen Militärschriftsteller Tacitus, der vor 2000 Jahren lebte, weiß man, dass er zwanzig verschiedene Geheimschriftmethoden erfand. Diese Zahl ist heute zu Millionen angewachsen. Fast jeder große Heerführer, Fürst oder Staatsmann (Cäsar, Napoleon, Mirabeau, Graf Gronfeld, Richelieu, usw.) hat uns eine oder mehrere Methoden überliefert. Die kryptographische Literatur stand besonders im Mittelalter als Teil der magischen Wissenschaften sehr in Blüte.

Auch heute noch wird in großem Umfang chiffriert, wobei die Privatwirtschaft ebenfalls beteiligt ist, denken wir nur an Computer, wo nur noch Lochstreifen und Lochkarten, aber keine eigentliche Schrift zu sehen waren. Grundsätzlich muss davon ausgegangen werden, dass jede Geheimschrift zu entziffern ist. Diplomatie und Behörden, Armee und Flotte benutzen heute Chiffriermaschinen. Der Verbrecher und der Liebende gebraucht Versetzungschiffren oder sympathetische Tinten.

Wir wollen nun unserem Freund etwas mitteilen, das nur er erfahren darf. Dafür haben wir eine Geheimschrift. Oder wir wollen uns etwas aufschreiben, das nicht jeder auf den ersten Blick erkennen und lesen soll. Auch dann werden wir eine Geheimschrift benutzen.

Für uns und unseren Freund heißt es zunächst:

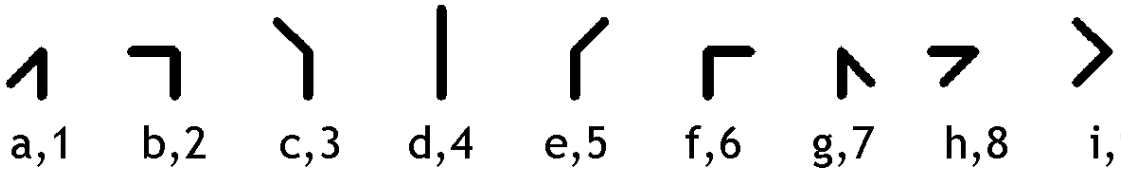
Je einfacher, desto besser. Wir sollen nicht stundenlang für eine kurze Mitteilung brauchen, andererseits soll unser Freund nicht genauso lange an der Entschlüsselung sitzen.

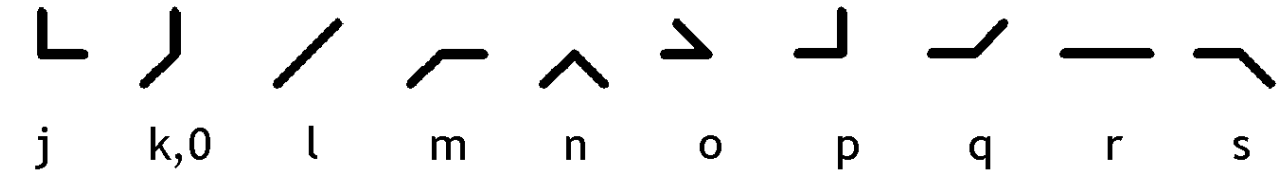
Natürliche Schriften

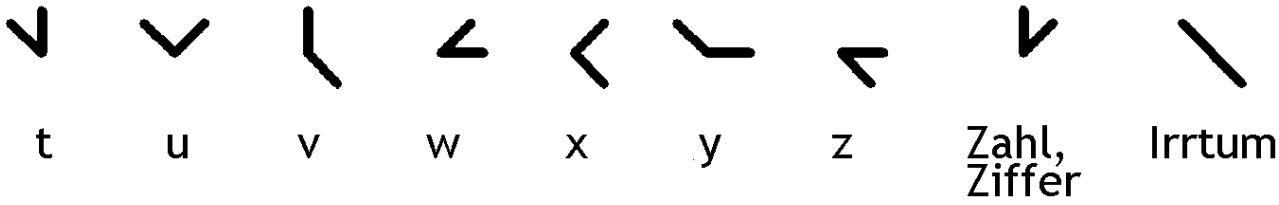
Runenalphabet

x = ks , q = kw

Winkeralphabet (Semaphorzeichen)







Einfache Schriften

Rückwärts schreiben

Meistens wird als Geheimschrift schon genügen, wenn du die Wörter jeweils rückwärts schreibst.

Beispiel: **SEMIEHEG TBIELB RUN OS EGNAL MIEHEG EIW .NAM SE RÜF HCIS TLÄHEB DNU THCIN LIEW NAM SE RÜFAD TLÄH**

Lösung: **geheimes bleibt nur so lange geheim, wie man es für sich behält, und nicht, weil man es dafür hält**

Umstellung

Eine einfache Methode: Vom Klartext trennt man jeweils fünf aufeinander folgende (oder auch drei, vier oder sechs) Buchstaben ab und schreibt diese in umgekehrter Reihenfolge.

Beispiel: **UJREDHCSGNRELRATSEINIGÄTIESHCBIBENCBALE!**

Lösung: **UJRED HCSGN RELRA TSEIL LIGÄT IESHC BIBEN CBALE**

DERJU NGSCH ARLER LIEST TÄGLI CHSEI NEBIB ELABC!

der jungscharler liest täglich seine bibel!

Zwischenbuchstaben

Setze vor den Text eine »2« . Das bedeutet: »Nur jeder zweite Buchstabe gilt!«

Beispiel: **2AABLCSDJEUFNGGHSICJHKALRMLNEERPWCIRLSLTIUCVHWDXEY MZHAEBRCRDNEJFEGSHUISJCKHLRMINSOTPUGS-RNSATCUHVFWOXLYGZEAN**

Lösung: 2A**A**B**L**C**S**D**J**E**U**F**N**G**G**H**S**I**C**J**H**K**A**L**R**M**L**N**E**E**R**P**W**C**I**R**L**S**L**T**I**U**C**V**H**W**D**-**X**E**Y**M**Z**H**A**E**B**R**C**R**D**N**E**J**F**E**G**S**H**U**I**S**J**C**K**H**L**R**M**I**N**S**O**T**P**U**G**S**R**N**S**A**T**C**U**H**-**V**F**W**O**X**L**Y**G**Z**E**A**N**

als jungscharler will ich dem herrn jesus christus nachfolgen

Buchschrift

Ein Buch ist vorher vereinbart worden. Für unsere Meldung bezeichnen wir nun Buchstaben in diesem Buch durch Angabe der Seitenzahl, Reihe und Stelle des Buchstabens in der betreffenden Reihe (im Beispiel: »Das Geheimnis des Kamins«, Jumbo-Buch von Max Hamsch).

Beispiel: **13-5-36 / 13-6-11 /13-6-16/13-7-14/13-8-5/ 13-8-24**

Lösung: **gefahr**

Verschiebungsschrift (Caesar-Verschlüsselung)

Wir schreiben die Buchstaben des Alphabets zweimal hintereinander auf zwei Papierstreifen, legen sie untereinander und verschieben den unteren Streifen um eine abgemachte Anzahl von Buchstaben.

Verschieben wir z.B. um vier Buchstaben nach vorn:

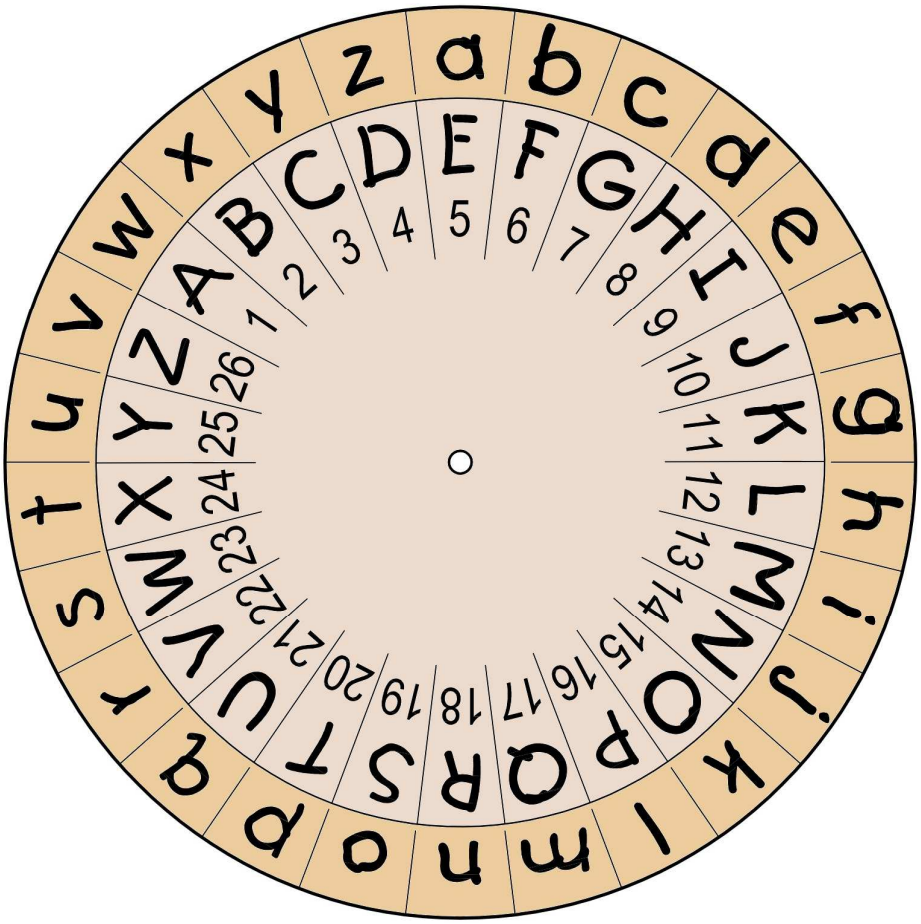
```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z     (= Buchstaben Klartext)
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D     (= Buchstaben Geheimtext)
```

Beispiel: **HIV NYRKWGLEVPIV MWX OEQIVEHWGLEJXPMGL**

Lösung: **der jungscharler ist kameradschaftlich**

Caesar-Scheibe oder »Alberti-Maschine«

Zur Vereinfachung der Chiffrierung hatte bereits 1470 Leon Battista Alberti (1404 bis 1472) eine »Maschine« erfunden, die das Verschlüsseln mechanisiert. Diese »Chiffriermaschine« sieht wie folgt aus:



Die »Maschine« hat insgesamt zwei Scheiben. Die innere Scheibe ist gegenüber der äußeren verdrehbar, so dass man die gewünschte Verschiebechiffre einstellen kann.

Außen suchen wir den Buchstaben im Klartext und innen lesen wir die Buchstaben bzw. Zeichen des Geheimtextes ab.

Bei einer weiteren Art der Caesar-Verschlüsselung verwenden wir ein Schlüsselwort. Wir schreiben zunächst das Schlüsselwort unter das Klartextalphabet und danach die restlichen Buchstaben in ihrer normalen Reihenfolge.

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

Beispiel: **NF UPO CNFUPFDSPICP NQR PQ QEIJPF**

Lösung: **in der lindenmuehle ist es schoen**

Zahlenschrift

Wenn wir die Buchstaben einfach durchnummerieren, können wir mit Zahlen unsere Nachricht schreiben:

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	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

Beispiel: **1,14,11,5,18,11,18,5,21,26**

Lösung: **ankerkreuz**

Buchstaben rückwärts durchnummeriert:

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
26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Buchstaben mit ungeraden / geraden Zahlen durchnummeriert:

A	B	C	D	E	F	G	H	I	J	K	L
1	3	5	7	9	11	13	15	17	19	21	23

A	B	C	D	E	F	G	H	I	J	K	L
2	4	6	8	10	12	14	16	18	20	22	24

Buchstaben mit teils mehrfachen Zahlen:

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
33	5	6	8	10	12	14	16	18	19	22	23	26	28	30	32	34	36	38	40	43	44	45	48	51	52
15			43	21			47	7					27				35	1	13	23					
				17									4				20	9	37						
				49									11												
				3																					

Für häufiger auftretende Buchstaben verwenden wir hier verschiedene Zahlen.

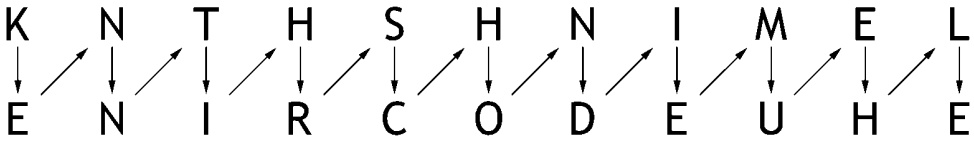
Jetzt wird es schwieriger, den Text durch Häufigkeitsanalyse zu entschlüsseln.

Beispiel: **33,28,22,21,35,22,36,10,43,52**

Lösung: **ankerkreuz**

Gartenzaun-Chiffre

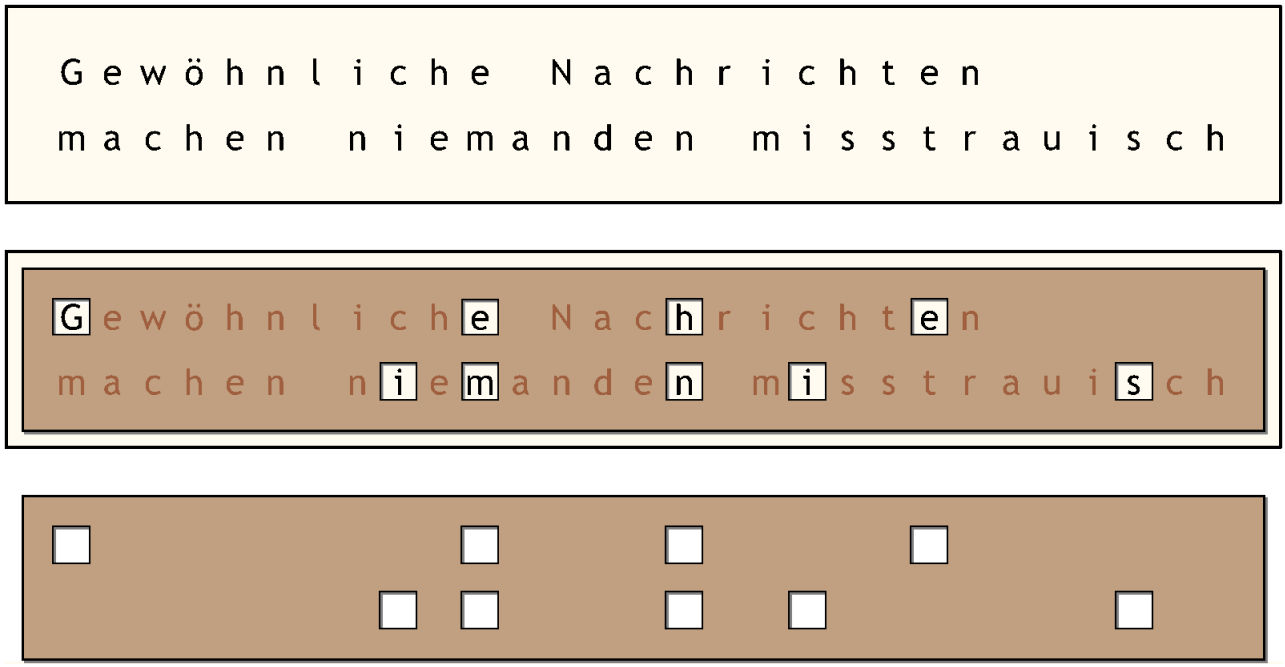
Hier schreiben wir die Meldung im Zickzack in zwei Reihen untereinander. Anschließend schreiben wir die erste Zeile auf und dahinter die zweite Zeile.



Beispiel: **KNTHSHNIMELENIRCODEUHE**

Lösung: **kennt ihr schon die muehle**

Cardano-Verschlüsselung



Mit der Cardano-Verschlüsselung verstecken wir die eigentliche Nachricht in einer harmlosen Nachricht ohne dass jemand erkennen kann, dass es eine Geheimschrift ist. Erfinder war der italienische Arzt, Philosoph und Mathematiker Gerolamo Cardano (1501 bis 1576).

Das Prinzip ist sehr einfach. Wir benutzen eine Schablone, die aus rechteckigen Öffnungen besteht, die ihrerseits den geheimen Text sichtbar machen. Die Schablone legen wir auf das Papier und schreiben die geheime Nachricht durch die offenen Felder der Schablone. Danach entfernen wir die Schablone und füllen den Rest mit Zeichen auf, so dass ein sinnvoller Text gebildet wird und harmlos erscheint.

Zur Entschlüsselung der Nachricht braucht der Empfänger die gleiche Schablone.

Lösung: **geheimnis**

Systemschriften

Quadratschrift

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

Zunächst erstellen wir ein Polybios-Quadrat. Die 25 Buchstaben des Alphabets (J fällt weg) schreiben wir in ein Quadrat. An den oberen Rand schreiben wir die Zahlen 1-5 und an den linken Rand die Zahlen 6-0.

Wir wenden nun den Schlüssel so an, dass wir für jeden Buchstaben zwei Zahlen setzen. Wir suchen den betreffenden Buchstaben auf und verfolgen dann die Reihe nach links und nach oben bis zu den Zahlen. Die am linken wir zuerst, daneben die Zahl des oberen Randes.

Beispiel: **64950274929594726573657482926194**

Lösung: **64 95 02 74 92 93 94 72 65 73 65 74 82 92 61 94**

du wirst geheimrat

Abwandlung

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

Bei dieser Abwandlung schreiben wir an Stelle der Zahlen jeweils ein Schlüsselwort. In das Quadrat schreiben wir zunächst ein (möglichst langes) Kennwort, in dem jeder Buchstabe nur einmal vorkommen darf. Die restlichen Buchstaben tragen alphabetischer Reihenfolge nach.

Beispiel: **KUALLIALKKUKALLSULUSKSLKLLLAAAUS**

Lösung: **KU AL LI AL KK UK AL LS UL US KS LK LL LA AA US**

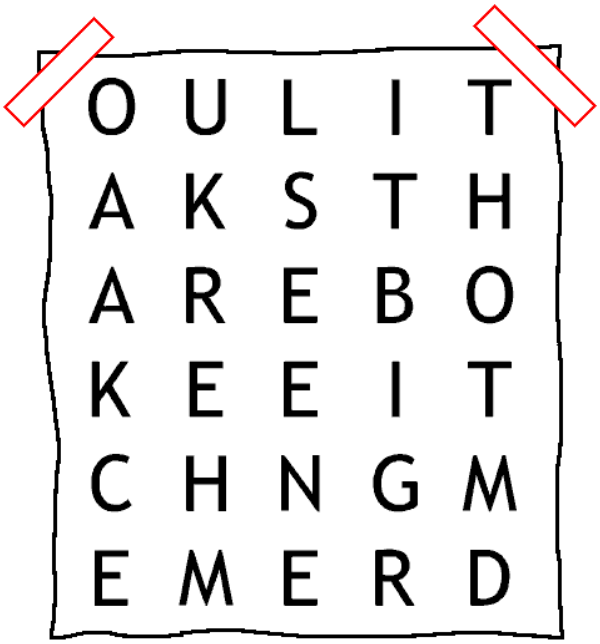
geheime botschaft

Pflügen

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

Wir zeichnen ein Gitter mit 5 x 5 Kästchen. Dahinein schreiben wir nun den Klartext unserer Nachricht. Wir setzen jeden Buchstaben in ein Kästchen und beginnen jede Zeile wieder von links. Falls am Ende noch Kästchen frei sind, füllen wir sie mit beliebigen Buchstaben und Ziffern auf. Das sind die »Faulen« – sie haben mit deiner Nachricht nichts zu tun und führen nur andere in die Irre.

Nun »pflügen« wir die Buchstaben im Gitter um, so wieder Bauer sein Feld: Wir beginnen die Linie des Pfluges unten rechts in der Ecke und pflügen erst nach oben, dann nach unten, wieder nach oben und so weiter...



Die Buchstaben der »gepflügten« Spalten tragen wir in Richtung der »Furche« in die Zeilen eines neuen Kästchengitters ein und zwar von rechts nach links.

Die »umgepflügten« durcheinander gepurzelten Buchstaben können wieder entschlüsselt werden, indem sie zeilenweise abgelesen werden und in die Spalten eines Gitters geschrieben werden, wieder auf der Linie des Pfluges! Anschließend kann man den Text von oben links angefangen wieder lesen!

Gitter-Code

Dies ist der Schlüssel dazu:

1 ABC	2 DEF	3 GHI
4 JKL	5 MNO	6 PQR
7 STU	8 VWX	9 YZE

Das Alphabet ist in 9 Gruppen eingeteilt. Diese Gruppen nummerieren wir fortlaufend, und zwar von links nach rechts, oben links beginnend:

ABC = 1, GHI = 3, VWX = 8, usw.

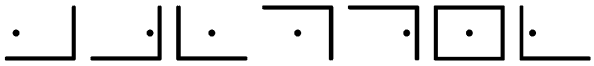
In jeder Gruppe werden die Buchstaben von 1 -3 nummeriert. Auf diese Weise lässt sich jeder Buchstabe des Alphabets durch zwei Zahlen bestimmen. Da im Feld 9 noch Platz für einen Buchstaben leer bleibt, füllen wir ihn mit dem E, das ja im deutschen Text am meisten vor-kommt. (Abwechslungsweise chiffrieren wir E mit 22 und 93, was Dechiffrierungsversuche Unbefugter erschwert. Der Buchstabe M z.B. ist in der Gruppe 5 die Nummer 1. 51 bedeutet also M.

Beispiel: **42/53/51/51,92/73/63,21/33/13/42/22/52,**
12/73/13/32/93

Lösung: **komm zur dicken buche**

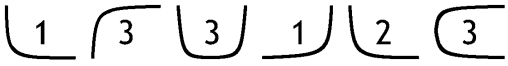
Variante

Statt die Gruppe mit einer Zahl zu bezeichnen, kann man sie darstellen, indem man die Zwischenlinien angibt. In diese Linien setzt man dort einen Punkt, wo der Buchstabe steht. Siehe Beispiel a).

Beispiel: 

Lösung: **achtung**

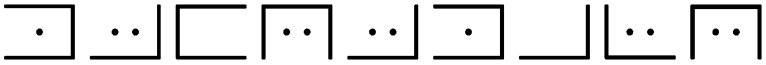
Oder man rundet diese Zwischenlinien ab, was sehr verwirrend aussieht, und gibt darin den Buchstaben in Zahlen von 1-3 an. Siehe Beispiel b).

Beispiel: 

Lösung: **gefahr**

Abwandlung 1

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

Beispiel: 

Lösung: `max hamsch`

Abwandlung 2

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

	W	
Z		X
	Y	

Beispiel: 

Lösung: `lindenmuehle`

Skytale

Ein sehr alte Verschlüsselungsmethode stellt »die Skytale von Sparta« dar. »Die Skytale von Sparta« wurde von der Regierung von Sparta vor etwa 2500 Jahren ververwendet, um die geheimen Nachrichten im militärischen Bereich zu übermitteln. Um eine Nachricht zu verfassen, wickelte der Absender ein Pergamentband oder einen Streifen Leder wendelförmig um die Skytale, schrieb die Botschaft längs des Stabs auf das Band und wickelte es dann ab. Das Band ohne den Stab wird dem Empfänger überbracht. Fällt das Band in die falschen Hände, so kann die Nachricht nicht gelesen werden, da die Buchstaben scheinbar willkürlich auf dem Band angeordnet sind. Der richtige Empfänger des Bandes konnte die Botschaft mit einer identischen Skytale (einem Stab mit dem gleichen Durchmesser) lesen. Der Durchmesser des Stabes ist somit der geheime Schlüssel bei diesem Verschlüsselungsverfahren.

Schlüsselwort

2	3	4	5	1
J	O	S	U	A
D	E	R	J	U
N	G	S	C	H
A	R	L	E	R
H	Ö	R	T	T
Ä	G	L	I	C
H	A	U	F	G
O	T	T	E	S
W	O	R	T	A

Zu dieser Geheimschrift vereinbaren wir vorher ein Schlüsselwort. Die Buchstaben des Schlüsselwortes bezeichnen wir mit Zahlen nach der Reihenfolge im Alphabet und schreiben diese darüber.

Wir verschlüsseln nun einen der Zielsätze für Jungscharler: »Der Jungscharler hört täglich auf Gottes Wort« mit dem Schlüsselwort JOSUA. Wir schreiben den Satz jetzt von links nach rechts immer in Fünfergruppen unter das Schlüsselwort. Die letzte Reihe füllen wir mit den ersten Buchstaben des Alphabets auf.

Nun schreiben wir die Spalten von oben nach unten in der Reihenfolge der darüber stehenden Zahlen:

UHRTCGSA DNAHÄHOW EGRÖGATO RSLRLUTR JCETIFET

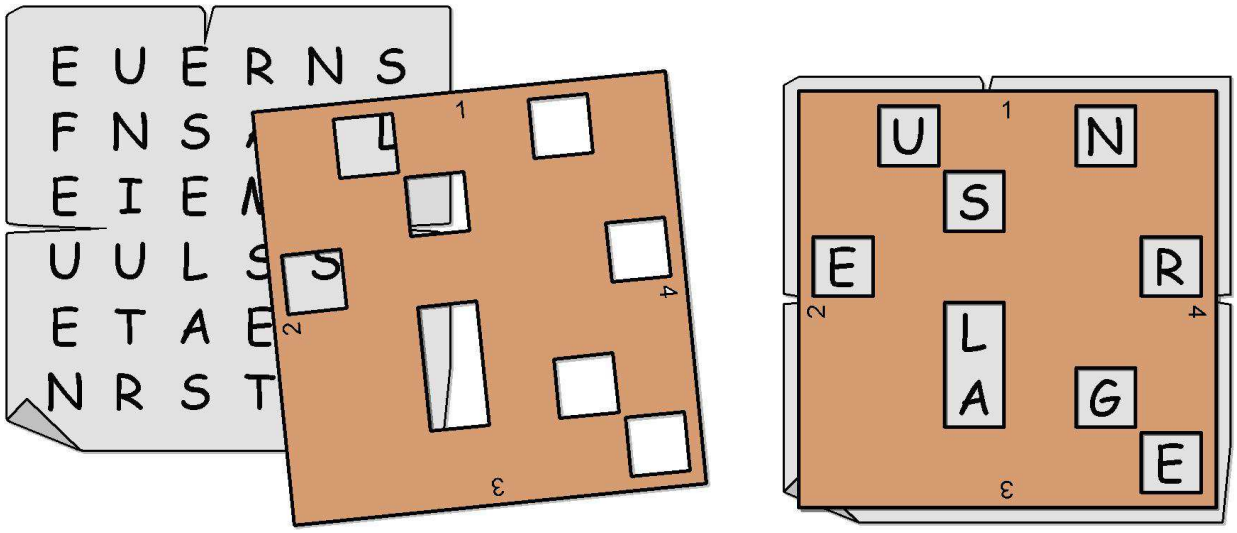
oder auch

UHR TCGSADN AHÄ HOWE GRÖGATOR SLRLUT RJCE TIFET

Wollen wir nun diese Geheimschrift entschlüsseln, dann zählen wir zuerst die Anzahl Buchstaben und teilen diese Zahl durch die Anzahl Buchstaben des Schlüsselwortes. Jetzt schreiben wir das nummerierte Schlüsselwort und darunter die entsprechenden Buchstabengruppen.

UHR TCGSA,DN AHÄ HOW,E GRÖGATO,R SLRLUT R,JCE TIFET

Schablonenschrift (Fleißner-Schablone)



Mit Hilfe einer (Fleißner-)Schablone lässt sich eine Geheimschrift herstellen, die wir sehr rasch schreiben und lesen können. Die erforderliche Schablone schneiden wir uns gemäß der Abbildung aus Karton, Blech oder Plastik: Wir legen sie zuerst so auf

den Briefbogen, dass sich die Zahl 1 oben befindet. Dann schreiben wir den Text in die Öffnungen und zwar immer nur ein Buchstabe in ein Loch. Sind alle Öffnungen mit Buchstaben angefüllt, drehen wir die Schablone so, dass die mit 2 bezeichnete Seite nach oben kommt. Nun können wir die durch das Drehen freigewordenen Öffnungen beschreiben. Ähnlich machen wir es mit den Zahlen 3 und 4. Die am Schluss der Mitteilung verbleibenden Lücken des Schriftbildes füllen wir mit Faulen aus, was dem Uneingeweihten die Entzifferung erschwert.

Beispiel: **unser lager liegt unten am ufer des flusses**

Vigenère-Schlüssel

Die Vigenère Verschlüsselung ist ähnlich aufgebaut, wie die Caesar Verschlüsselung mit dem Unterschied, das statt nur einem Alphabet – mehrere Alphabete verwendet werden.

Der Vignère Code wurde im 16. Jahrhundert von Blaise de Vigenère erfunden. Damals galt diese Verschlüsselung als sicherer Chiffrieralgorithmus – im Zeitalter der Technik ist das natürlich nicht mehr der Fall.

Wie funktioniert die Verschlüsselung?

Man denkt sich zunächst ein Codewort aus, z.B. **MULTI**. Das Wort **MULTI** bestimmt nun, wie viele und vor allem welche Alphabete verwendet werden. Grundlage hierfür bildet das sog. Vigenère-Quadrat: (siehe rechte Seite)

In unserem Beispiel wollen wir das Wort **geocaching** in Geheimtext schreiben. Die Klartextbuchstaben entnimmt man der ersten Zeile. In unserem Fall ist es das **g** von **geocaching**. Wir suchen uns in der ersten Zeile das **G** und bewegen uns in dieser Spalte soweit runter, bis in der linken Spalte das **M** von unserem Codewort **MULTI** auftaucht. An der Stelle, wo sich dann die beiden grünen Balken überschneiden, befindet sich der verschlüsselte Buchstabe. In unserem Fall das **S**.

Am einfachsten ist es, wenn man sich eine kleine Tabelle baut. Oben das Codewort, darunter den Klartext und in der letzten Zeile dann den erstellten Geheimtext.

Codewort	M	U	L	T	I	M	U	L	T	I
Klartext	g	e	o	c	a	c	h	i	n	g
Geheimtext	S	Y	Z	V	I	O	B	T	G	O

Problem bei der Vignère Entschlüsselung

Das Schlüsselwort muss dem Empfänger bekannt sein – sonst wird es ziemlich mühsam. Je länger das Schlüsselwort, umso schwerer lässt sich die geheime Botschaft entschlüsseln.

Wie entschlüssele ich die Geheimbotschaft, wenn das Codewort bekannt ist?

In diesem Fall ist es ganz einfach. Ich nehme wieder meine Tabelle zur Hilfe und notiere zunächst in der ersten Zeile die geheime Botschaft. In Zeile 2 wird das Codewort eingesetzt, so oft wie erforderlich (entspricht: Textlänge des Geheimtextes). In der dritten und damit letzten Zeile übertrage ich dann den Klartext.

Ich beginne nun mit dem ersten Buchstaben unseres Codewortes **MULTI** **(M)** und bewege mich in dieser Zeile nach rechts bis ich auf das **S** von unserem Geheimtext stoße. Nun schaue ich in der ersten Zeile nach, welchem Klartextbuchstaben das **S** entspricht.

Geheimtext	S	Y	Z	V	I	O	B	T	G	O
Codewort	M	U	L	T	I	M	U	L	T	I
Klartext	g	e	o	c	a	c	h	i	n	g

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Unsichtbare Schriften

Wir können als Geheimschrift auch völlig unsichtbare Tinten benutzen, z.B. Milch, Zwiebelsaft, Zitronensaft, Salz- oder Zuckerlösung. Nach dem Eintrocknen wird diese »Tinte« unsichtbar. Durch vorsichtiges Erwärmen können wir sie wieder sichtbar machen. Wir halten das Papier über eine Kerze, dann wird die »Tinte« bräunlich.

Es wäre nun töricht, wollten wir unsere Nachricht auf einem leeren Zettel überbringen. Ein Vorsichtiger oder Eingeweihter, der uns kennt, würde sofort durchschauen, was hier gemeint ist. Wir nehmen lieber ein einseitig beschriebenes Blatt mit einer ganz belanglosen Mitteilung und schreiben zwischen die Zeilen mit unserer Geheimtinte den gültigen Text!

Soll der Geheimtext mehrfach gebraucht werden, müssen wir eine andere Tinte wählen. Denn unsere erwärmte Tinte bleibt braun! Wenn wir ein Gramm Cobalt-II-Chlorid in zehn Gramm Wasser (= 10 ccm) lösen, erhalten wir eine Tinte, die nach Erwärmen blau erscheint und nach dem Abkühlen wieder verschwindet.

Das Schreiben mit Geheimtinten ist nicht so einfach, wie man annehmen könnte. Mit einigem Geschick lässt sich nämlich eine Schrift in unsichtbarer Tinte doch entziffern. Besonders wenn ein Greenhorn die Meldung mit einer Spitzfeder schrieb. Eine solche raubt nämlich das Papier bei jedem Strich leicht auf. Und der Schriftzug lässt sich von bloßem Auge, sicher aber mit einer Lupe, erkennen.

Vorteilhafter ist es also, mit einer breiten Feder, z.B. mit einer breiten. Redisfeder, zu schreiben. Aber auch dies hat einen Haken. Die Schreibflüssigkeit weist auf dem Papier einen leichten Glanz auf. Und wenn der Schreibstrich zu breit ist dann ist die Schrift als Glanzschrift ganz gut lesbar, wenn man das Blatt so hält, dass das Licht schräg darauf fällt.

Das Geeignetste ist ein weiches Holzstäbchen, das man sich zuspitzt und als Feder verwendet.

Als Schreibfläche ist helles Papier zu nehmen, besonders bei Verwendung von Geheimtinten nach Naturrezepten, Das Papier darf nicht zu dünn sein, denn dünnes Papier zieht sich dort, wo es befeuchtet worden ist, stets leicht zusammen beim Eintrocknen. Das kann das Vorliegen einer Geheimschrift verraten, ja sogar die Schrift leserlich machen.

Dechiffrieren

Besonders spannend ist die Aufgabe, eine Geheimschrift zu dechiffrieren, ohne dass man den betreffenden Code kennt. Sofern der Text einfach chiffriert ist, so gibt uns die Häufigkeit der verschiedenen Buchstaben einen wichtigen Anhaltspunkt.

Ist die Meldung jedoch mehrfach chiffriert, so ist eine Dechiffrierung ohne Code sozusagen unmöglich.

In der deutschen Sprache ist die Häufigkeit der einzelnen Buchstaben durchschnittlich folgendermaßen:

1. Gruppe: E 17,4 %, N 9,8 %, I 7,6 %, S 7,3 %, R 7% (= 49 %)

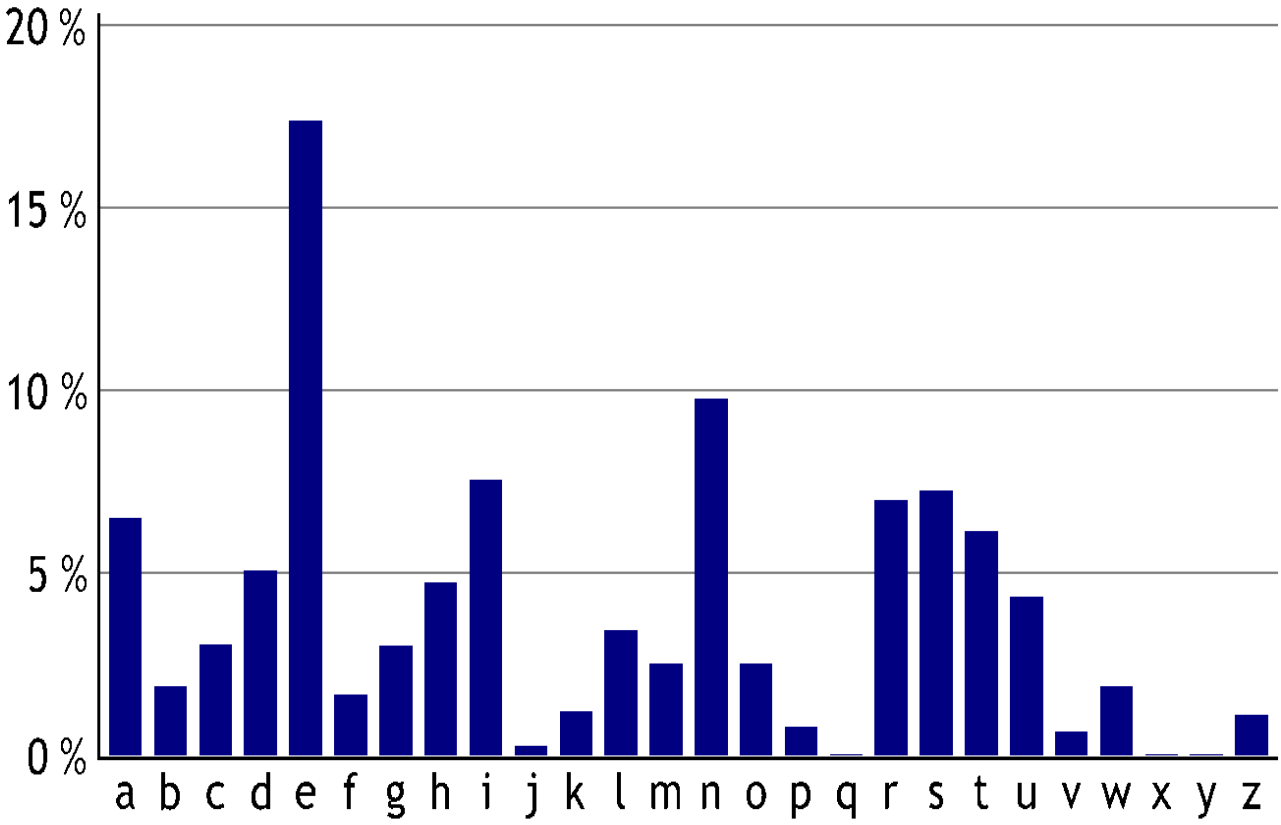
In einer deutschsprachigen Meldung werden also die Hälfte aller Zeichen auf diese 5 Buchstaben entfallen.

2. Gruppe: A, T, D, H, H, U, L, C, G alle 3 – 6,5 %

3. Gruppe: M, O, B, W, F alle 1,6 – 2,5 %

4. Gruppe: K, Z, P, V, J alle 0,3 – 1,2 %

5. Gruppe: X, Y, Q kommen praktisch nicht vor (ausgenommen Fremdwörter).



Häufigkeitsverteilung der Buchstaben des deutschen Alphabets.
(Nach A. Beutelspacher, *Kryptologie*, Braunschweig 1993.)

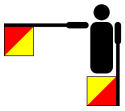
Beachte, dass ein C zu 80 % in Verbindung mit einem H steht und etwa zu 20 % mit einem K. Beginne mit den kürzesten Wörtern (sofern man diese überhaupt feststellen kann). Bei zweibuchstabigen Wörtern, die mit E beginnen, ist der zweite Buchstabe fast immer ein R oder ein S.

Indem wir die Häufigkeit der verschiedenen Zeichen feststellen, können wir einige kurze Wörter entziffern. Da die Worte meistens einen sinngemäßen Zusammenhang haben, sollte uns mit einiger Geduld auch bei längeren Wörtern die Dechiffrierung gelingen.

Anhang

Winkeralphabet

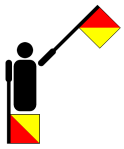
Alpha, 1



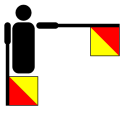
Bravo, 2

Charlie, 3

Delta, 4



Echo, 5

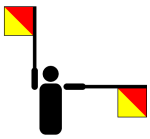


Foxtrott, 6

Golf, 7

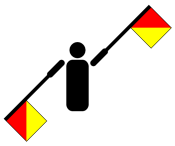
Hotel, 8

India, 9

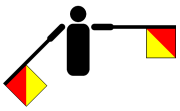


Juliet, Buchstaben folgen

Kilo, 0



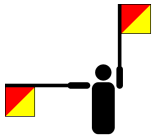
Lima



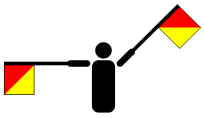
Mike

November

Oscar

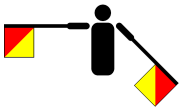


Papa

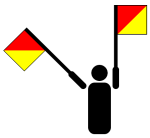


Quebec

Romeo

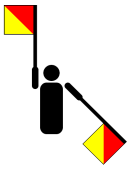


Sierra



Tango

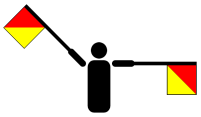
Uniform



Victor

Whiskey

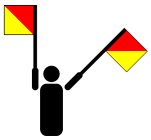
X-ray



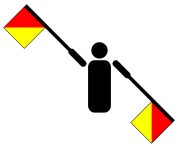
Yankee

Zulu

Unter-brechung



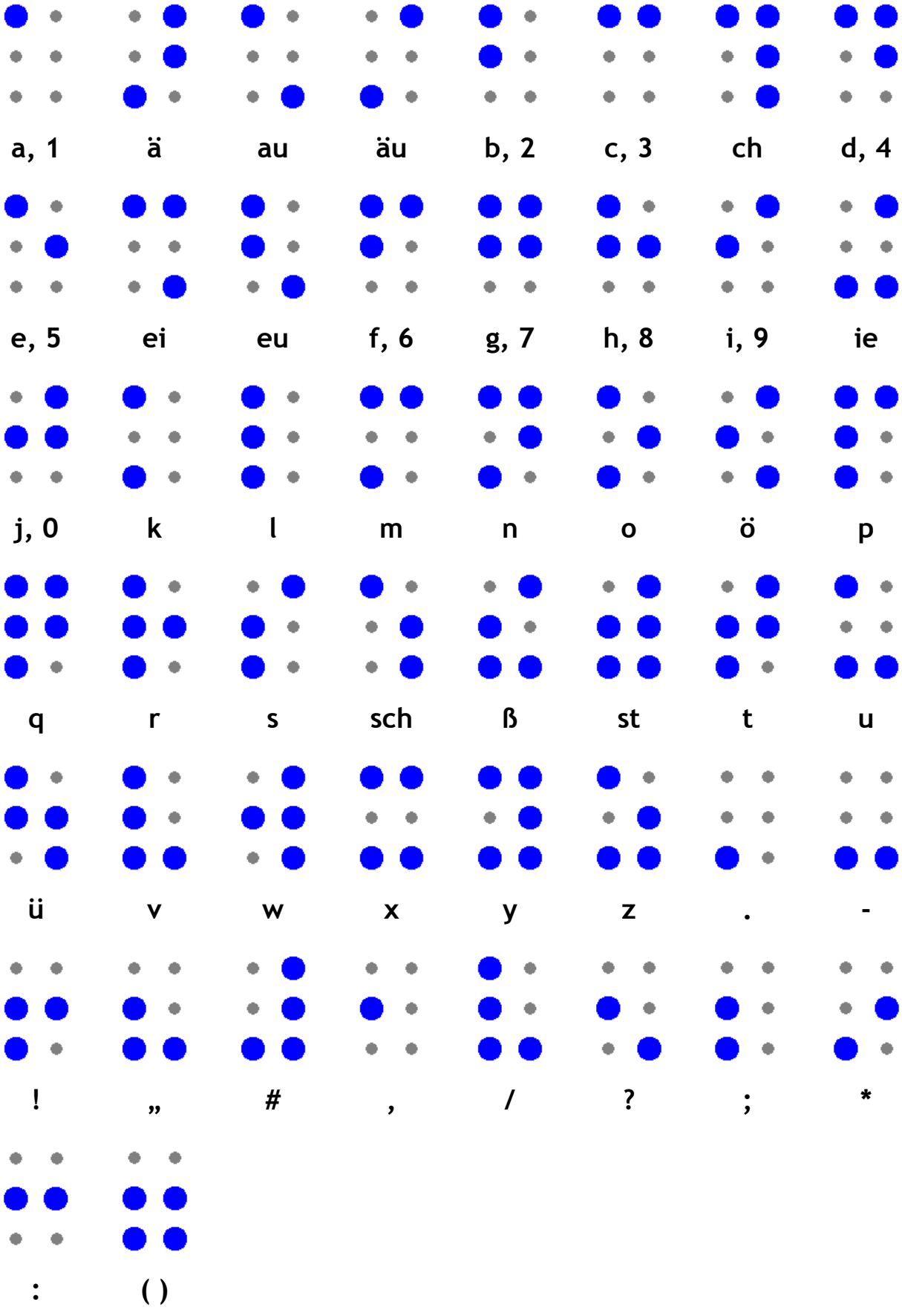
Zahlen folgen



Annullieren

Fehler

Blindenschrift



Morsealphabet

a		A-tom	w		Wind-mo-tor
b		Boh-nen-sup-pe	x		Xox Keks-kar-ton
c		Co-ca-Co-la	y		Yo-ri-no-ko
d		Dro-ge-rie	z		Zoll-vor-ste-her
e		Eis	ä		Ä-sop ist tot
f		Fens-ter-bo-gen	ö		Ö-ko-lo-gie
g		Groß-mo-gul	ü		Ü-berm Hof-tor
h		Hun-de-hüt-te	ch		Chro-no-lo-gos
i		In-sel	.		(AAA)
j		Ja-wohl O-dol	,		(MIM)
k		Klos-ter-hof	?		(IMI)
l		Li-mo-na-de	:		(OS)
m		Mo-tor	-		(BA)
n		Nor-den	(		(KN)
o		Oh Ot-to	)		(KK)
p		Per Mo-tor-rad	/		(WG)
q		Quo-ko-ri-ko	„“		(RR)
r		Re-vol-ver	=		
s		Sa-la-mi	+		
t		Ton	´		
u		U-ni-form	_		
v		Ven-ti-la-tor	@		

1		6	
2		7	
3		8	
4		9	
5		0	

Flaggenalphabet


Alpha

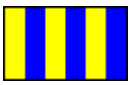

Bravo


Charlie


Delta


Echo

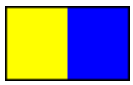

Foxtrott


Golf


Hotel


India


Juliett


Kilo


Lima


Mike


November

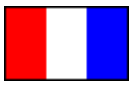

Oscar


Papa


Quebec

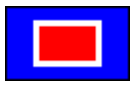

Romeo


Sierra


Tango


Uniform


Victor


Whiskey

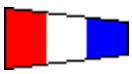

X-Ray


Yankee


Zulu


1


2


3


4


5


6


7


8


9


0

Die Entschlüsselung eines Geheimtextes

(aus Simon Singh »Geheime Botschaften«)

PR ISRSQ YSPUD SYOCREBS GPS NFRZB GSY NCYBVEYCWDPS SPRS ZVOUDS HVOONVQQSRDSPB, GCZZ GPS NCYBS SPRSY SPRMPESR WYVHPRM GSR YCFQ SPRSY ECRMSR ZBCGB SPRRCDQ FRG GPS NCYBS GSZ YSPUDZ GSR SPRSY WYVHPRM. QPB GSY MSPB ASTYPSGPEBSR GPSZS FSASYQCSZZPE EYVZZSR NCYBSR RPUDB OCSRESY, FRG QCR SYZBSOOBS SPRS NCYBS GSZ YSPUDZ, GPS ESRCF GPS EYVSZZS GSZ YSPUDZ DCBBS.

AVYESZ, HVR GSY ZBYSRES GSY JPZZSRZUDCTB

Stell dir vor, wir hätten diesen verschlüsselten Text abgefangen und müssten ihn dechiffrieren. Wir wissen, dass es sich um einen deutschen Text handelt, der mittels monoalphabetischer Substitution verschlüsselt wurde, doch vom Schlüssel wissen wir nichts. Alle möglichen Schlüssel durchzuprobieren ist praktisch unmöglich, also müssen wir die Häufigkeitsanalyse einsetzen. Ich gebe im Folgenden eine schrittweise Anleitung zur Entschlüsselung dieses Geheimtextes.

Die erste Reaktion jedes Kryptoanalytikers wäre, die Häufigkeit jedes Buchstabens festzustellen. Dann ergibt sich diese Tabelle.

Buchstabe	Häufigkeit	in %	Buchstabe	Häufigkeit	in %
A	3	0,9	N	7	2,1
B	20	6,1	O	7	2,1
C	18	5,5	P	30	9,1
D	11	3,3	Q	8	2,4
E	6	3,6	R	32	9,7
F	12	1,8	S	67	20,4
G	20	6,1	T	2	0,6
H	4	1,2	U	7	2,1
I	1	0,3	V	10	3,1
J	1	0,3	W	3	0,9
K	0	0,0	X	0	0,0
L	0	0,0	Y	29	8,8
M	5	1,5	Z	24	7,3

Häufigkeitsanalyse der verschlüsselten Botschaft (gerundete Prozentwerte)

Wie erwartet, kommen die Buchstaben unterschiedlich oft vor. Die Frage ist nur, ob wir aufgrund dieser Häufigkeiten wirklich ausfindig machen können, wofür zumindest einige dieser Buchstaben stehen? Es wäre naiv zu glauben, wir könnten alle Buchstaben auf mechanische Weise identifizieren und etwa sagen, der achthäufigste Buchstabe im Geheimtext, E, stehe für den achthäufigsten Buchstaben im Deutschen, nämlich d. Eine sture Anwendung der Häufigkeitsanalyse würde zu Kauderwelsch führen.

Wir können jedoch beginnen, indem wir uns den fünf häufigsten Buchstaben zuwenden, nämlich **S, R, P, Y** und **Z**. Wir können mit guten Gründen davon ausgehen, dass der bei

weitem häufigste Buchstabe, **S**, für den mit Abstand häufigsten Klartextbuchstaben im Deutschen, nämlich **e** steht. Bei den folgenden vier Buchstaben können wir zwar annehmen, dass es sich um die zweit- bis fünfthäufigsten Buchstaben handelt, doch nicht unbedingt in der richtigen Reihenfolge. Mit anderen Worten, wir können nicht sicher sein, dass **R = n, P = i, Y = s und Z = r**.

Wir können jedoch die Annahme wagen, dass es sich um die nach **e** häufigsten Buchstaben im deutschen Alphabet handelt, also:

R = n, s oder r, P = n, s oder r, Y = n, s oder r, Z = n, i, s oder r.

Um auf einigermaßen sicherem Grund weiterzugehen, müssen wir die Häufigkeitsanalyse ein wenig verfeinern. Anstatt einfach von der Häufigkeit dieser vier Geheimbuchstaben auf die Klartextbuchstaben zu schließen, suchen wir nach den im Deutschen häufigsten sogenannten *Bigrammen*, Zweierkombinationen von Buchstaben. Wir nehmen den mutmaßlichen Geheimtextbuchstaben für e, also S, und fragen, wie oft er zusammen mit den oben genannten zweit- bis fünfthäufigsten Geheimbuchstaben auftritt. Dann ergibt sich folgende Häufung von Bigrammen:

Bigramme	RS / SR	PS / SP	YS / SY	ZS / SZ
Häufigkeit	7 / 13	8 / 13	5 / 11	4 / 7

Zu vermuten ist, dass die drei häufigsten Bigramme, nämlich **SR, SP** und **SY**, den häufigsten Bigrammen mit **e** im Deutschen, **er**, **en** und **ei** entsprechen. Damit wäre unsere Annahme abgesichert. Von den beiden weniger häufigen Bigrammen, ZS und SZ, können wir annehmen, dass es sich um **se** und **es** handelt, und sie zunächst beiseitelassen.

Wir gehen nun einen Schritt weiter und versuchen, n und i ausfindig zu machen, indem wir nach dem im Deutschen häufigsten Trigramm, nämlich ein suchen. Hier ist das Ergebnis eindeutig: **SPR** kommt siebenmal vor, **SRP**, **SPY**, **SYP**, **SRY** und **SYR** überhaupt nicht. Wir entschlüsseln also **P = i** und **R= n**. Zusammen mit **S = e** haben wir nun mit einiger Sicherheit drei Buchstaben dingfest gemacht. Wie finden wir nun heraus, ob die verbleibenden häufigen Buchstaben **Y** und **Z** für **r** und **s** oder für **s** und **r** stehen? Am besten, wir gehen einen Umweg und machen zunächst den Buchstaben **d** ausfindig. Da in der Kryptoanalyse alle Mittel erlaubt sind, nutzen wir den Umstand aus, dass im Geheimtext die Wortzwischenräume beibehalten wurden. Das häufigste Wort im Deutschen ist **die**, und da wir **PS** als **ie** identifiziert haben, sehen wir fast auf den ersten Blick, dass es sich bei **G** um **d** handeln muss, denn **GPS** kommt im Geheimtext allein fünfmal als Einzelwort vor.

Zurück zur Unterscheidung von **r** und **s**. Das zweithäufigste Wort im Deutschen ist **der,** es kommt jedenfalls nach der Statistik sehr viel öfter vor als **des**. Wir überprüfen die in Frage kommenden Kombinationen **GSY** und **GSZ** und stellen fest, dass **GSY** viermal auftaucht, **GSZ** jedoch immerhin dreimal. Festigen können wir unsere Vermutung, dass **Y = r** und **Z = s**, indem wir uns noch einmal die Häufigkeit anschauen, mit der diese Buchstaben zusammen mit **S** auftreten. **SY**, das mutmaßliche **er**, kommt elfmal vor, **SZ**, das mutmaßliche **es,** siebenmal. Da er das häufigste Bigramm im Deutschen ist, können wir nun mit guten Gründen sagen, dass **Y = r** und **Z = s**.

Wir haben nun mit einiger Sicherheit fünf Buchstaben identifiziert und können die entsprechenden Geheimbuchstaben durch die Klarbuchstaben ersetzen:

> in IeneQ reiUD erOCnEBe die NFnsB der NCrBVErCWDie eine sVOUDe HVOONVQQenDeiB, dCss die NCrBe einer einMiEen WrVHinM den rCFQ einer ECnMen sBCdB einnCDQ Fnd die NCrBe des reiUDs den einer WrVHinM. QiB der MeiB AeTriediEBen diese FeAerQCessiE ErVssen NCrBen niUDB OCenEer, Fnd QCn ersBeOOBe eine NCrBe des reiUDs, die EenCF die ErVesse des reiUDs DCBBe.
>
> AVrEes, HVn der sBrenEe der JissensUDCTB

Dieser Schritt hilft uns, einige der anderen Buchstaben einfach zu erraten. Das Wort **reiUD** etwa wird, da **e** und **n** für die letzten beiden Buchstaben ausgeschlossen sind, das Klarwort **Reich** ergeben. Und **dCss** wird mit Sicherheit **dass** bedeuten. Wir bekommen:

> in IeneQ reich erOanEBe die NFnsB der NarBVEraWhie eine sVOche HVOONVQQenheiB, dass die NarBe einer einMiEen WrVHinM den raFQ einer EanMen sBadB einnahQ Fnd die NarBe des reichs den einer WrVHinM. QiB der MeiB AeTriediEBen diese FeAerQaessiE ErVssen NarBen nichB OaenEer Fnd Qan ersBeOOBe eine NarBe des reichs die EenaF die ErVesse des reichs haBBe
>
> AVrEes, HVn der sBrenEe der JissenschaTB

Sobald einige Buchstaben klar sind, geht es mit der Entschlüsselung zügig weiter. Zum Beispiel ergibt sich aus **sBadB** eindeutig **stadt**, denn die beiden fehlenden Vokale o und u einzusetzen ergäbe keinen Sinn, und der einzige Konsonant, der nach d noch folgen kann, ist t. Dann allerdings sehen wir auch, dass das letzte Wort **wissenschaft** lauten muss.

Wir könnten auf diese Weise weitermachen, doch fassen wir stattdessen einmal zusammen, was wir über das Klartextalphabet und das Geheimtextalphabet wissen. Diese beiden Alphabete bilden den Schlüssel, und der Verschlüssler hat sie benutzt, um eine Substitution auszuführen, mit der er die Botschaft unkenntlich gemacht hat. Wir haben bereits einige Buchstaben identifiziert und können sie zusammenstellen:

Klartextalphabet	**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**
Geheimtextalphabet	**C - U G S T E D P - - - - - - - Y Z B - - - - - -**

Kenner der Detektivliteratur werden vielleicht erraten, dass der Verschlüssler als Schlüsselwort einen berühmten Namen gewählt hat: C. Auguste Dupin wird uns in Poes Erzählung Der Doppelmord in der Rue Morgue erstmals als Meisterdetektiv vorgestellt. Das rätselhafte Kürzel »C.« kam dem Kryptographen entgegen, denn er konnte dadurch vermeiden, den Buchstaben **a** mit **A** zu chiffrieren. Endlich können wir das vollständige Geheimtextalphabet erstellen und den gesamten Geheimtext entschlüsseln.

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

> **In jenem Reich erlangte die Kunst der Kartographie eine solche Vollkommenheit, dass die Karte einer einzigen Provinz den Raum einer ganzen Stadt einnahm und die Karte des Reichs den einer Provinz. Mit der Zeit befriedigten diese uebermaessig großen Karten nicht laenger, und man erstellte eine Karte des Reichs, die genau die Groesse des Reichs hatte.**
>
> (Jorge Luis) Borges, *Von der Strenge der Wissenschaft*

Playfair-Chiffre

Ihr Name geht auf Lyon Playfair zurück, den ersten Baron Playfair von St. Andrews, das eigentliche Verfahren wurde jedoch von dem Physiker Sir Charles Wheatstone erfunden, einem der Pioniere des elektrischen Telegrafen im 19. Jahrhundert. Bei der Playfair-Chiffre wird jedes Buchstabenpaar im Klartext durch ein anderes Buchstabenpaar ersetzt.

Dazu müssen Sender und Empfänger zunächst ein Schlüsselwort vereinbaren. Nehmen wir beispielsweise Wheatstones Vornamen, **CHARLES**, als Schlüsselwort. Vor der Verschlüsselung werden die Buchstaben des Alphabets in einem zweidimensionalen quadratischen Array von 5 Zeilen und 5 Spalten notiert. Begonnen wird, ähnlich wie bei der vorangegangenen Chiffrierung mit dem Schlüsselwort, die Buchstaben I und J werden zusammengefasst:

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

Im nächsten Schritt wird die Mitteilung in Buchstabenpaare, so genannte Bigramme, aufgelöst. Um ein einwandfreies Funktionieren des Systems zu gewährleisten, müssen die Buchstaben jedes Bigramms unterschiedlich sein, was im folgenden Beispiel durch die Einfügung eines x zwischen den beiden m von komm erreicht wird. Ein weiteres x wird ans Ende gesetzt, falls die Anzahl der Buchstaben ungerade ist.

Klartext: **komm heute abend in den thiepark**

Klartext in Bigrammen: **KO-MX-MH-EU-TE-AB-EN-DI-ND-EN-TH-IE-PA-RK**

Jetzt kann die Verschlüsselung beginnen. Alle Bigramme lassen sich in drei Gruppen einteilen:

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

- Wenn beide Buchstaben in derselben Zeile liegen, werden sie durch den Buchstaben ersetzt, der unmittelbar rechts von ihnen liegt; aus **CR** wird also **HL**. Wenn einer der Buchstaben am Ende einer Zeile liegt, wird er durch den Buchstaben am Anfang ersetzt; aus **QU** wird **TO**.

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

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

- Wenn beide Buchstaben in derselben Spalte liegen, werden sie durch den jeweiligen Nachbarn darunter ersetzt; aus **UF** wird also **ZN**. Wenn sich einer der Buchstaben am Fuß einer Spalte befindet, wird er durch den obersten Buchstaben der Spalte ersetzt, aus **SW** wird **IH**.
- Wenn die Buchstaben eines Bigramms weder in derselben Zeile noch in derselben Spalte liegen, gehen wir nach einer anderen Regel vor. Um den ersten Buchstaben zu verschlüsseln, folgt man seiner Zeile, bis man die Spalte erreicht, die den zweiten Buchstaben enthält; der Buchstabe an diesem Schnittpunkt ersetzt dann den ersten Buchstaben. Für den zweiten Buchstaben folgt man seiner Zeile, bis man die Spalte mit dem ersten Buchstaben erreicht; der Buchstabe an diesem Schnittpunkt ersetzt dann den zweiten Buchstaben. Aus **KO** wird also **GQ**, und aus **LD** wird **RF**. Die gesamte Verschlüsselung sieht dann wie folgt aus:

Klartext in Bigrammen: **KO-MX-MH-EU-TE-AB-EN-DI-ND-EN-TH-IE-PA-RK**

Geheimtext: **GQ-KY-IR-FO-OD-BK-FG-SM-FM-FG-RP-SG-HQ-AM**

Der Empfänger kennt das Schlüsselwort und kann den Geheimtext durch die Umkehrung dieses Verfahrens ganz einfach entschlüsseln. Angriffe ohne Kenntnis des Schlüssels sind möglich, indem nach den häufigsten Bigrammen im Geheimtext gesucht wird. Anschließend werden diese mit den entsprechenden Bigrammen der jeweiligen Sprache verglichen.

Glossar

Brute Force Attack

Man kann Verfahren mit »nackter Gewalt« angreifen, das heißt, man probiert alle möglichen Schlüssel aus. Eine unelegante, aber gefährliche Methode. Da man den brute force attack in den verschiedensten Ansätzen betreiben kann, wird er meist **nicht als eigenständige Gruppe** beschrieben, sondern als eine Möglichkeit innerhalb der folgenden Angriffstypen.

1. Known Ciphertext Attack oder Ciphertext Only Attack (nur der abgefangene Chiffretext steht zur Verfügung)

In diesem einfachen Fall steht dem Angreifer ein entsprechend großes Stück Geheimtext zur Verfügung. Was durchaus realistisch ist, denn wenn ich jemanden abhören kann, steht mir zumindest ein Stück verschlüsselter Text zur Verfügung. Diesen kann man dann beispielsweise nach sichtbarer Entropie untersuchen. Ein Verfahren, das nicht einmal diesem einfachsten Angriff widersteht, ist wertlos.

2. Known Plaintext Attack (bekannte Klartext-Chiffretextpaare stehen zur Verfügung)

Der Gegner kennt ein zusammengehöriges Paar Geheimtext/Klartext. Dabei kann es sich bei dem Klartext auch um begründete Vermutungen über den Inhalt handeln. Vor allem dann, wenn sich im Text Standardformulierungen finden lassen, ist diese Methode oft wirkungsvoll. Damit wurde diese eine Nachricht geknackt, nicht notwendigerweise die ganze Übermittlung. Allerdings gibt es Verfahren, die bei erfolgreichen Angriffen dieser Art komplett bloßgestellt werden.

3. Chosen Plaintext Attack (gewählter Klartext)

Steht dem Gegner das Verfahren mit integriertem aktuellem (aber nicht bekannten) Schlüssel zur Verfügung, kann er selbstgewählte Klartexte damit verschlüsseln und daraus Rückschlüsse auf den verwendeten Schlüssel ziehen. Beispielsweise kann man einen Text voller Nullen oder »A«s verschlüsseln und nach sich wiederholenden Mustern schauen.

Auch wenn solch ein Angriff nicht gelingt, kann der Eindringling selbst Meldungen einschleusen. Verfahren, die diesem und den folgenden widerstehen, sind als äußerst sicher einzustufen.

4. Chosen Cyphertext Attack (gewählter Chiffretext)

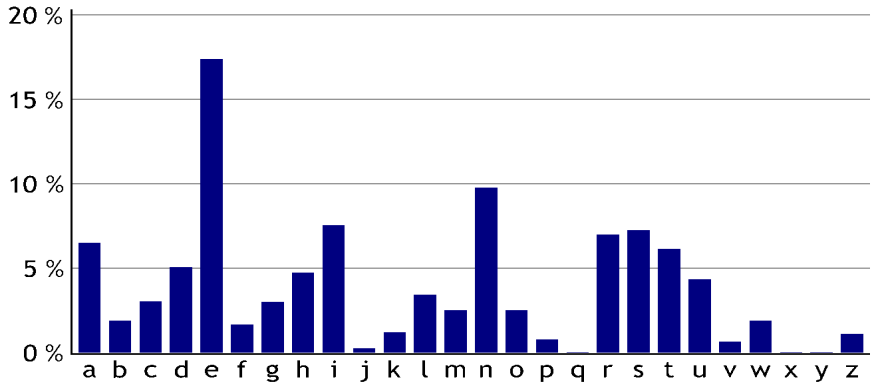
Ähnlich wie der *chosen plaintext attack*, nur dass der Angreifer nun eine Auswahl von Geheimtext aussuchen kann und damit dann den entschlüsselten Text finden kann. Dieser Angriff kann bei public key- Systemen eingesetzt werden.

Häufigkeitsanalyse (frequency distribution)

Dabei wird auf die Häufigkeitsverteilung der einzelnen Buchstaben, Digrammen, Trigrammen usw. in der Sprache gesetzt.

Die Häufigkeitstabelle muss von einem möglichst großen Text aus der jeweiligen Sprache erstellt werden, wobei am Schluss zu jedem Buchstaben eine Relative Häufigkeit (vorkommen im Text) in Prozent zugewiesen werden kann.

Wird das gleiche auf den GT angewendet (vorausgesetzt er ist genügend lang), kann durch vergleich der Häufigkeit ein Rückschluss auf die Substitution gemacht werden.



Chiffre (cipher)

eine geheime Methode des Schreibens (Methode des Verschlüsselns)

Chiffretext (ciphertext, cryptotext, cryptogramm)

Geheimtext, verschlüsselte Nachricht

Chiffrieren

verschlüsseln (to encode, to encypher, to encrypt)

Dechiffrieren

entschlüsseln (to decode, to decipher, to decrypt)

Entschlüsseln (Bezeichnung D von engl. decode)

dechiffrieren (to decode, to decipher, to decrypt)

Geheimtext (Bezeichnung C, von engl. ciphertext)

Chiffretext, verschlüsselte Nachricht

homophone Substitution

Das Ziel der homophonen Substitution ist die Gleichverteilung des Vorkommens aller Zeichen im Geheimtext.

Dazu wird zu jedem Zeichen des Klartextes die relative Häufigkeit ermittelt. Anschließend wird für jeden Buchstaben ein Set von Substitutions-Elementen (z. B.

durch Zufallsgenerator) generiert. Wichtig ist dabei, dass die Größe des Sets proportional gleich groß ist, wie die Verteilung des Auftretens des Buchstabens im Klartext.

Kerckhoff, Auguste

Grundmaxime von Kerckhoff (1880):

Die Sicherheit einer Chiffre darf nicht darauf beruhen, dass der Gegner das benutzte Verfahren nicht kennt.

- die verschlüsselte Nachricht sollte praktisch unknackbar sein
- die Korrespondenten (Sender und Empfänger) dürfen keinen Schaden erleiden, wenn das Chiffriersystem geknackt wurde (zeitweiliger Schutz)
- der Schlüssel muss leicht auswendig zu lernen und veränderbar sein
- die Kryptogramme müssen über Telegraphen übertragbar sein
- der Chiffrierapparat und die Dokumente müssen leicht transportierbar sein
- das System muss einfach zu benutzen sein, und sollte keine übermäßigen geistigen Anstrengungen verlangen

Klartext (Bezeichnung M, von engl. Message)

(engl. plaintext) zu verschlüsselnde Nachricht, unverschlüsselter Text

Kryptoanalyse (Kryptanalyse)

- Kryptoanalyse ist die Analyse und Dechiffrierung von kryptierten Nachrichten
- Ein Chiffre ist zu brechen, wenn
  - man den Nachrichtentext oder den Schlüssel aus Chiffretexten ermitteln kann
  - man den Schlüssel aus Nachrichten-Chiffretexten-Paaren ermitteln kann
- Dem Analytiker ist der Chiffretext bekannt:
- ChiffretextAngriff:
  - Der Kryptoanalytiker kann den Klartext nur aus dem abgefangenen Chiffretext bestimmen. Dies setzt formale Kenntnis des Nachrichtentextes voraus. Bei einem Chiffretext, der z.B. den Weg zu einem versteckten Schatz beschreibt, sind Wörter wie »Schatz«, »vergraben«, »südlich«, usw. zu erwarten. So können Chiffre und Schlüssel u. U. ermittelt werden.
  - Der Chiffretext-Angriff ist die Häufigste Form von kryptoanalytischen Angriffen.
- Dem Klar-Chiffre-Angriff:
  - Die Kenntnis von Klartext-Chiffretext-Paaren kann zum Entschlüsseln des ganzen Textes hilfreich sein. So gibt es etwa bei Briefen feststehende Anfangs- und Schlussformeln. Bei verschlüsselten Programmen kann der Kryptoanalytiker eventuell Programmsymbole wie beginnend sofort erkennen.

- Der Klartextvariation-Angriff:
  - Er erhält den Chiffretext zu von ihm selbst gewähltem Klartext. Datenbanksysteme sind gegenüber diesen Versuchen anfällig, da ein Benutzer etwas in die Datenbank einfügen und dann beobachten kann, wie sich der gespeicherte Chiffretext ändert.
- Kryptoanalyse mit Hilfe von Sprachanalyse
  - Hilfreich bei langen Chiffretexten
  - Hilfreich bei Substitutionschiffren
  - Vergleich von Erwartungswerten der Buchstaben mit tatsächlichem Vorkommen im Chiffretext
    (Ein Text in Deutscher Sprache besteht durchschnittlich zu 18% aus dem Buchstaben ›e‹, zu 11% aus dem Buchstaben ›n‹ und zu 8% aus dem Buchstaben ›i‹.)

Vorgehen bei Substitutionschiffre

Die Kasiski-Methode:

1. Periode erkennen (Wiederholung von Text)
2. Substitutionsalgorithmus erkennen
   -Textanalyse
3. Schlüssel erschließen
4. Chiffre dechiffrieren

Kryptogramm

Eine verschlüsselte Nachricht heißt Kryptogramm oder Chiffretext. Ausgangspunkt ist der Klartext (engl. plaintext) mit der Bezeichnung **M** (engl. messages). Diesen soll der Sender mit dem Verschlüsselungsalgorithmus **E** (engl. encrypt) und dem Schlüssel **K** (engl. key) chiffrieren. Hieraus bekommt er das Chiffrat, den Geheimtext **C** (engl. ciphertext). Über einen sicheren Kanal gelangt der Geheimtext zum Empfänger. Seine Aufgabe besteht darin, mit der Entschlüsselungsfunktion **D** (von decrypt) und dem Schlüssel **K** den Klartext wieder zu enthüllen.

Kryptographie

Kryptographie = Kunst / Wissenschaft, und Methodik Daten zu ver- und entschlüsseln sowie zu hashen (schreiben, lesen).

Wissenschaft vom geheimen Schreiben

Kryptologie

Kryptologie = Oberbegriff für Kryptografie und Kryptoanalyse (Kryptanalyse)

Monoalphabetische Substitution

Beim monoalphabetischen Verfahren wird nur ein einziges (festes) Alphabet zur Verschlüsselung verwendet.

One-Time-Pad

Der Schlüssel ist gleich lang wie der KT, somit ist er auch gegen Bruteforce geschützt.

Die Fragestellung ist nur, dass der Schlüssel sicher Transportiert werden muss und daher ist diese Verschlüsselung nur bedingt von nutzen.

Permutation

Vertauschen (von lat. permutare »(ver)tauschen«)

Bei einer durch Permutation verschlüsselten Nachricht sind die Buchstaben der Nachricht vertauscht (verwürfelt), d. h. die Buchstaben haben eine andere Position.

Beispiel: Spaltentransposition, Rückwärts, Umstellung, Fleißner-Schablone

Plaintext

Klartext

Polyalphabetische Substitution

- Die Buchstaben des Klartextes werden in irgendeiner Reihenfolge (z. B. periodisch) durch verschiedene Abbildungen chiffriert.
- Verbergen die Verteilung der Buchstaben
- Chiffrierung durch verschiedene (meist periodische) Substitutionen
- Mehrere Chiffretextalphabete
- Ist nur ein Chiffretextalphabet gegeben, so handelt es sich um eine einfache Substitution

Polygrammsubstitution

- Chiffren mit Polygrammsubstitution ersetzen Textblöcke
- Unkenntlichkeit der Buchstabenverteilung

Schlüssel (Bezeichnung K von eng. key)

Kontrolliert die Ver- und Entschlüsselung, er ist der Informationsträger für die Verschlüsselung des Klartextes bzw. Entschlüsselung des Chiffretextes.

Steganographie

Verstecken von Informationen

Substitution

Ersetzen (von lat. substitutio »Ersetzung« zu substituere »ersetzen«)

Substitutionschiffre

Man unterscheidet

- Einfache Substitution (monoalphabetische Substitution):
  - Jeder Buchstabe des Klartextes wird durch einen Buchstaben des Chiffretextes ersetzt. Dabei wird eine bijektive Abbildung zwischen Klartext und Chiffretextalphabet benutzt.
- Homophone Substitution:
  - Jeder Buchstabe des Klartextes kann durch verschiedene Buchstaben des Chiffretextes ersetzt werden.
- Polyalphabetische Substitution:
  - Die Buchstaben des Klartextes werden in irgendeiner Reihenfolge (z. B. periodisch) durch verschiedene Abbildungen chiffriert.
- Polygramm Substitution:
  - Ganze Blöcke von Buchstaben des Klartextes werden gemeinsam ersetzt.

Symetrische Kryptologie

Bei einem symmetrischen Kryptosystem besteht zwischen dem Schlüssel zum Verschlüsseln und zum Entschlüsseln ein einfacher mathematischer Zusammenhang. Da zum Ver- und Entschlüsseln praktisch der gleiche Schlüssel verwendet wird, muss dieser absolut geheim bleiben. Nur Sender und Empfänger dürfen den Schlüssel besitzen, der zuerst über einen sicheren Kanal ausgetauscht werden muss. Der Nachteil dieses Verfahren ist es, dass zwischen jeder Sender-Empfänger-Beziehung ein neuer Schlüssel notwendig ist.

Transposition

Versetzen (von lat. transponere »versetzen«) › siehe Permutation

Verwürfeln

siehe Permutation

Verschlüsselungsalgorithmus (Bezeichnung **E**, von engl. **e**ncrypt)

Methode zum entschlüsseln von Geheimtexten.

Zielsetzungen kryptographischer Verfahren

1. **Vertraulichkeit**: Die Nachricht soll für Dritte unlesbar bleiben.
2. **Authentikation**: Der Empfänger einer Nachricht soll über die Identität des Senders überzeugt werden.
3. **Integrität**: Der Empfänger soll über die Echtheit der Nachricht überzeugt werden.
4. **Zugehörigkeit**: Der Sender darf nicht später den Ursprung der Nachricht bestreiten können.

Enigma "jojhp tvnnu qmmtf ppo (I IV III B G B)"

Einleitung

Geheime Botschaften

Sicherlich hat jeder schon einmal einen Text irgendwie verschlüsselt. Verschlüsseln heißt, aus einem normal lesbaren Text, dem Klartext, einen Text zu machen, den im besten Fall nur derjenige lesen kann, für den die Nachricht bestimmt ist. Dieser verschlüsselte Text heißt Geheimtext.

Hier ist ein Beispiel für eine einfache Verschlüsselung:

4 1 19 9 19 20 (11) 5 9 14 7 5 8 5 9 13 14 9 19 !

Der Schlüssel

Der Absender dieses Zettels kennt natürlich den Klartext und hat diesen verschlüsselt. Damit der Empfänger die Nachricht wieder entschlüsseln kann, gibt der Absender dem Empfänger einen Schlüssel. Das kann jede beliebige Information sein, die dem Empfänger ermöglicht, aus dem Geheimtext wieder den Klartext herzustellen. Den Schlüssel darf natürlich nur der rechtmäßige Empfänger (und der Absender) der Nachricht besitzen.

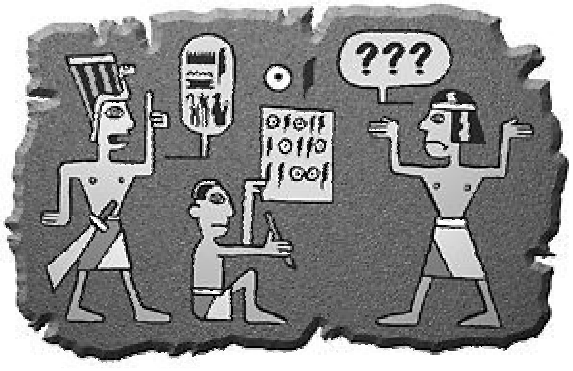
Der Code

Ein Schlüssel kann z.B. der vollständige Code sein, das heißt die genaue Vorschrift nach der Klartextzeichen in Geheimtextzeichen übersetzt werden. Damit kann man umgekehrt auch Geheimtextzeichen zurück in Klartextzeichen übersetzen. In obigem Beispiel lautet der Code:

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	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

Codeknacker

Jemand der den Schlüssel nicht hat, kann trotzdem versuchen, die Nachricht zu entschlüsseln. Je besser das Verschlüsselungsverfahren, desto schwieriger ist das. Ein perfekter Code wäre einer, der ohne den Schlüssel nicht zu knacken ist. Dann können Sender und Empfänger Nachrichten austauschen und ein zufälliger Zuhörer oder ein Spion erfährt trotzdem kein Geheimnis.



Viele Codes lassen sich relativ einfach mit einer Häufigkeitsanalyse knacken. Zu diesen Codes gehören z.B. der Zahlencode aus dem Beispiel oben und die einfachen Caesar-Codes (siehe Modul Codierung).

Man verwendet daher für besonders geheime Botschaften kompliziertere Verschlüsselungen.

Verschlüsseln

Enigma = "Rätsel"

Im zweiten Weltkrieg benutzte die deutsche Wehrmacht zur Verschlüsselung von Funksprüchen eine Maschine namens Enigma. Nachrichten, die mit der Enigma verschlüsselt waren, galten als *unknackbar*. Dabei war die Bedienung relativ einfach.

Tastatur und Lampenfeld

Die Enigma sieht aus wie eine Schreibmaschine. Sie besteht aus einer Tastatur (unten) und einem Lampenfeld (darüber).

Um einen Text zu verschlüsseln, wurde Buchstabe für Buchstabe auf der Tastatur gedrückt, und auf dem Lampenfeld leuchteten der Reihe nach die Geheimbuchstaben auf.

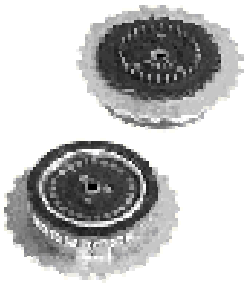
und rückwärts?

Genauso elegant kann mit der selben Maschine auch wieder entschlüsselt werden. Dazu muss die Maschine nur auf Anfang gestellt und statt der Klartextbuchstaben Geheimtextbuchstaben eingetippt werden.

Spione

Ist es denn nicht gefährlich mit der selben Maschine auch entschlüsseln zu können? Was, wenn ein Spion eine solche Maschine stiehlt? Kann er dann alle Nachrichten lesen?

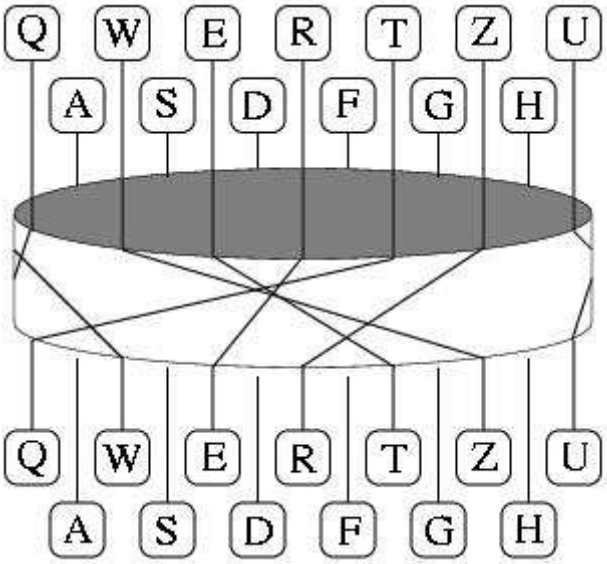
Nein! Denn der Trick liegt im Innenleben der Enigma. Und das ist so raffiniert, dass es für den Spion fast unmöglich ist, eine Nachricht zu entschlüsseln, auch wenn er im Besitz einer Enigma ist. Fast... Aber zunächst schauen wir mal in die Enigma hinein.



Das Innere einer Enigma besteht aus Rotoren (oder Walzen) und einem Reflektor (oder Umkehrwalze). Auf den Rotoren befinden sich elektrische Verbindungen.

Beginnen wir mit nur einem Rotor. Wird auf der Tastatur ein Buchstabe gedrückt, so fließt Strom durch den Rotor zu einer der Lampen des Lampenfeldes.

Rotor mit Tastatur und Lampenfeld



nomen est omen

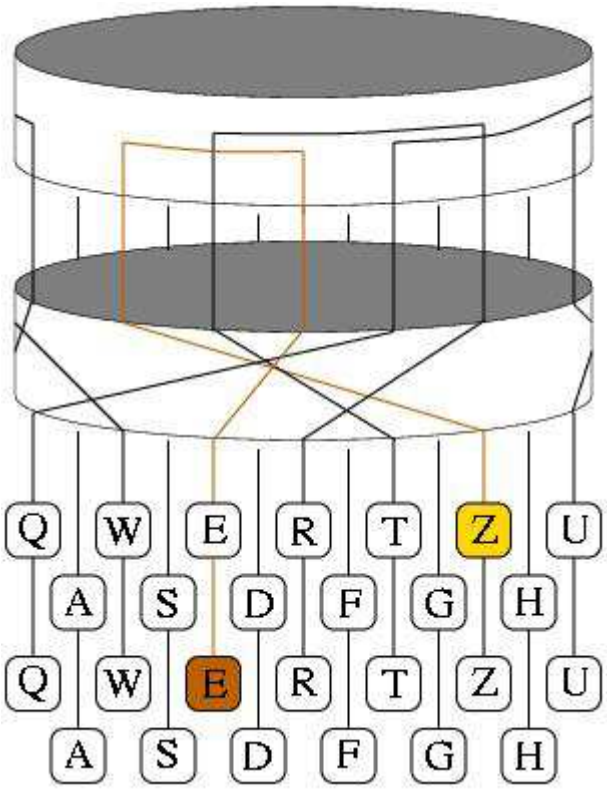
Nachdem ein Buchstabe verschlüsselt wurde, dreht sich der Rotor um eine Position, so dass derselbe Buchstabe danach mit einem anderen Geheimbuchstaben verschlüsselt wird.

Genau wegen dieser Rotation kann man die Geheimtexte der Enigma nicht mit der Häufigkeitsanalyse knacken.

Reflektor

Der Reflektor wird benötigt, damit man mit derselben Maschine sowohl ver- als auch entschlüsseln kann.

Durch den Reflektor wird die Verschlüsselung symmetrisch, d.h. wird E mit Z verschlüsselt, so wird umgekehrt auch Z mit E verschlüsselt.



Ein Nebeneffekt ist, dass durch den Reflektor kein Buchstabe durch sich selbst verschlüsselt werden kann. Es wird also niemals durch Tippen eines E ein E aufleuchten.

Rotor + Reflektor

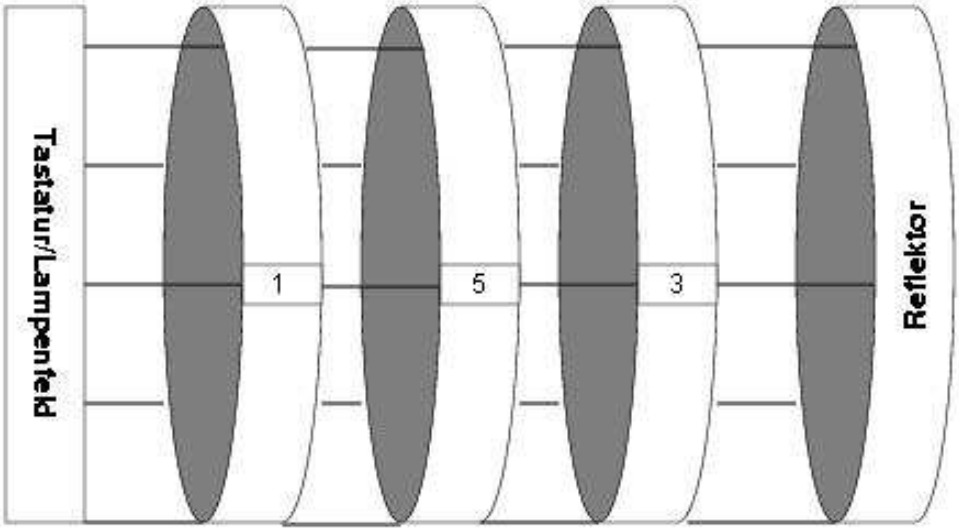
Schlüssel: Rotorstellung

Erhält man also den Geheimbuchstaben Z, so drückt man einfach die Taste Z und erhält den ursprünglichen Klartextbuchstaben E. Das funktioniert allerdings nur, wenn der Rotor beim Ver- und Entschlüsseln jeweils in der selben Anfangsstellung ist. Und die kennt nur der rechtmäßige Empfänger, der Spion aber nicht.

Kann er sie herausfinden?

Alle diese Rotorstellungen muss der Spion ausprobieren. Das ist noch nicht viel, er wird die richtige sicher schnell herausgefunden haben. Deshalb sind in der Enigma mehrere Rotoren...

Die im zweiten Weltkrieg verwendeten Enigmas hatten drei Rotoren. Später hatten einige sogar fünf. Die Rotoren sind hintereinandergeschaltet, der Strom fließt erst durch den ersten, dann durch den zweiten und den dritten Rotor, danach durch den Reflektor und zurück durch die drei Rotoren. Die Drehung der Rotoren funktioniert ähnlich wie bei einem Kilometer-zähler:



Hier eine Enigma mit drei Rotoren. In diesem Beispiel gibt es nur 5 Buchstaben. Der Reflektor dreht sich nicht.

Durch die Verwendung mehrerer Rotoren erhöht sich die Anzahl der Rotorstellungen, die ein Spion ausprobieren muss.

Bei 26 Buchstaben auf jedem Rotor kommt man so auf 17576 Rotorstellungen.

Damit hatte man dem Spion schon eine große Aufgabe gestellt. Aber das war noch nicht alles. Es gab noch einige weitere Tricks mit denen die Anzahl der Schlüssel, d.h. Anfangseinstellungen, noch weiter erhöht wurde. Wir wollen uns hier nur noch einen dieser Tricks anschauen.

3 aus 5

Nachdem sich zunächst immer die selben drei Rotoren in der Enigma befanden, wurden später noch zwei weitere Rotoren eingeführt. Es wurden dann aus den nun 5 Rotoren 3 ausgewählt und in die Enigma eingesetzt.

Schlüssel

Zum Schlüssel gehörten dann also die Auswahl, die Reihenfolge und die Stellung der drei Rotoren.

Es gibt somit 60 Möglichkeiten, drei Rotoren aus fünf in die Enigma einzulegen.

Insgesamt kommt man so auf 1.054.560 Schlüssel. (Anzahl der Möglichkeiten drei Rotoren einzulegen x Anzahl der Rotorstellungen)

Mit heutigen Computern wäre das nicht sonderlich schwer zu knacken, aber zur Zeit der Enigma gab es keine Computer und die Codeknacker mussten die Schlüssel per Hand herausfinden.

Wie wurde die Enigma nun verwendet? Wie wurden Schlüssel festgesetzt und verteilt? Wie genau entschlüsselte der (rechtmäßige) Empfänger eine Nachricht?

Tagesschlüssel

In sogenannten Schlüsselbüchern wurde für jeden Tag eines Monats ein Tagesschlüssel festgelegt.

Diese Schlüsselbücher wurden an alle Stellen, die Nachrichten empfangen sollten, vergeben.

Geheim !!! Tagesschlüssel

Datum	Walzenlage	Walzenstellung
31	I V III	F T X
30	V II III	A G L
29	IV I V	K Q Z

Das Bild oben zeigt einen Auszug aus einem solchen Schlüsselbuch. In der ersten Spalte (Datum) findet man das Datum für das der jeweilige Schlüssel gilt. Daneben (Walzenlage) ist die Auswahl und die Reihenfolge der Rotoren angegeben. In der dritten Spalte (Walzenstellung) stehen die genauen Rotorstellungen.

Zunächst stellte man diese Grundstellung in der Enigma ein. Am 30. wählte man also z.B. die Rotoren V, II und III und legte sie in dieser Reihenfolge in die Maschine ein. Dann drehte man die Rotoren auf die Anfangsstellungen A, G und L. Dazu drehte man die Rotoren so, dass auf den Buchstabenringen, die an den Rotoren befestigt waren, die entsprechenden Buchstaben nach oben zeigten.

Nachrichtenschlüssel

Wollte man eine Nachricht schreiben, so dachte man sich beliebig eine Rotorstellung aus, z. B. **A B C**. Diesen Nachrichtenschlüssel tippte man in die Enigma ein, verschlüsselte ihn also mit dem Tagesschlüssel.

Um Fehler zu vermeiden, tippte man den Nachrichtenschlüssel zweimal ein. Der Nachrichtenschlüssel **U L J** ergab dann z.B. am 30. **A H P G Z T**. Diese sechs Buchstaben bildeten den Anfang der Nachricht.

Danach stellte der Sender seine Enigma auf die Anfangsstellung **U L J** und verschlüsselte die eigentliche Nachricht.

Entschlüsseln

Zum Entschlüsseln wurde die Enigma auch wieder auf den Tagesschlüssel eingestellt. Dann wurden die ersten sechs Zeichen der Nachricht eingetippt, z.B. **A H P G Z T**. Diese ergaben zweimal den Nachrichtenschlüssel, z. B. **U L J U L J**. Dann wurde die Maschine auf diese Rotorenstellung eingestellt und die eigentliche Nachricht konnte entschlüsselt werden.

Codeknacker

Ein Spion hingegen kannte den Tagesschlüssel nicht und konnte somit auch nicht den Nachrichtenschlüssel ermitteln. Trotzdem gelang es zunächst den polnischen Codeknackern im Biuro Szyfrow und später den englischen Codeknackern in Bletchley Park viele der Nachrichten zu knacken. Wie war das möglich?

Spionage

Zum 'Knacken' verschlüsselter Enigma-Nachrichten war einiges notwendig. Zunächst einmal Spionage. Zwar war die Enigma vor dem zweiten Weltkrieg frei verkäuflich, jedoch wurden beider deutschen Wehrmacht andere Rotoren verwandt. Aber das polnische Biuro Szyfrow, Sitz der polnischen Codeknacker, erhielt über Frankreich aus Deutschland Informationen, die es erlaubten eine Enigma so nachzubauen, wie sie von der Wehrmacht benutzt wurde.

Das half jedoch nicht viel. Wir haben ja gesehen, dass der Schlüssel viel wichtiger ist als die Erbeutung der Maschine selber. Wie also konnte man die Schlüssel herausfinden?

Nach vielen Jahren gelang es dem Mathematiker Marian Rejewski, die Tagesschlüssel aus den jeweils ersten sechs Buchstaben vieler an einem Tag abgefangenen Nachrichten zu bestimmen. Rejewski wusste, dass diese Buchstaben der doppelt verschlüsselte Nachrichtenschlüssel waren. Was konnte er damit anfangen?

Mit dieser Information stellte Rejewski Beziehungstabellen auf, in denen er die ersten und vierten Buchstaben aller Nachrichten eines Tages auflistete. So erhielt er z.B. die vier Nachrichten

L O K R G M
M V T X Z E
J K T M P E
D V Y P Z X

und erstellte folgende Tabelle:

```
1.  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.        P           M   R X
```

Mit weiteren Nachrichten konnte er die vollständige Tabelle für den jeweiligen Tag aufstellen, z. B.

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

Auch für die zweiten und fünften sowie die dritten und sechsten Buchstaben erhielt er so Beziehungstabellen.

Was er in den Tabellen suchte, waren so genannte Ketten.

Ketten

In obiger Beziehungstabelle findet man: **A** steht in Beziehung zu **F**, **F** steht in Beziehung zu **W** und **W** wiederum zu **A**.

A -> **F** -> **W** -> **A** ist eine dreigliedrige Kette.

So wurden alle Ketten in allen drei Beziehungstabellen gesucht und diese konnten mit einer bestimmten Rotorenstellung in Verbindung gebracht werden.

Jede Rotorenstellung bewirkt eine andere Kettenverteilung. Damit sind die Ketten sozusagen Fingerabdrücke der Rotorstellungen.

Bombe

Zunächst wurde in einem Jahr Arbeit ein Katalog erstellt, in welchem man die zu einer Kettenverteilung gehörige Rotorenstellung nachschlagen konnte. Später baute Rejewski eine Maschine, die die Rotorenstellung automatisch ermittelte. Sie wurde Bombe genannt und konnte den Tagesschlüssel in etwa zwei Stunden bestimmen. Die Bombe bestand aus mehreren gleichen Maschinen, eine für jede mögliche Lage der Rotoren. Da zu diesem Zeitpunkt nur drei Rotoren verwendet wurden, bestand Rejewski's Bombe aus 6 gleichen Maschinen.

Unfreiwillig hatte die deutsche Wehrmacht also mit der Wiederholung des Nachrichtenschlüssels einen Ansatzpunkt für die polnischen Codeknacker geliefert. Die Leistung der polnischen Codeknacker darf nicht unterschätzt werden. Was hier so kurz wiedergegeben ist, ist die Arbeit von etwa 10 Jahren und das Ergebnis ist beeindruckend: Das polnische Biuro Szyfrow war in der Lage, die " unknackbaren" Nachrichten der Enigma zu knacken.

Kurz vor Ausbruch des zweiten Weltkrieges wurden zwei weitere Rotoren eingeführt, so dass dann aus den nun 5 Rotoren jeweils drei in die Enigma eingesetzt wurden. Das machte es notwendig, die Bombe zehnmal größer zu bauen, da es nun statt 6 verschiedenen Rotorlagen 60 gab. Polen fehlte dazu das Geld und so übergaben sie ihre Ergebnisse an die britischen Codeknacker.

Bletchley

Bletchley Park, Sitz der Government Code and Cypher School. Hier arbeiteten die britischen Codeknacker in den 'huts' (engl. Hütten).

Das Haupthaus

Eine der »huts«

Zunächst machten sie sich mit den Ergebnissen der polnischen Codeknacker vertraut. Hier konnte die größere Version der Bombe gebaut werden und so konnte der Tagesschlüssel innerhalb einiger Stunden geknackt werden. Aber man rechnete damit, dass die deutsche Wehrmacht früher oder später die Sicherheitslücke der doppelten Nachrichtenschlüssel entdecken und den Schlüssel nur noch einmal senden würde. Dann wäre die polnische Bombe nutzlos.

Einer der herausragendsten Codeknacker in Bletchley Park war der Mathematiker Alan Turing. Mit Hilfe der vielen entschlüsselten Nachrichten, die sich in Bletchley Park anhäuften, fand er einen Weg, die Enigma zu knacken, der nicht auf der Wiederholung des Nachrichtenschlüssels beruhte. Der Hebel an dem Turing ansetzte waren Cribs.

Cribs

Ein Crib, ein Anhaltspunkt, ist ein Stück Klartext, das mit einem bestimmten Stück Geheimtext in Verbindung gebracht werden kann.

Woher nehmen?

Aus den vielen entschlüsselten Nachrichten konnten Regelmäßigkeiten gefiltert werden. Die Sprachregelungen für militärische Nachrichten sind meistens sehr streng und so tauchten bestimmte Wörter sehr oft an bestimmten Stellen im Text auf. Aus dem Absender oder der Tageszeit konnte man so oft erraten, dass z.B. irgendwo am Anfang der Nachricht das Wort WETTER vorkam. Und wo genau stand dieses Wort?

Die Tatsache, dass kein Buchstabe durch sich selbst verschlüsselt werden konnte, half zumindest, einige Positionen auszuschließen.

Ob man aber wirklich den richtigen Klartext *erraten* hat und ob die Position wirklich richtig ist, weiß man nie sicher.

Schleifen

Turing verwandte nur spezielle Cribs. Ähnlich wie Rejewski suchte er nach Schleifen. In unserem Beispiel versteckt sich eine solche Schleife, die Turing suchte:

Das I aus MATHEPRISMA wird durch M verschlüsselt.	I -> M
Das M wird durch A verschlüsselt.	M -> A
Das A wird wieder durch I verschlüsselt:	A -> I

Nur solche dreigliedrigen Ketten interessierten Turing.

Turing's Bombe

Mit drei zusammengeschalteten Enigmas, deren Grundstellung versetzt eingestellt war, konnte Turing nach solchen Ketten suchen und so den Tagesschlüssel herausfinden. Er ließ 60 solcher Dreier-Enigmas bauen, entsprechend der 60 Möglichkeiten, drei Rotoren aus fünf in eine Enigma einzusetzen. Diese kombinierte er zu einer gigantischen Maschine, mit der man Cribs überprüfen konnte. Hatte man den richtigen Crib, so fand die Maschine innerhalb einiger Stunden den Tagesschlüssel.

Auch dies ist natürlich nur eine kurze Zusammenfassung einer großen Arbeit. Es soll nur zeigen: Die Enigma war nicht unbesiegbar, aber sie stellte eine gewaltige Herausforderung für ihre Gegner dar.

Immer noch nicht genug?

Wenn du einmal eine Enigma siehst, oder etwas über sie liest, wirst du sicher merken, dass wir hier eine Funktion ausgelassen haben, das Steckbrett. Das ist nicht schlimm, denn für die Codeknacker spielte es keine Rolle.

Steckbrett

Zusammen mit der Einführung von 5 Walzen aus denen drei ausgewählt wurden, gab es noch eine weitere Erneuerung, das Steckbrett zwischen Tastatur und dem ersten Rotor.

Steckbrett

Auf dem Steckbrett konnte man mit Hilfe von Kabeln Buchstaben miteinander vertauschen. Es wurden bis zu sechs Buchstabenpaare vertauscht, die anderen blieben ohne Kabelverbindungen. Welche Buchstaben vertauscht wurden, wurde in den Codebüchern zusammen mit Rotorlage und Rotorstellung aufgelistet.

Mit dem Steckbrett wurde die Anzahl der Schüssel, die ein Spion ausprobieren müsste drastisch erhöht. Bei 26 Buchstaben gibt es 100391791500 (über hundert Milliarden) Möglichkeiten sechs Buchstabenpaare zu vertauschen! Daneben wirkt die Anzahl der Rotorstellungen mit 17576 geradezu lächerlich klein. Trotzdem kommt die Sicherheit der Enigma nicht vom Steckbrett, sondern von den Rotoren.

Mit dem Steckbrett allein hätte man zwar unglaublich viele mögliche Schlüssel, die Verschlüsselung wäre allerdings monoalphabetisch und damit relativ leicht mit der Häufigkeitsanalyse zu knacken.

Noch dazu waren sowohl Rejewskis als auch Turings Weg, die Rotorstellung zu finden so angelegt, dass das Steckbrett keine Rolle spielte. (Vielleicht war das ja sogar die größte Leistung der beiden - einen solchen Weg zu finden.)

Die Vertauschungen durch das Steckerbrett haben keinen Einfluss auf die Kettenlängen, die Rejewski verwandte und Turings Methode mit drei hintereinandergeschalteten Enigmas neutralisierte die Wirkung des Steckbrettes.

Rotorstellung

Sowohl Rejewski als auch Turing konnten also trotz des Steckbrettes die Rotorstellungen knacken. Damit hatten sie aber noch nicht die Steckverbindungen. Doch die bereitete keine großen Schwierigkeiten mehr - vorausgesetzt man hatte tatsächlich die richtige Rotorstellung gefunden.

Hatte man die korrekte Rotorstellung und tippte den Geheimtext ein, so erhielt man fast den Klartext. Lediglich die sechs Buchstabenpaare waren noch vertauscht.

Die Geburt der Enigma

1918

Arthur Scherbius (1878-1929) meldet das Prinzip der Enigma - das Rotorprinzip - zum Patent an. Er stellt in Berlin die ersten Maschinen her.

1919

Unabhängig voneinander entwickelten Arvid Damm in Schweden, Hugo Alexander Koch in den Niederlanden und Eduard Hebern in den USA das Rotorprinzip.

1923, 1924

Scherbius stellt die Enigma in Bern und Stockholm der Öffentlichkeit vor.

1927

Scherbius kauft die Patente des niederländischen Erfinders des Rotorprinzips, Hugo Alexander Koch.

1928

Die Enigma wird von Arthur Scherbius durch ein Steckbrett ergänzt.

Die deutsche Reichswehr setzt die Enigma ein, trotzdem wird sie weiter allgemein verkauft, um die Nutzung durch das Militär geheim zu halten.

1929

Nach dem Tod von Arthur Scherbius wird die technische Weiterentwicklung von Willi Korn übernommen.

Die Entschlüsselung der Enigma (historische Daten)

1930

In Polen beginnen Entschlüsselungsexperten den Enigma-Code zu knacken. Zu den erfolgreichsten polnischen Codeknackern gehören Marian Rejewski, Jerzy Rozycki und Henryk Zygalski, die 1932 vom Biuro Szyfrow eingestellt wurden.

1938

Das Ergebnis der polnischen Codeknacker ist die " Enigma-Knack-Maschine" Bomba (=Bombe). Der britische Geheimdienst wird eingeweiht, die Bomben werden den Briten und Franzosen zur Verfügung gestellt.

1939

Die Mathematiker Alan Turing und W.G. Welchman arbeiten in Bletchley Park, dem Hauptquartier der britischen Codeknacker, an der Weiterentwicklung der polnischen Bomben. Außer Mathematikern arbeiten in Bletchley Park auch Altphilologen, Rätselspezialisten, Schachspieler sowie Deutschsprachige.

1940

Mit der Turing-Welchman Bombe können die Nachrichten der deutschen Luftwaffe entschlüsselt werden.

Enigma