

Verschlüsselungsmethoden

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de , Raum 149B
Version: 1.1.5.3
Quelle: *Cryptography and Network Security - Principles and Practice, 8th Edition, William Stallings*

Kontrollfragen

Folien: [HTML] <https://delors.github.io/sec-klassische-verschluesselungsverfahren/folien.de.md.html>
[PDF] <https://delors.github.io/sec-klassische-verschluesselungsverfahren/folien.de.md.html.pdf>
Fehler melden: <https://github.com/Delors/delors.github.io/issues>

KI Verwendung: Bei der Erstellung der Unterlagen wurden KI Assistenten (insbesondere Claude aber ggf. auch ChatGPT, Ollama mit Gemma/LLama/Qwen oder OpenCode mit Kimi/Qwen/Deepseek...) unterstützend eingesetzt. Dies erfolgte insbesondere zur Unterstützung bei der Generierung von Grafiken (d. h. SVG Dateien), oder um sich Übersichtstabellen generieren zu lassen. Weiterhin wurde KI zur allgemeinen Qualitätssicherung eingesetzt. Inhalte, die ggf. von der KI vorgeschlagen wurden, wurden im Falle der Übernahme explizit validiert und angepasst.

1. Einführung

Zentrale Begriffe

Definition: Klartext ( *Plaintext*)

Die Originalnachricht, die verschlüsselt werden soll.

Definition: Geheimtext oder Chiffretext ( *Ciphertext*)

Die kodierte/verschlüsselte Nachricht.

(Im Deutschen gelegentlich auch Kryptogramm genannt.)

Definition: Verschlüsselung ( *Encryption*)

Der Prozess der Umwandlung von Klartext in Geheimtext.

Definition: Entschlüsselung ( *Decryption*)

Der Prozess der Wiederherstellung des Klartextes aus dem Geheimtext.

Definition: Kryptographie ( *Cryptography*)

Das Studiengebiet der Verschlüsselungsschemata.

Definition: Kryptoanalyse ( *Cryptanalysis*)

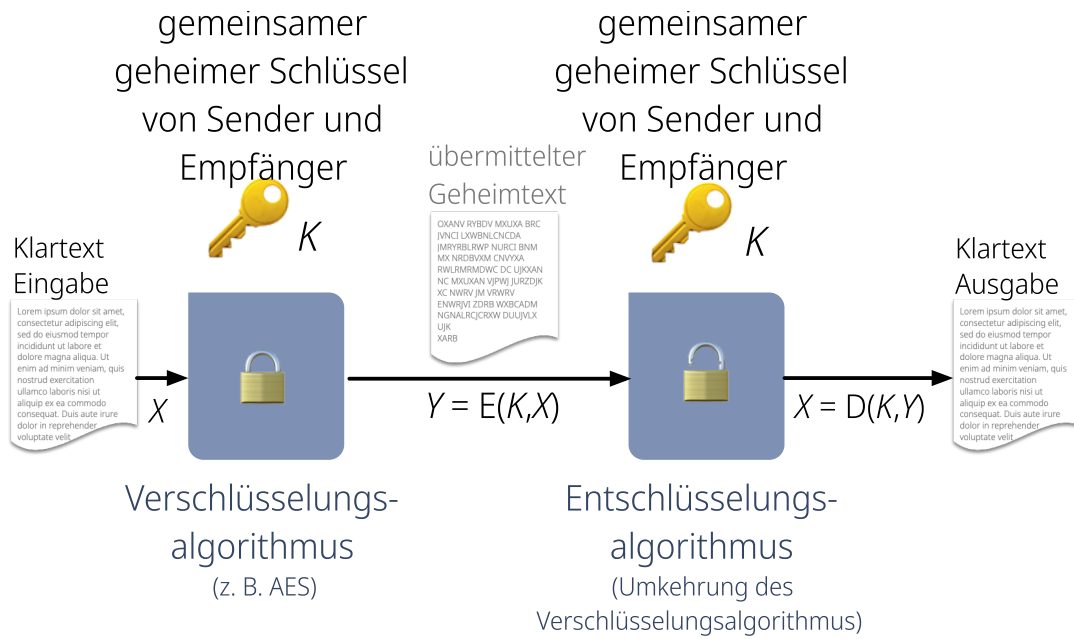
Methoden und Techniken, die zur Gewinnung von Informationen aus einer verschlüsselten Nachricht dienen.

Analyse von kryptographischen Verfahren.

Definition: Kryptologie ( *Cryptology*)

Die Bereiche Kryptographie und Kryptoanalyse.

Vereinfachtes Modell der symmetrischen Verschlüsselung

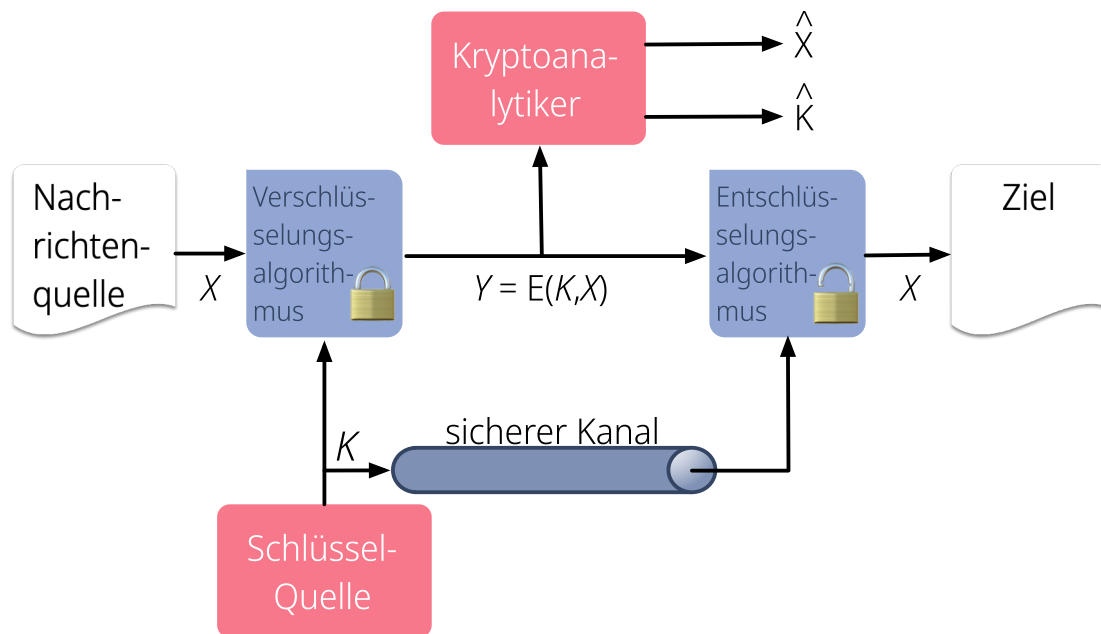


Symmetrisches Verschlüsselungsmodell

Es gibt zwei Voraussetzungen für die sichere Verwendung der herkömmlichen Verschlüsselung:

1. Ein starker Verschlüsselungsalgorithmus.
2. Effektive Schlüsselverwaltung:
 - a. Sender und Empfänger müssen Kopien des geheimen Schlüssels auf sichere Weise erhalten haben und
 - b. den Schlüssel sicher aufbewahren.

Modell eines symmetrischen Kryptosystems



Kryptografische Systeme können entlang dreier unabhängiger Dimensionen charakterisiert werden



Bemerkung

Eine Permutation ist eine Folge von Vertauschungen.

1. Die Art der Operation, die zur Umwandlung von Klartext in Chiffretext verwendet wird:

- Substitution
- Transposition (Vertauschungen)

2. Die Anzahl der verwendeten Schlüssel.

Symmetrisch: Ein-Schlüssel bzw. **Secret-Key**- (*konventionelle Verschlüsselung*)

Asymmetrisch: Zwei-Schlüssel bzw. **Public-Key**-Verschlüsselung

3. Die Art und Weise, in der der Klartext verarbeitet wird:

- Blockchiffre
- Stromchiffre

Klassifizierung von Angriffen

Art des Angriffs	dem Kryptoanalytiker bekannt
Ciphertext Only	■ Verschlüsselungsalgorithmus und Chiffretext
Known Plaintext	■ Verschlüsselungsalgorithmus und Chiffretext ■ <i>ein oder mehrere Klartext-Chiffretext-Paare, die mit dem geheimen Schlüssel verschlüsselt wurden</i>
Chosen Plaintext	■ Verschlüsselungsalgorithmus und Chiffretext ■ <i>Klartextnachricht, die vom Kryptoanalytiker gewählt wurde, zusammen mit dem zugehörigen Chiffretext, der mit dem geheimen Schlüssel verschlüsselt wurde.</i>
Chosen Ciphertext	■ Verschlüsselungsalgorithmus und Chiffretext ■ <i>Chiffretext, der vom Kryptoanalytiker gewählt wurde, zusammen mit dem zugehörigen entschlüsselten Klartext, der mit dem geheimen Schlüssel entschlüsselt wurde.</i>
Chosen Text	■ Verschlüsselungsalgorithmus und Chiffretext ■ <i>vom Kryptoanalytiker gewählte Klartextnachricht, zusammen mit dem zugehörigen Chiffretext, der mit dem geheimen Schlüssel verschlüsselt wurde.</i> ■ <i>vom Kryptoanalytiker gewählter Chiffretext zusammen mit dem entsprechenden entschlüsselten Klartext, der mit dem geheimen Schlüssel erzeugt wurde.</i>

Das Ziel ist es immer den Schlüssel zu ermitteln, damit man weitere Kommunikation effektiv entschlüsseln kann.

Sicherheit von Verschlüsselungsschemata

Bedingungslos Sicher (*Unconditionally Secure*)

- Unabhängig davon wie viel Zeit ein Gegner hat, ist es ihm unmöglich, den Geheimtext zu entschlüsseln, weil die erforderlichen Informationen nicht vorhanden sind.

Rechnerisch Sicher (*Computationally Secure*)

- Die Kosten für das Brechen der Chiffre übersteigen den Wert der verschlüsselten Informationen.
- Die zum Knacken der Chiffre benötigte Zeit übersteigt die Lebensdauer der Informationen.

? Frage

Wie lange könnte der Nutzen einer bestimmten Information andauern?

Kryptoanalyse

Kryptoanalyse

- Der Angriff beruht auf den Eigenschaften des Algorithmus und einer gewissen Kenntnis der allgemeinen Merkmale des Klartextes.
- Der Angriff nutzt die Eigenschaften des Algorithmus aus, um zu versuchen, einen bestimmten Klartext zu entschlüsseln oder den verwendeten Schlüssel zu ermitteln.

Brute-Force Angriff

- Es werden alle möglichen Schlüssel ausprobiert, bis eine verständliche Übersetzung des Chiffriertextes in Klartext erreicht wird.
- Im Durchschnitt muss die Hälfte aller möglichen Schlüssel ausprobiert werden, um Erfolg zu haben.
- Zur Durchführung des Brute-Force-Ansatzes ist ein gewisses Maß an Wissen über den zu erwartenden Klartext erforderlich. Es werden Mittel zur automatischen Unterscheidung von Klartext und „Müll“ benötigt.

? Frage

Was bedeutet somit *bis eine verständliche Übersetzung des Chiffriertextes in Klartext erreicht wird*?

Wie können Sie feststellen ob Sie erfolgreich entschlüsselt haben, wenn der Klartext zum Beispiel ein Bild, ein Video oder ein Computerprogramm ist?

Wie können Sie feststellen, ob Sie erfolgreich entschlüsselt haben, wenn die Datei zweifach (d. h. mit zwei verschiedenen Schlüsseln) verschlüsselt wurde?

2. Substitutions-Chiffren

Substitutionsverfahren - Allgemeine Vorgehensweise

- Bei der Substitution werden die Buchstaben des Klartextes durch andere Buchstaben oder durch Zahlen oder Symbole ersetzt.
- Wenn der Klartext als eine Folge von Bits betrachtet wird, beinhaltet die Substitution das Ersetzen von Bitmustern des Klartextes durch Bitmuster des Geheimtextes.

Cäsar-Chiffre

- Einfachste und früheste bekannte Verwendung einer Substitutions-Chiffre; verwendet von Julius Cäsar.
- Dabei wird jeder Buchstabe des Alphabets durch einen Buchstaben ersetzt, der drei Stellen weiter hinten im Alphabet steht.
- Am Ende des Alphabets wird wieder am Anfang begonnen. Somit folgt auf den Buchstabe Z der Buchstabe A.

unverschlüsselt: meet me after the toga party

verschlüsselt: PHHW PH DIWHU WKH WRJD SDUWB

Cäsar-Chiffre: historische Verwendung

Die Transformation kann mit folgender Tabelle ausgedrückt werden:

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

Mathematisch, wenn wir jedem Buchstaben einen Wert zuweisen:

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
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

Der Algorithmus zur Verschlüsselung ist dann (p sei der Wert des zu verschlüsselnden Buchstabens):

$$Y = E(3,p) = (p + 3) \bmod 26$$

Verallgemeinerter Cäsar-Chiffre-Algorithmus

Eine Verschiebung (k) kann beliebig groß sein, so dass der allgemeine Cäsar-Algorithmus lautet:

$$Y = E(k, p) = (p + k) \bmod 26$$

Wobei k einen Wert im Bereich von 1 bis 25 annimmt; der Entschlüsselungsalgorithmus ist einfach:

$$p = D(k, Y) = (Y - k) \bmod 26$$

Brute-Force-Kryptoanalyse der Cäsar-Chiffre

Key	PHHW PH DIWHU WKH WRJD SDUWB (Ciphertext)
1	oggv og chvgt vjg vqic rctva
2	nffunf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydr cpr fcr mey nyprw
6	jbbq jbx cqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fxtymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsj lq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvj uh jxu j ewq fqhjo
...	
25	qiixqi ejxiv xli xske tevxc

Brute-Force-Kryptoanalyse (z. B. der Caesar-Chiffre)

Die Entschlüsselung ist komplizierter, wenn der Klartext bereits eine sehr hohe Entropie aufweist, wie z. B. im Falle einer komprimierten ZIP Datei:

00000000:	504b	0304	1400	0000	0800	afb1	4257	1da9	PK.....BW..
00000010:	b0b9	4b00	0000	4f04	0000	0800	1c00	6465	..K...O.....de
00000020:	6d6f	2e74	7874	5554	0900	036a	241b	65a4	mo.txtUT...j\$.e.
00000030:	a9c0	6575	780b	0001	04f8	0100	0004	1400	..eux.....
00000040:	0000	edcc	db09	8030	0c05	d07f	a7c8	049d	0.....
00000050:	a28b	c4f6	6203	e983	18d0	6e2f	ee91	ffc3	b.....n/....
00000060:	c928	b697	cb1c	2437	f569	a032	fb52	29ec	.(....\$7.i.2.R).
00000070:	a8f4	340c	f206	5aca	321c	afff	8cd5	c075	..4...Z.2.....u
00000080:	d3c5	762a	d291	2389	2492	48d2	0750	4b01	..v*...#.\$..H..PK.
00000090:	021e	0314	0000	0008	00af	b142	571d	a9b0	BW...
000000a0:	b94b	0000	004f	0400	0008	0018	0000	0000	.K...O.....
000000b0:	0001	0000	00ff	8100	0000	0064	656d	6f2e	demo.
000000c0:	7478	7455	5405	0003	6a24	1b65	7578	0b00	txtUT...j\$.eux..
000000d0:	0104	f801	0000	0414	0000	0050	4b05	0600	PK...
000000e0:	0000	0001	0001	004e	0000	008d	0000	0000	N.....
000000f0:	00								

? Frage

Wie kann man - wenn man weiss, dass es sich um eine ZIP Datei handelt - die Caesar-Chiffre knacken?

Monoalphabetische Chiffren

- Eine Permutation einer endlichen Menge von Elementen S ist eine geordnete Folge aller Elemente von S , wobei jedes Element genau einmal vorkommt.



Beispiel

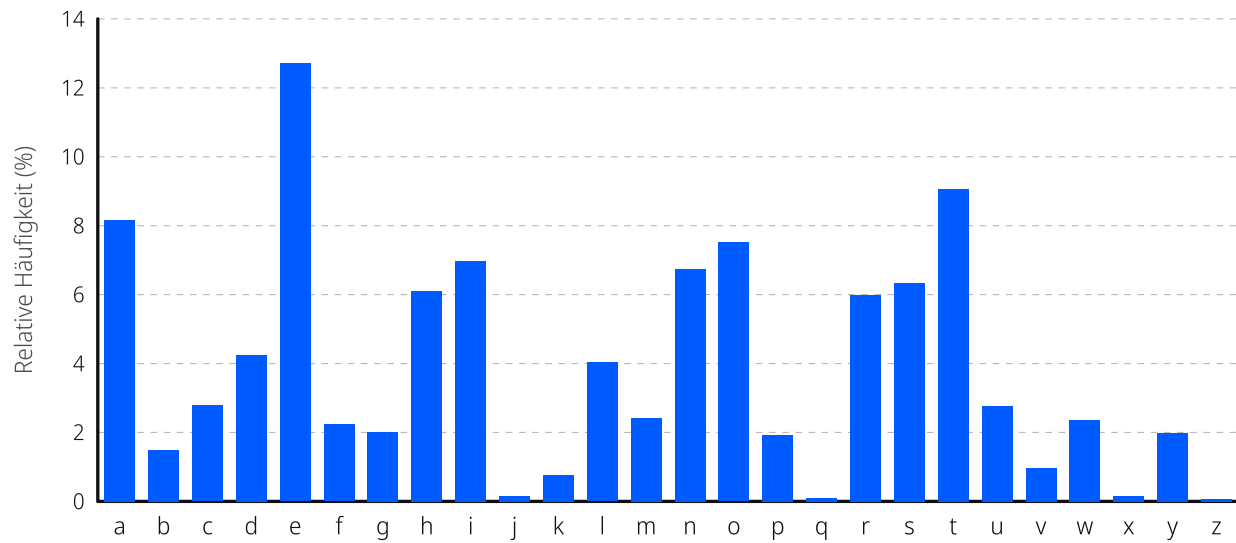
Zeichen	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ersetzung	d	f	v	e	n	k	i	b	s	p	t	q	l	w	u	c	x	r	j	g	z	m	a	h	y	o

Erzeugung einer beliebigen Permutation der 26 Buchstaben mit Python

```
from random import shuffle
alphabet=["a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v",
shuffle(alphabet)
print(alphabet)
```

- Wenn die „Chiffre“-Zeile (siehe Cäsar-Chiffre) eine beliebige Permutation der 26 alphabetischen Zeichen sein kann, dann gibt es $26!$ (*26 Fakultät*) oder mehr als $4 \cdot 10^{26}$ mögliche Schlüssel.
 - Dies ist um 10 Größenordnungen größer als der Schlüsselraum des Verschlüsselungsalgorithmus DES!
 - Der Ansatz wird als monoalphabetische Substitutions-Chiffre bezeichnet, da pro Nachricht ein einziges Chiffre-Alphabet verwendet wird.

Angriffsvektor: Häufigkeit der (hier: englischen) Buchstaben[1]



[1] Analyse des Concise Oxford Dictionary (9th edition, 1995) – <https://www.nd.edu>

Angriffe auf Monoalphabetische Chiffren

Sie sind leicht zu knacken, da sie die Häufigkeitsdaten des ursprünglichen Alphabets widerspiegeln.

Die Gegenmaßnahme besteht darin, mehrere Substitute (Homophone) für einen einzigen Buchstaben anzubieten.

Playfair Cipher

Erfunden vom britischen Wissenschaftler Sir Charles Wheatstone im Jahr 1854.



Bemerkung

Digram

- Zwei-Buchstaben-Kombination
- am häufigsten im Englischen: "th"

Trigram

- Drei-Buchstaben-Kombination
- am häufigsten im Englischen: "the"

- Bekannteste Chiffrierung mit mehreren Buchstaben.
- Behandelt Digramme im Klartext als einzelne Einheiten und übersetzt diese Einheiten in Digramme des Geheimtextes.
- Basiert auf der Verwendung einer 5 x 5 Buchstabenmatrix, die mit Hilfe eines Schlüsselworts konstruiert wird.
- Wurde von der britischen Armee im Ersten Weltkrieg und von der US-Armee und anderen alliierten Streitkräften im zweiten Weltkrieg als Standardfeldsystem verwendet.

Playfair Key Matrix

Füllen Sie die Buchstaben des Schlüsselworts (abzüglich der Duplikate) von links nach rechts und von oben nach unten aus, dann füllen Sie den Rest der Matrix mit den restlichen Buchstaben in alphabetischer Reihenfolge aus. Die Buchstaben I und J zählen als ein Buchstabe.

Sei das Schlüsselwort MONARCHY:

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

Playfair Verschlüsselung

Die Verschlüsselung wird für jedes Buchstabenpaar des Klartextes durchgeführt.

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

1. Wenn beide Buchstaben gleich sind (oder nur ein Buchstabe übrig ist), fügen Sie ein x hinter dem ersten Buchstaben ein. Verschlüsseln Sie das neue Paar und fahren Sie fort (z. B. würde `ballon` als `ba 1X lo nX` verschlüsselt werden).
2. Wenn die Buchstaben in der gleichen Zeile stehen, ersetzen Sie sie durch die Buchstaben unmittelbar rechts davon (ggf. umbrechen) (z. B. wird `ar` als `RM` verschlüsselt).
3. Tauchen die Buchstaben in derselben Spalte auf, so sind sie durch die unmittelbar darunter liegenden Buchstaben zu ersetzen (ggf. umbrechen) (z. B. wird `mu` als `CM` verschlüsselt).
4. Befinden sich die Buchstaben nicht in derselben Zeile oder Spalte, so werden sie durch die Buchstaben in derselben Zeile bzw. in dem anderen Paar von Ecken des durch das ursprüngliche Paar definierten Rechtecks ersetzt (z. B. `hs` $\rightarrow$ `BP`; `ea` $\rightarrow$ `IM`).

Hill Chiffre

Entwickelt von dem Mathematiker Lester Hill im Jahr 1929.

- Die Stärke ist, dass die Häufigkeit von einzelnen Buchstaben vollständig ausgeblendet wird.
 - Durch die Verwendung einer größeren Matrix werden mehr Frequenzinformationen verborgen.
 - Eine 3 x 3 Hill-Chiffre verbirgt nicht nur die Häufigkeiten einzelner Buchstaben sondern auch von Digrammen.
- Stark gegen einen Angriff auf den Geheimtext, aber leicht zu brechen sobald ein Klartext vorliegt (*known plaintext attack*).

Polyalphabetische Chiffren

© Bemerkung

Alle diese Techniken haben die folgenden Merkmale gemeinsam:

- Es wird ein Satz verwandter monoalphabetischer Substitutionsregeln verwendet.
- Ein Schlüssel bestimmt, welche bestimmte Regel für eine bestimmte Umwandlung gewählt wird.

Polyalphabetische Substitutions-Chiffren verbessern einfache monoalphabetische Chiffren, indem sie verschiedene monoalphabetische Substitutionen verwenden, während man die Klartextnachricht verschlüsselt.

Vigenère Chiffre

- Die bekannteste und eine der einfachsten polyalphabetischen Substitutions-Chiffren.
- In diesem Schema besteht die Menge der verwandten monoalphabetischen Substitutionsregeln aus den 26 Cäsar-Chiffren mit Verschiebungen von 0 bis 25.
- Jede Chiffre wird durch einen Schlüsselbuchstaben identifiziert, der den Klartextbuchstaben durch den Chiffretextbuchstaben ersetzt.

Aufbau des Vigenère-Tableaus

- Kopfzeile:
Klartextbuchstabe
- 1. Spalte:
Schlüsselbuchstabe
- Tableau: Verschlüsselter Buchstabe

Beispiel

Sei der Schlüssel **D** und der Klartextbuchstabe **b**, dann ist der Chiffretextbuchstabe **E**.

/	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

Beispiel einer Vigenère-Verschlüsselung

- Um eine Nachricht zu verschlüsseln, wird ein Schlüssel benötigt, der so lang ist wie die Nachricht.
- In der Regel ist der Schlüssel ein sich wiederholendes Schlüsselwort.

Beispiel

Wenn das Schlüsselwort `deceptive` ist, wird die Nachricht: `We are discovered save yourself`, wie folgt verschlüsselt:

Schlüssel:	DECEPTIVEDECEPTIVEDECEPTIVE
Klartext:	wearediscoveredsaveyourself
Geheimtext:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Vigenère *Autokey System*

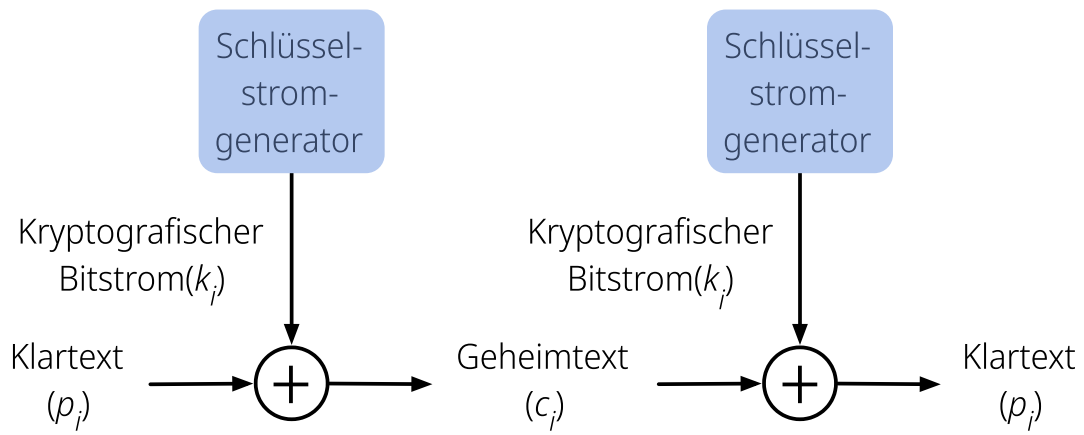
Ein Schlüsselwort wird mit dem Klartext selbst verkettet, um einen laufenden Schlüssel zu erhalten.

Beispiel

Schlüssel:	DECEPTIVEwearediscoveredsav
Klartext:	wearediscoveredsaveyourself
Geheimtext:	ZICVTWQNGKZEIIGASXSTSLVVWLA

Auch dieses Verfahren ist anfällig für eine Kryptoanalyse, da der Schlüssel und der Klartext die gleiche Häufigkeitsverteilung der Buchstaben aufweisen und eine statistische Technik angewendet werden kann.

Vernam Chiffre



One-Time Pad

- Verbesserung der Vernam-Chiffre, vorgeschlagen von dem Offizier Joseph Mauborgne des Army Signal Corp.
- Verwendung eines Zufallsschlüssels, der so lang wie die Nachricht ist, so dass der Schlüssel nicht wiederholt werden muss.
- Der Schlüssel wird zum Ver- und Entschlüsseln einer einzigen Nachricht verwendet und dann verworfen.
- Jede neue Nachricht erfordert einen neuen Schlüssel mit der gleichen Länge wie die neue Nachricht.
- Das Schema ist nachweislich nicht zu knacken.
 - Erzeugt eine zufällige Ausgabe, die in keinem statistischen Zusammenhang mit dem Klartext steht.
 - Da der Chiffriertext keinerlei Informationen über den Klartext enthält, gibt es keine Möglichkeit, den Code zu knacken.

Schwierigkeiten von One-Time-Pads

- Das One-Time-Pad bietet vollständige Sicherheit, hat aber in der Praxis zwei grundlegende Schwierigkeiten:

1. Es gibt das praktische Problem der Herstellung großer Mengen von Zufallsschlüsseln.

Jedes stark genutzte System würde regelmäßig Millionen von zufälligen Zeichen benötigen.

2. Ein „gigantisches“ Schlüsselverteilungsproblem

Für jede zu übermittelnde Nachricht benötigen Sender und Empfänger einen gleich langen Schlüssel.

- Aufgrund dieser Schwierigkeiten ist das One-Time-Pad nur von begrenztem Nutzen; es eignet sich vor allem für Kanäle mit geringer Bandbreite, die eine sehr hohe Sicherheit erfordern.
- Das One-Time-Pad ist das einzige Kryptosystem, das eine perfekte Geheimhaltung bietet.

3. Transpositions-Chiffren

Rail Fence Chiffre

- Einfachste Transpositions-Chiffre (d. h. Chiffre basierend auf *Vertauschung*).
- Der Klartext wird als eine Folge von Diagonalen aufgeschrieben und dann als eine Folge von Zeilen abgelesen.

Beispiel

Um die Nachricht: „Meet me after the Toga-Party“ mit einer Rail Fence Chiffre der Tiefe 2 (Schlüssel) zu verschlüsseln, würden wir schreiben:

m e m a t r h t g p r y

e t e f e t e o a a t

Die verschlüsselte Nachricht ist: MEMATRHTGPRYETEFETEOAAT

Um die Nachricht zu entschlüsseln, konstruieren Sie eine *Railfence* mit der entsprechenden Tiefe und Länge des Chiffretexts. Danach können Sie die Nachricht direkt ablesen.

Geben Sie die folgende Nachricht: v o e o d r g y und der Schlüssel sei 4.

Nachricht	v	o	e	o	d	r	g	y
Index	1	2	3	4	5	6	7	8

1. Railfence der Tiefe 4 für eine Nachricht der Länge 8.

-
- -
- -
-

2. Daraus ergibt sich unmittelbar welcher Buchstabe an welcher Stelle im Chiffretext gelandet ist (wir numerieren einfach die Platzhalter zeilenweise durch):

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

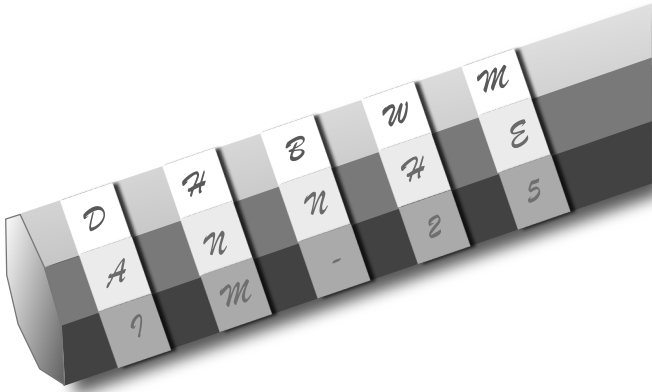
3. Ersetzen des Index mit dem Buchstaben aus der verschlüsselten Nachricht:

- 1 ⇒ v 2 ⇒ o
- - 3 ⇒ e 4 ⇒ o 5 ⇒ d
- 6 ⇒ r 7 ⇒ g
- 8 ⇒ y

Plaintext = very good

Skytale

- Ältestes bekannte (militärische) Verschlüsselungsverfahren.
- Vor mehr als 2500 Jahren (vermutlich) von den Spartanern entwickelt.
- Die Verschlüsselung erfolgte mit einem (Holz-)Stab mit einem bestimmten Durchmesser („Schlüssel“) (Skytale).



Zeilenverschiebungs-Chiffre

- Ist eine komplexere Transposition.
- Vorgehen: Schreiben Sie die Nachricht zeilenweise in ein Rechteck mit wohldefinierter Breite und lesen Sie die Nachricht spaltenweise ab, aber vertauschen Sie die Reihenfolge der Spalten.
- Die Reihenfolge der Spalten ist dann der Schlüssel.

📄 Beispiel: Verschlüsselung von: `attack postponed until two am`

Schlüssel:	4312567
Klartext:	attackp ostpone duntilt woamxyz
Geheimtext:	TTNA APTM TSUO AODW COIX KNLY PETZ
Spalte:	3--- 4--- 2--- 1--- 5--- 6--- 7---

-
- Zeilenverschiebungs-Chiffre = 🇺🇸 *Row Transposition Cipher*
 - Wenn der Schlüssel 4312567 ist, dann wird:
 - die erste Spalte wird als die *vierte* (4),
 - die zweite Spalte als die *dritte* (3),
 - die dritte Spalte als die *erste* (1),
 - ...geschrieben
 - Beim Entschlüsseln ergibt sich die Anzahl der Reihen trivial aus der Länge der Nachricht (28 Zeichen) und der Länge des Schlüssels (7 Zeichen); $28/7 = 4$.
 - xyz am Ende der Nachricht sind nur Platzhalter (*Padding*), um die letzte Zeile zu füllen, damit die Nachricht in ein Rechteck passt. Sie werden bei der Entschlüsselung einfach ignoriert.

4. Steganografie

Text-basierte Steganografie

4.1. Entschlüsseln

Dear Friend ; We know you are interested in receiving cutting-edge announcement . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1626 ; Title 4 , Section 305 . This is a legitimate business proposal ! Why work for somebody else when you can become rich in 96 months . Have you ever noticed nobody is getting any younger & nobody is getting any younger . Well, now is your chance to capitalize on this ! We will help you decrease perceived waiting time by 170% and use credit cards on your website ! You are guaranteed to succeed because we take all the risk ! But don't believe us . Mrs Anderson of Indiana tried us and says "I was skeptical but it worked for me" . We assure you that we operate within all applicable laws . You will blame yourself forever if you don't order now . Sign up a friend and you'll get a discount of 10% ! Thank-you for your serious consideration of our offer !

Mit Spammimic <https://www.spammimic.com/>, kann die Nachricht extrahiert werden.

Auswahl anderer Steganographie-Techniken

Zeichenmarkierung:

Ausgewählte Buchstaben eines gedruckten oder maschinengeschriebenen Textes werden mit Bleistift überstrichen. Die Markierungen sind nur sichtbar, wenn das Papier schräg in helles Licht gehalten wird.

Unsichtbare Tinte: Es gibt eine Reihe von Substanzen, die zum Schreiben verwendet werden können, aber keine sichtbaren Spuren hinterlassen, solange das Papier nicht erhitzt oder mit einer chemischen Substanz behandelt wird.

Nadelstiche: Kleine Nadelstiche auf ausgewählten Buchstaben sind normalerweise nicht sichtbar, es sei denn, das Papier wird vor ein Licht gehalten.

Sehr helle Tinte: Druckerhersteller drucken winzige Punktmuster in sehr hellen Farben auf die Seiten. Dies erlaubt es Dokumente zu dem Drucker zurückzuverfolgen, auf dem sie gedruckt wurden.

Steganographie vs. Verschlüsselung

■ Steganografie hat eine Reihe von *Nachteilen* im Vergleich zur Verschlüsselung:

- ✗ Es erfordert einen hohen Overhead, um relativ wenige Bits an Informationen zu verbergen.
- ✗ Sobald das System entdeckt wird, wird es praktisch wertlos.

■ Der *Vorteil* der Steganografie:

- ★ Sie kann von Parteien eingesetzt werden, die etwas zu verlieren haben, wenn allein die Tatsache ihrer geheimen Kommunikation (unabhängig vom Inhalt) entdeckt wird.
- ★ Verschlüsselung kennzeichnet den Verkehr als wichtig oder geheim oder kann den Sender oder Empfänger als jemanden identifizieren, der etwas zu verbergen hat.



Übung

4.2. Playfair Chiffre

Entschlüsseln Sie: XGAWMGAZ. Das Passwort ist MONARCHY (wie auf den Folien.)

4.3. Vigenère Chiffre

Sie haben das folgende Klartext-Chiffretext-Paar:

P: secret

C: HSFGSW

1. Wie ist der Schlüssel?
2. Welche Art von Angriff haben Sie durchgeführt?



Übung

4.4. Rail-fence Chiffre

Entschlüsseln Sie: gestugmitrtee

D. h. finden Sie den Schlüssel k.

4.5. Rail-fence Chiffre

Verschlüsseln Sie "i love crypto" mit dem Schlüssel/der Tiefe 3. (Ignorieren Sie Leerzeichen.)

Übung

4.6. Zeilenverschiebungs-Chiffre

Sie haben die folgende Nachricht erhalten:

YSFRITTUNCOSPJU

Außerdem konnten Sie den Schlüssel bis auf einen Wert ermitteln: 4153.

- a. Wie viele Entschlüsselungsmöglichkeiten gibt es (noch)?
- b. Bestimmen Sie den richtigen Schlüssel und entschlüsseln Sie den Text?

4.7. Eigenschaften von Chiffren

1. Wie unterscheiden sich Transpositions- und Substitutions-Chiffren?
2. Handelt es sich bei Monoalphabetischen Chiffren um Transpositions- oder Substitutions-Chiffren?
3. Kann man Transpositions- und Substitutions-Chiffren kombinieren?

