GEHEIME BOTSCHAFTEN

Eine kleine Einführung in das Codieren von Texten

Seit jeher wurden wichtige Botschaften verschlüsselt. Z.B. auch von Julius Caesar (60 v.Chr.)

1 Geheime Beispiel-Botschaften in verschiedenen Jahrhunderten:

Geheimtext 1: B N D R A N N O E T N X E T E T U I A C O R E X K E W E G X

Geheimtext 2: 

Geheimtext 3: U S A K K A L X P M M N P O C Y

Geheimtext 4: L W M T P C N Y L Z N D P A M I F E

Geheimtext 5: k,lw?jb?iwwitj.?efbnzjtwmwbeundefinedxnceg

Geheimtext 6: 610 203 1712 1323 2424 1411 1611 203 3720

Können wir diese Botschaften irgendwie entschlüsseln?

Wie könnte man ansetzen?

Welche Verschlüsselungsprinzipien können wir erkennen?

2 Der Unterschied zwischen Codieren und Chiffrieren:

Es gibt verschiedene Möglichkeiten eine Nachricht zu verschlüsseln.

2.1 Codieren:

Man ersetzt Wörter z. B. durch Symbole oder andere Wörter.
Bsp: Ψ e x (Ψ =König e=übermorgen x=ermorden)
Diese Codesymbole werden in einem Codebuch aufbewahrt.
Vorteil: Völlig freie Wahl der Symbole. Schwer entschlüsselbar.
Nachteil 1: Wenn dieses Codebuch in fremde Hände gerät, kann man damit die Geheimbotschaften entziffern.
Nachteil 2: Nur diejenigen Themen können vermittelt werden, zu denen man im Voraus Codes abgemacht hat.

2.2 Chiffrieren:

Man ersetzt einzelne Buchstaben durch andere Buchstaben / Symbole.
Vorteil gegenüber Codes: Man kann vielfältigere Themen kommunizieren. Man braucht „nur“ ein Chiffreverfahren, kein Codebuch.
Nachteil wie bei Codes: Wenn das Verfahren / Codewort in fremde Hände fällt ist die Chiffre schnell entschlüsselt.

3 Ausgewählte Chiffren im Laufe der Zeit

3.1 Eine Transpositions Chiffre (ca. 470 v.Chr.)

B	A	U	M
2	1	4	3
h	a	l	l
o	e	m	p
f	a	e	n
g	e	r	x

Codewort Baum
alphabetische Reihenfolge der Buchstaben

Klartext: Hallo empfaenger

Geheimtext Spaltenweise notieren:

GT: ?

1. Aufgabe: Geheimtext (GT): _____

Lösung: GT: a e a e h o f g l p n x l m e r

3.1.1 Überschlüsselung

Wenn man einen Geheimtext erneut verschlüsselt, nennt man dies eine Überschlüsselung.

Man kann z.B. den erhaltenen Geheimtext mit einem zweiten Codewort ein zweites Mal Transponieren. Doppelte Transposition.
Noch effektiver (aber auch aufwendiger) ist es, wenn man den erhaltenen Geheimtext mit einer zweiten Methode überschlüsselt.

3.2 Die Schiebe-Cäsar Chiffre

Beim Chiffrieren wird das Klar-Alphabet (KA) durch ein Geheimalphabet (GA) ersetzt.

KA	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
GA	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

Klartext (KT): hallo (KT z.B. in Kleinbuchstaben darstellen)
Geheimtext (GT): JCNNQ (GT z.B. in Grossbuchstaben darstellen)

Dieses Beispiel ist eine einfache Buchstabenverschiebung um + 2 Buchstaben nach Vorne.
Man nennt es darum einen „**Schiebecäsar**“, nach Julius Cäsar (ca. 60 v.Chr.)

Klartext: koenig wird ermordet
Geheimtext: mqgpki yktf gtoqtfgv

2. Aufgabe: Schiebe-Caesar – Verschlüsselung (ca. 60 v. Chr.) mit +2

Klartext: diktator bei vollmond ermorden

Geheimtext? _____

3. Aufgabe: Wie viele mögliche Verschlüsselungen gibt es beim Schiebe Cäsar?

4 Verschlüsselungsprinzipien:

Die Grundlegenden Prinzipien, wie man Texte verschlüsselt, wurden im Laufe der Geschichte stets raffinierter. Je nach Fortschritt der Mathematik und der Technik ergaben sich neue Ansätze.

Verschlüsselungs-Prinzip	**Entwickelt von wem:**	**Name des Verfahrens Ein Beispiel**
Transposition Vertauschung von Zeichen	470 v.Chr. Griechen	(Doppel-) Transpositionsverfahren Angriffspunkte: Häufige Wörter erkennen, geschicktes Probieren, …
Substitution Ersetzung von Zeichen	60 v.Chr. Cäsar	Cäsar-Verfahren Angriffspunkte: Häufigkeitsverteilung, Bigramme, …
Polyalphabetisch (= Homophon) Ein gleiches Zeichen wird verschieden verschlüsselt	1600 Blaise de Vigenère	Homophone Chiffre: Vigenère-Verschlüsselung, Enigma im II.Weltkrieg Angriffspunkte: Bigramme, Trigramme,
Häufigkeiten verschleiern mit Buchstabenpaaren, homophone Ersetzung	1650	(Agenten-) Handchiffre 5x5 Angriffspunkte: Bigramme, Trigramme, Doppelte Buchstaben
Häufigkeiten verschleiern mit Buchstabenpaaren	1854 Charles Wheatstone	Playfair-Methode im 5x5 Quadrat Angriffspunkte: Bigramme, Trigramme, Doppelte Buchstaben
Kerckhoffs' Prinzip Codewort soll geheim sein, nicht aber das Verfahren	1900 Kerkhoff	Kerkhoff Prinzip
Einmaliges Codewort	1918 Gilbert Vernam	One Time Pad Vorteil: Keine mathematischen Angriffspunkte Nachteil: Aufwändig, Schlüsselübergabe unsicher
Öffentlicher Schlüssel Public Key Verschlüsselung	1977 Rivest Shamir, Adelman	RSA-Verfahren Schwäche: Primzahlen finden mit Rechnergeschwindigkeit

… und viele Geheimcodes und Chiffren mehr …

4.1 Die allgemeine Cäsar-Chiffre

Nun wird ein beliebiges GA mit Hilfe eines geheimen Codewortes „Fuchshetzjagd“ definiert. Die restlichen fehlenden Buchstaben werden hinten in ihrer Reihenfolge ergänzt.

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

4. Aufgabe: Wie viele mögliche Verschlüsselungen gibt es, wenn anstatt einer reinen Alphabet Verschiebung eine beliebige Permutation (Vertauschung) als Geheimalphabet benutzt werden kann?

5. Aufgabe: Warum ist es im Beispiel des GA im Punkt 3.3 sinnvoll, wenn im Codewort mindestens ein hinterer Buchstabe wie x, y, oder z vorkommt?

4.2 Handchiffre mit 5 x 5 Quadrat und „homophone“ Ersetzung

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

der buchstabe a als beispiel wird beliebig (zufällig) durch eines der folgenden buchstabenpaare der selben zeile und spalte substituiert:

a = md mi mg mz pd pi pg pz ed ei eg ez nd ni ng nz

jeder buchstabe hat jeweils 16 solche verschiedene homophone

H O M O P H O N E	E R S E T Z U N G	Z E I L E	S P A L T E
D A S	I S T	E I N	G E H E I M E R	T E X T	F G	G R I P
rg ez ik	la co dy	mh lg et	ui nf sw mj lg ao pw dp	dy aj zs db	rh kd	zu fv ld mr

Diese Handchiffre scheint „einfach und stark“ .

Vorteile:
Nachteile:

6. Aufgabe: Begründe warum jeder Buchstabe 16 verschiedene Kodierungen hat. Wie viele Möglichkeiten ergäben sich für eine Kodierung eines Buchstabens mit einem 8x8 Quadrat und 64 verschiedenen Zeichen darin?

Methode von Playfair (ca. 1854):
Quelle: https://www.informatik.uni-leipzig.de/~meiler/Schuelerseiten.dir/BLuebeck/playfair.html

Um 1854 erfand der Physiker Charles Wheatstone eine Chiffre, bei der nicht Buchstaben sondern Buchstabengruppen verschlüsselt werden. Baron Playfair von St.Andrews, ein Freund Wheatstones, veröffentlichte es später unter seinem Namen.

Fall 1 Beide Buchstaben liegen in der selben Reihe: Jeder Buchstabe wird verschlüsselt, indem er durch den nächstfolgenden der selben Zeile ersetzt wird. Handelt es sich beim Klartextbuchstaben um den letzten der Zeile, wird mit dem Ersten der Zeile verschlüsselt.

Fall 2 Beide Buchstaben liegen in der selben Spalte: Jeder Buchstabe wird verschlüsselt, indem er durch den unter ihm stehenden der selben Spalte ersetzt wird. Handelt es sich beim Klartextbuchstaben um den Untersten der Spalte, wird er mit dem Obersten der Spalte verschlüsselt.

Fall 3 Beide Buchstaben liegen weder in der selben Reihe noch in der selben Spalte: Man geht in der Zeile des ersten Klarbuchstaben nach rechts oder links zur Spalte des zweiten Buchstaben. Der dort stehende Buchstabe ist die Chiffre für diesen. Mit dem zweiten Buchstaben wird ebenso verfahren. Die Entschlüsselung erfolgt ebenso, nur mit umgekehrter Richtung, statt nachfolgend wird vorangehend, statt darunter stehend wird darüber genommen. Allein im dritten Fall kann genau so verfahren werden wie bei der Verschlüsselung.

4.2.1 Beispiel Playfair: 5 x 5 Quadrat mit Codewort „Extrawurst“

Das Quadrat wird mit dem Codewort aufgefüllt. Doppelt vorkommende Buchstaben werden weggelassen. Die restlichen Quadratfelder werden mit den restlichen Buchstaben des Alphabets aufgefüllt.

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

```
Klartext:     mrx kauft am mittwoch

Zerlegung:    mr  xk au ft am mi tx tw oc hx

Geheimtext:   nt  le cx gx to og rt eb yi fr
```

Der entstehende Chiffretext weist die normalen Häufigkeiten der natürlichen Sprache nicht mehr auf, da die Verteilung der Buchstabenpaare gleichmäßiger ist als die der Einzelbuchstaben. Dennoch kann auch dieses Verfahren gebrochen werden, wenn genügend auf gleiche Weise verschlüsselter Text zur Verfügung steht. Der besondere Vorteil des Verfahrens liegt aber darin, dass mit einer Entschlüsselung eines Teiles der Chiffre noch nicht auf den ganzen Klartext geschlossen werden kann.

5 Geheimcodes „knacken“:

Einen Geheimtext zu dechiffrieren ohne Wissen um den Schlüssel ist schwierig. (Falls man keinen gegnerischen Agenten fangen, ihn zur Herausgabe des Codes „überreden“ kann) nutzt man z.B. Häufigkeitsanalysen, Bigramme, Trigramme, geschicktes Raten, fingierte bekannte Botschaften vom Gegner verschlüsseln lassen und abfangen, grosse Beispielgeheimtexte, etc.

5.1 Häufigkeitsanalyse

Entschlüssle den Geheimtext 1 mit Hilfe einer Häufigkeitsanalyse. Nutze die Häufigkeitsverteilung der deutschen Buchstaben in Tabelle 1 im Anhang.
Hilfreich ist es, wenn man sich das Klaralphabet (KA) aufschreibt und darunter nach und nach das Geheimalphabet (GA) ergänzt. Falls Leerzeichen , d.h. Wörter) erkennbar sind, kann man kurze Wörter erraten.

KA	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
GA																										

Geheimtext 1:

ojijw mfy ifx wjhmy fzk inj kwjnj jsykfqyzsl xjnsjw ujwxtjsqnhmpjny

Falls die Leerzeichen mitverschlüsselt wurden, kann man das Leerzeichen als häufigstes Zeichen herausfinden.

Geheimtext 2:

oqtigpuvwpfbjcvbiqnfbkobowpfbfcubkuvbgkpgbuejykgtkigbcwhicdgbfgppbj kgtbygtfgpbcwejbrwpmvbwpfbmqoocbokvxgtuejqdgpbwpfbfcokvbfgtbvgzv bncgpigtbyktfbmqoovbjkgtbpqejbgkpbucv?

Tipp : Falls beim Geheimtext 2 die Leerzeichen mitverschlüsselt wurden ist das häufigste Zeichen dieses Leerzeichen. Finde es zuerst mit einer Häufigkeitsanalyse heraus. (Hier ist ein Programm zur Häufigkeitsanalyse: http://www.matheprisma.de/Module/Caesar/index.htm)

5.2 Bigramme, Trigramme

Im Anhang sind auch die Wahrscheinlichleiten von Bigrammen, Trigrammen zu entnehmen.
Mit Computerunterstützung ist die Auswertung eines Geheimtextes gut möglich.
Hat man ein Bigramm entschlüsselt, fallen weitere Schritte leichter.

6 Aufgaben:

7. Aufgabe: Überlege Dir weitere Stärken und Schwächen vom Codieren bzw. Chiffrieren.

8. Aufgabe: Möglichst vielseitiges Codebuch entwickeln
Stelle ein kleines Codebuch zusammen, in dem Du für einige wesentliche Wörter Symbole erfindest. Dieses geheime Codebuch hat der Sender und der Empfänger. Es soll für einen Spion in einer Technikfirma seine Dienste leisten, um zu einem Kontaktmann via Brief / mail unauffällig Kontakt aufzunehmen und Treffpunkte und Zeiten abzumachen. Kannst du mit nur 12 Symbolen möglichst viele Aussagen machen?

Klartextwort / Satz	**Symbol / Geheimwort**	**Klartextwort / Satz**	**Symbol / Geheimwort**
1		7	
2		8	
3		9	
4		10	
5		11	
6		12	

Formuliere einen Abschnitt in einer Geheimbotschaft (Brief/mail) in der der Sender (Spion) Treffpunkt und Zeit für ein Treffen vorschlägt. Der Empfänger (Kontaktmann) soll antworten.

Spion Botschaft:
Kontaktmann Antwort:

9. Aufgabe: Folgender GT ist eine Transpositionschiffre:
Wir nehmen an, wir wissen das Codewort „BLUME“:
Entschlüssle den Geheimtext, in dem Du das Transpositions-Verfahren umkehrst.

GT: B N D R A N N O E T N X E T E T U I A C O R E X K E W E G X

KT: _____

10. Aufgabe: Probiere auf www.sternenwind.ch → Codierung die Funktionsweise des „einfachen Schiebe – Caesarverfahrens“. Prüfe den obigen Geheimtext mit Verschiebung um +2 indem du beim Verschlüsselungsprogramm **secret02** „b“ als Codewort eingibst und den Geheimtext so entschlüsseln lässt. Was stellst du fest?

11. Aufgabe: Nutze secret 02 auf www.sternenwind.ch und entschlüssle den
GT: gi?fjwlm.ktuqnxkbingynlui?u ujbeudvpkcr
KT: _____

Tipp: Codewort ist der Fachausdruck, wenn man Zeichen ersetzt, im Gegensatz zum Codieren.

6.1.1 Weitere Cäsar-Übungsaufgaben:

12. Aufgabe: Wiederholung zum Cäsarverfahren: Gehe auf http://www.matheprisma.de → Cäsar Chiffren und weitere Cäsar Varianten. Studiere die Übungen.

13. Aufgabe: Konstruiere eine Verschlüsselungsmaschine (Schiebe Cäsar-Scheibe) aus Karton / Papier

14. Aufgabe: Erfinde eine eigene einfache Verschlüsselungsmethode.
Tipps: Buchstaben vertauschen, Buchstaben hinzusetzen, . . .

6.1.2 Handchiffre Verfahren:

15. Aufgabe: Verfahren mit Handchiffre und 5x5 Quadrat und homophone Ersetzung.
Codewort ist DORFTISCHLAMPEN
Entschlüssle diesen Geheimtext:

GT: OL FU PW OE RW SA MY PX PH AL CK ED

KT: _____

16. Aufgabe:
Verschlüssle partnerweise einen Text mit der Playfair Methode mit einem selbst ausgedachten Codewort im 5x5 Quadrat

z.B. Klartext: treffen ist mittwoch

Geheimtext: _____

Lösungen:
9) Bekannte Codewoerter taugen nix xx 11) Codewort chiffrieren 15) Treffen Mensa

7 Anhang

7.1 Tabelle 1: Buchstabenhäufigkeiten im Deutschen

E	17,98 %	h	4,61 %	z	1,21 %
N	11,06 %	g	3,25 %	k	1,12 %
i	7,97 %	l	3,19 %	v	0,76 %
s	7,48 %	c	3,17 %	p	0,59 %
r	6,42 %	m	2,47 %	j	0,06 %
a	5,96 %	w	2,03 %	q	0,01 %
t	5,55 %	o	2,00 %	x	0,01 %
d	5,22 %	b	1,77 %	y	0,01 %
u	4,87 %	f	1,23 %		

Die häufigsten 15 Bigramme:

en	4,47 %	de	2,14 %	un	1,73 %
er	3,40 %	in	2,04 %	ge	1,68 %
ch	2,80 %	es	1,81 %	st	1,24 %
nd	2,58 %	te	1,78 %	ic	1,19 %
ei	2,26 %	ie	1,76 %	he	1,17 %

Die 10 häufigsten Trigramme:

ein	1,22 %	der	0,86 %
ich	1,11 %	che	0,75 %
nde	0,89 %	end	0,75 %
die	0,87 %	gen	0,71 %
und	0,87 %	sch	0,66 %

7.2 Tabelle 2: Buchstabenhäufigkeiten im Englischen

e	12.70 %	h	6,09 %	w	2,36 %	k	0.77%
t	9,06 %	r	5,99 %	f	2,23 %	j	0.15%
a	8,17 %	d	4,25 %	g	2,02 %	x	0,15%
o	7,51 %	l	4,03 %	y	1,97 %	q	0,10%
i	6,97 %	c	2,78 %	p	1,93 %	z	0.07%
n	6,75 %	u	2,76 %	b	1,49 %		
s	6,33 %	m	2,41 %	v	0,98 %		

Die häufigsten 10 Bigramme:

th	3,21 %	er	2,13 %	an	1,81%	st	1,22%
he	3,05 %	re	1,90 %	es	1,36%		
in	2,30 %	on	1,83%	ed	1,32%		

Die 10 häufigsten Trigramme:

the	her	tha	eth
ing	ere	nyh	
and	ent	was	

7.3 Lösungen der Beispiel-Geheimtexte

Geheimtext 1: B N D R A N N O E T N X E T E T U I A C O R E X K E W E G X
KT1: Einfache Transposition: , Codewort Blume:
Bekannte Codewoerter taugen nix xx

Geheimtext 2:

KT2: Freimaurercode

Geheimtext 3: U S A K K A L X P M M N P O C Y
KT3: (Playfair, 5x5 abcd.. , Treffen Vollmond))

Geheimtext 4: L W M T P C N Y L Z N D P A M I F E
KT4: Agentenhandchiffre 5x5 , homophon, Monopol ok.

Geheimtext 5: k,lw?jb?iwwitj.?efbnzjtwmwbeundefinedxnceg
KT2: Vigenere: Codewort: sternenwind, vigenere ist ein vielfacher caesar
z.B. auf www.sternenwind.ch → Codieren nachprüfen

Geheimtext 6: 610 203 1712 1323 2424 1411 1611 203 3720
KT5: RSA Verfahren: N=4141 (öffentlich), M=4000 (geheim),
E=23(öffentlich), D=18087 (geheim)
Jeder kann senden
z.B. auf www.sternenwind.ch → Codieren nachprüfen