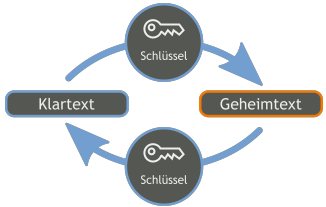
ETH zürich

Klassische Verschlüsselungen

Patrick Amrein
Alessandro Lägeler
Markus Schwagenscheidt

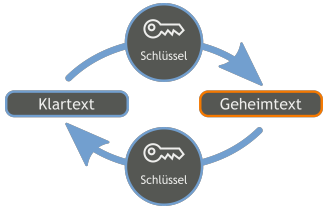
Was ist Kryptographie?

Kryptographie bezeichnet die Wissenschaft von der **Verschlüsselung** von Daten.



Was ist Kryptographie?

Kryptographie bezeichnet die Wissenschaft von der **Verschlüsselung** von Daten.



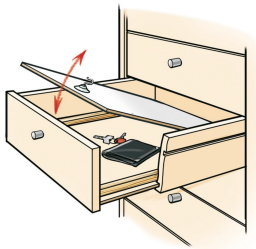
Kryptoanalyse befasst sich mit Methoden zum **Brechen** kryptographischer Verfahren.

Verschlüsseln vs. Verstecken

Kryptographie ist die Wissenschaft von der **Verschlüsselung** von Daten.

Steganographie ist die Wissenschaft vom **Verstecken** von Daten.

Verschlüsseln



Verstecken

Steganographie: Versteckte Nachricht im Bild

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

Welche Automarken verbergen sich als Morsecode im Bild?

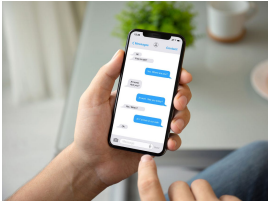
Kryptogaphie von der Antike bis heute

Skytale (400 v.Chr.)

Chiffrier-Scheibe (15. Jh.)

Enigma (zweiter Weltkrieg)

Online Banking



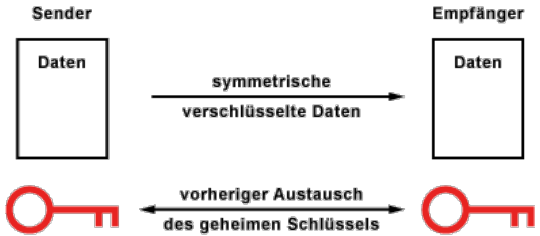
Text Messaging

Cloud Speicher

Symmetrische Kryptoverfahren

Wir wollen uns heute mit **symmetrischen** kryptographischen Verfahren beschäftigen.

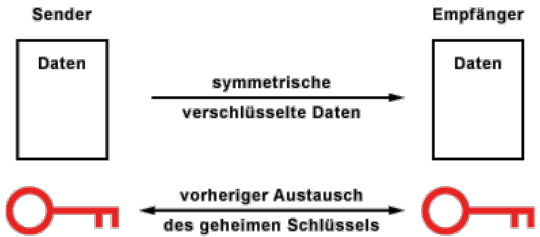
Dabei wird **derselbe Schlüssel** zum Ver- und Entschlüsseln von Nachrichten verwendet.



Symmetrische Kryptoverfahren

Wir wollen uns heute mit **symmetrischen** kryptographischen Verfahren beschäftigen.

Dabei wird **derselbe Schlüssel** zum Ver- und Entschlüsseln von Nachrichten verwendet.



Daher müssen Sender und Empfänger **beide** den Schlüssel kennen.

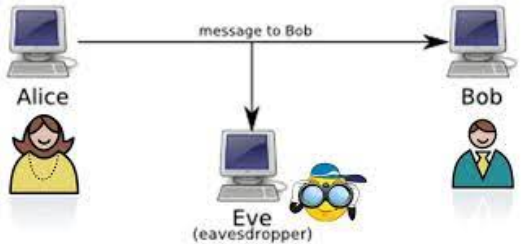
Der **Austausch des Schlüssels** ist ein **logistisches Problem** und ein **großes Sicherheitsrisiko**.

Kryptographische Annahmen

Kerckhoff's Prinzip: Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen, sondern nur von der Geheimhaltung des Schlüssel.

Kryptographische Annahmen

Kerckhoff's Prinzip: Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen, sondern nur von der Geheimhaltung des Schlüssel.



Wir wollen also folgende Annahmen machen:

1. **Klartexte und Schlüssel sind geheim**, und nur Sender und Empfänger bekannt.
2. **Geheimtexte sind öffentlich**, und Angreifern bekannt.
3. Das verwendete **Kryptoverfahren ist Angreifern bekannt**.

Kryptographische Annahmen

Kerckhoff's Prinzip: Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen, sondern nur von der Geheimhaltung des Schlüssel.

Wir wollen also folgende Annahmen machen:

1. **Klartexte und Schlüssel sind geheim**, und nur Sender und Empfänger bekannt.
2. **Geheimtexte sind öffentlich**, und Angreifern bekannt.
3. Das verwendete **Kryptoverfahren ist Angreifern bekannt**.

Ziel: Sichere Ver- und Entschlüsselung von Nachrichten unter obigen Annahmen.

Klartextalphabet und Geheimtextalphabet

Wir benutzen als **Klartextalphabet** die 26 lateinischen Kleinbuchstaben

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

Als **Geheimtextalphabet** benutzen wir die 26 Großbuchstaben

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

Beispiel

Klartext: treffen im park um zehn uhr

Geheimtext: WUHIIHQ LP SDUN XP CHKQ XKU

Monoalphabetische Verschlüsselung - Die Caesar Chiffre

Bei der **monoalphabetischen Verschlüsselung** wird jeder Buchstabe des Klartexts durch einen Geheimtextbuchstaben ersetzt.

Beispiel

Bei der **Caesar Chiffre** werden die Buchstaben des Klartexts um eine vorgegebene Anzahl Stellen nach rechts verschoben.
Verschieben wir etwa um 3 Stellen, so erhalten wir die Ersetzungsvorschrift

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

Der **Schlüssel** ist die Anzahl der Verschiebungen, in unserem Fall 3.

Monoalphabetische Verschlüsselung - Die Caesar Chiffre

Bei der **monoalphabetischen Verschlüsselung** wird jeder Buchstabe des Klartexts durch einen Geheimtextbuchstaben ersetzt.

Beispiel

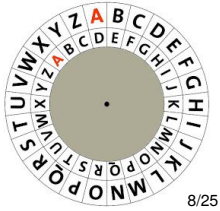
Bei der **Caesar Chiffre** werden die Buchstaben des Klartexts um eine vorgegebene Anzahl Stellen nach rechts verschoben.
Verschieben wir etwa um 3 Stellen, so erhalten wir die Ersetzungsvorschrift

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

Der **Schlüssel** ist die Anzahl der Verschiebungen, in unserem Fall 3.

Aufgaben:

1. Verschlüssele den Klartext `treffen im park um zehn uhr`
2. Entschlüssele den Geheimtext `DOOHV NODU BLV EDOG`



Sicherheit der Caesar Chiffre

Die Caesar Chiffre ist **sehr unsicher**!

Sicherheit der Caesar Chiffre

Die Caesar Chiffre ist **sehr unsicher**!

Es gibt nur 25 verschiedene Schlüssel. Durch **Ausprobieren** aller möglichen Schlüssel kann man den Klartext herausfinden und damit das Verfahren **brechen**.

Aufgabe: Entschlüssele den Geheimtext

```
ZIRM ZMHM ZMGM
```

Er ist mit der Caesar Chiffre (mit unbekannter Verschiebung) verschlüsselt.

Bessere monoalphabetische Verschlüsselung?

Problem bei der Caesar-Chiffre: Zu wenige mögliche Schlüssel, Brechen durch Ausprobieren.

Bessere monoalphabetische Verschlüsselung?

Problem bei der Caesar-Chiffre: Zu wenige mögliche Schlüssel, Brechen durch Ausprobieren.

Idee: Benutze **chaotischere** oder sogar **zufällige** Ersetzungsregeln, zum Beispiel

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

Der **Schlüssel** ist die vollständige Ersetzungsvorschrift.

Bessere monoalphabetische Verschlüsselung?

Problem bei der Caesar-Chiffre: Zu wenige mögliche Schlüssel, Brechen durch Ausprobieren.

Idee: Benutze **chaotischere** oder sogar **zufällige** Ersetzungsregeln, zum Beispiel

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

Der **Schlüssel** ist die vollständige Ersetzungsvorschrift.

Aufgabe: Wieviele mögliche Schlüssel gibt es?

Die Methode des Schlüsselworts

Problem: Eine **zufällige** Ersetzungsregel ist schwer zu merken. Aufschreiben des Schlüssels ist ein Sicherheitsrisiko.

Die Methode des Schlüsselworts

Problem: Eine **zufällige** Ersetzungsregel ist schwer zu merken. Aufschreiben des Schlüssels ist ein Sicherheitsrisiko.

Idee: Benutze ein **einfach zu merkendes Schlüsselwort**, aus dem die Ersetzungsregel abgeleitet werden kann.

Die Methode des Schlüsselworts

Problem: Eine **zufällige** Ersetzungsregel ist schwer zu merken. Aufschreiben des Schlüssels ist ein Sicherheitsrisiko.

Idee: Benutze ein **einfach zu merkendes Schlüsselwort**, aus dem die Ersetzungsregel abgeleitet werden kann.

Beispiel

Wir wählen das Schlüsselwort `GEHEIMSCHRIFT`.
1) Streiche alle doppelten Buchstaben (`GEHIMSCRFT`) und schreibe das verkürzte Schlüsselwort unter das Klartextalphabet.
2) Fülle die restlichen Buchstaben des Geheimtextalphabets der Reihe nach auf, beginnend mit dem Buchstaben, mit dem das Schlüsselwort endet

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

Die Methode des Schlüsselworts

Problem: Eine **zufällige** Ersetzungsregel ist schwer zu merken. Aufschreiben des Schlüssels ist ein Sicherheitsrisiko.

Idee: Benutze ein **einfach zu merkendes Schlüsselwort**, aus dem die Ersetzungsregel abgeleitet werden kann.

Beispiel

Wir wählen das Schlüsselwort `GEHEIMSCHRIFT`.
1) Streiche alle doppelten Buchstaben (`GEHIMSCRFT`) und schreibe das verkürzte Schlüsselwort unter das Klartextalphabet.
2) Fülle die restlichen Buchstaben des Geheimtextalphabets der Reihe nach auf, beginnend mit dem Buchstaben, mit dem das Schlüsselwort endet

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

Aufgabe: Stelle die Ersetzungsvorschrift für den Schlüssel `ETHZUERICH` auf.

Häufigkeitsanalyse - Brechen der monoalphabetischen Verschlüsselung

Problem der monoalphabetischen Verschlüsselung:

Ein Buchstabe des Klartexts wird **immer mit dem gleichen Symbol** verschlüsselt.

Dadurch übertragen sich **Häufigkeiten** und **Muster** im Klartext auf den Geheimtext.

Häufigkeitsanalyse - Brechen der monoalphabetischen Verschlüsselung

Problem der monoalphabetischen Verschlüsselung:

Ein Buchstabe des Klartexts wird **immer mit dem gleichen Symbol** verschlüsselt.

Dadurch übertragen sich **Häufigkeiten** und **Muster** im Klartext auf den Geheimtext.

Beispiel

Folgender Geheimtext wurde monoalphabetisch verschlüsselt:

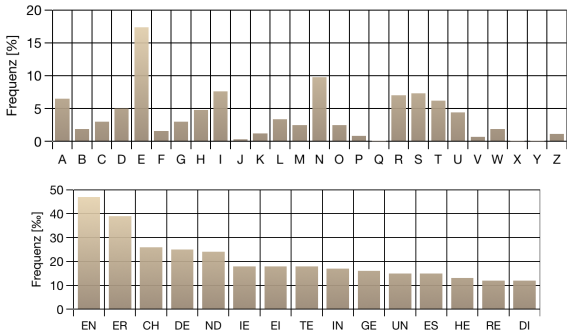
```
KAIQ AQWNI KIW IUOIWSXIWQNIW PXLP QV UQLPC, BQIOIW KIW MGIANIWPIAABLPIAW QW QPAIW
PTUUIW TDB BCIQW, KIW BCIAOUQLPIW, IGQN KIV CXKI FIAETUUIW, WIDW, IQWIA KIV KDWSUIW
PIAAW TDE KDWSUIV CPAXW QV UTWKI VXAKXA, GX KQI BLPTCCIW KAXPW. IQW AQWN, BQI MD
SWILPCIW, BQI TUUI MD EQWKIW, QWB KDWSIU MD CAIQOIW DWK IGQN MD OQWKIW QV UTWKI
VXAKXA, GX KQI BLPTCCIW KAXPW.
```

Der Buchstabe `I` taucht am häufigsten auf. Der häufigste Buchstabe im deutschen ist `e`. Wir vermuten daher

$$\texttt{I} = \texttt{e}$$

Häufigkeitsanalyse - Brechen der monoalphabetischen Verschlüsselung

Relative Häufigkeiten der Buchstaben und Bigramme in deutschen Texten:



Idee zum Brechen der monoalphabetischen Verschlüsselung:

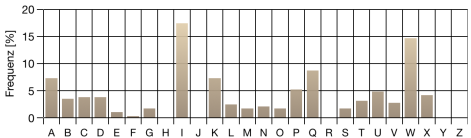
1. Zähle Häufigkeiten der Buchstaben im Geheimtext und finde so `e` und `n` und {`a`,`i`,`r`,`s`,`t`}.
2. Zähle Bigramme und finde so `a`,`i`,`r`,`s`,`t` heraus.
3. Rest ergibt sich durch Ausprobieren.

Häufigkeitsanalyse - Buchstaben zählen

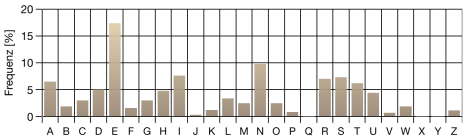
Geheimtext

```
KAIQ AQWNI KIW IUOIWSXIWQNIW PXLP QV UQLPC, BQIOIW KIW MGIANIWPIAABLPIAW QW QPAIW
PTUUIW TDB BCIQW, KIW BCIAOUQLPIW, IGQN KIV CXKI FIAETUUIW, WIDW, IQWIA KIV KDWSUIW
PIAAW TDE KDWSUIV CPAXW QV UTWKI VXAKXA, GX KQI BLPTCCIW KAXPW. IQW AQWN, BQI MD
SWILPCIW, BQI TUUI MD EQWKIW, QWB KDWSIU MD CAIQOIW DWK IGQN MD OQWKIW QV UTWKI
VXAKXA, GX KQI BLPTCCIW KAXPW.
```

Relative Häufigkeit der Buchstaben im Geheimtext



Relative Häufigkeiten in deutschen Texten



Wir vermuten:

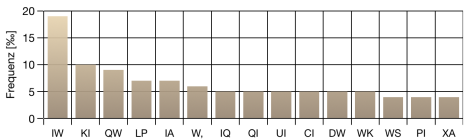
$$\texttt{e} = \texttt{I}, \quad \texttt{n} = \texttt{W}, \quad \{\texttt{a},\texttt{i},\texttt{r},\texttt{s},\texttt{t}\} \subset \{\texttt{A},\texttt{K},\texttt{P},\texttt{Q},\texttt{U},\texttt{X}\}$$

Häufigkeitsanalyse - Bigramme zählen

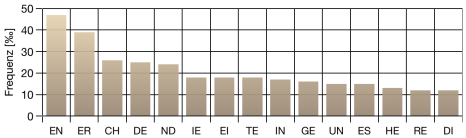
Geheimtext

```
KAIQ AQWNI KIW IUOIWSXIWQNIW PXLP QV UQLPC, BQIOIW KIW MGIANIWPIAABLPIAW QW QPAIW
PTUUIW TDB BCIQW, KIW BCIAOUQLPIW, IGQN KIV CXKI FIAETUUIW, WIDW, IQWIA KIV KDWSUIW
PIAAW TDE KDWSUIV CPAXW QV UTWKI VXAKXA, GX KQI BLPTCCIW KAXPW. IQW AQWN, BQI MD
SWILPCIW, BQI TUUI MD EQWKIW, QWB KDWSIU MD CAIQOIW DWK IGQN MD OQWKIW QV UTWKI
VXAKXA, GX KQI BLPTCCIW KAXPW.
```

Häufigste Bigramme im Geheimtext



Häufigste Bigramme in deutschen Texten



Wir vermuten $\texttt{de} = \texttt{KI}$ und $\texttt{in} = \texttt{QW}$ und $\texttt{er} = \texttt{IA}$ und $\texttt{ei} = \texttt{IQ}$, $\texttt{ie} = \texttt{QI}$, dann $\texttt{ch} = \texttt{LP}$ also

$$\texttt{e} = \texttt{I}, \quad \texttt{n} = \texttt{W}, \quad \texttt{d} = \texttt{K}, \quad \texttt{i} = \texttt{Q}, \quad \texttt{r} = \texttt{A}, \quad \texttt{c} = \texttt{L}, \quad \texttt{h} = \texttt{P}, \qquad \{\texttt{a},\texttt{s},\texttt{t}\} = \{\texttt{U},\texttt{X}\}$$

Häufigkeitsanalyse - Teilweise entschlüsselter Text

Geheimtext

KAIQ AQWNI KIW IUOIWSXIWQNIW PXLP QV UQLPC, BQIOIW KIW MGIANIWPIAABLPIAW QW QPAIW PTUUIW TDB BCIQW, KIW BCIAOUQLPIW, IGQN KIV CXKI FIAETUUIW, WIDW, IQWIA KIV KDWSUIW PIAAW TDE KDWSUIV CPAXW QV UTWKI VXAKXA, GX KQI BLPTCCIW KAXPW. IQW AQWN, BQI MD SWILPCIW, BQI TUUI MD EQWKIW, QWB KDWSIU MD CAIQOIW DWK IGQN MD OQWKIW QV UTWKI VXAKXA, GX KQI BLPTCCIW KAXPW.

$$\mathtt{e} = \mathtt{I}, \quad \mathtt{n} = \mathtt{W}, \quad \mathtt{d} = \mathtt{K}, \quad \mathtt{i} = \mathtt{Q}, \quad \mathtt{r} = \mathtt{A}, \quad \mathtt{c} = \mathtt{L}, \quad \mathtt{h} = \mathtt{P}, \qquad \{\mathtt{a},\mathtt{s},\mathtt{t}\} = \{\mathtt{U},\mathtt{X}\}$$

Teilweise entschlüsselter Text

drei rinNe den eUOenSXeninen hXch iV UichC, BieOen den MGerNenherrBchern in ihren hTUUen TBD BCein, den BCerOUichen, eGiN deV CXde FerETUUen, neDn, einer deV dDnSUen herrn TDE dDnSUeV ChrXn iV UTnde VXrdXr, GX die BchTCCen drXhn. ein rinN, Bie MD SnechCen, Bie TUUe MD Einden, inB dDnSeU MD CreiOen Dnd eGiN MD Oinden iV UTnde VXrdXr, GX die BchTCCen drXhn.

Häufigkeitsanalyse - Teilweise entschlüsselter Text

Geheimtext

KAIQ AQWNI KIW IUOIWSXIWQNIW PXLP QV UQLPC, BQIOIW KIW MGIANIWPIAABLPIAW QW QPAIW PTUUIW TDB BCIQW, KIW BCIAOUQLPIW, IGQN KIV CXKI FIAETUUIW, WIDW, IQWIA KIV KDWSUIW PIAAW TDE KDWSUIV CPAXW QV UTWKI VXAKXA, GX KQI BLPTCCIW KAXPW. IQW AQWN, BQI MD SWILPCIW, BQI TUUI MD EQWKIW, QWB KDWSIU MD CAIQOIW DWK IGQN MD OQWKIW QV UTWKI VXAKXA, GX KQI BLPTCCIW KAXPW.

$$\mathtt{e} = \mathtt{I}, \quad \mathtt{n} = \mathtt{W}, \quad \mathtt{d} = \mathtt{K}, \quad \mathtt{i} = \mathtt{Q}, \quad \mathtt{r} = \mathtt{A}, \quad \mathtt{c} = \mathtt{L}, \quad \mathtt{h} = \mathtt{P}, \qquad \{\mathtt{a},\mathtt{s},\mathtt{t}\} = \{\mathtt{U},\mathtt{X}\}$$

Teilweise entschlüsselter Text

drei rinNe den eUOenSXeninen hXch iV UichC, BieOen den MGerNenherrBchern in ihren hTUUen TBD BCein, den BCerOUichen, eGiN deV CXde FerETUUen, neDn, einer deV dDnSUen herrn TDE dDnSUeV ChrXn iV UTnde VXrdXr, GX die BchTCCen drXhn. ein rinN, Bie MD SnechCen, Bie TUUe MD Einden, inB dDnSeU MD CreiOen Dnd eGiN MD Oinden iV UTnde VXrdXr, GX die BchTCCen drXhn.

rinNe könnte rinde oder ringe heißen, aber da d = K, ist wahrscheinlich g = N.
hXch könnte hoch heißen, also vermuten wir o = X.
iV könnte in oder im sein, aber da n = W, ist wahrscheinlich m = V.

Häufigkeitsanalyse - Entschlüsselter Text

Geheimtext

KAIQ AQWNI KIW IUOIWSXIWQNIW PXLP QV UQLPC, BQIOIW KIW MGIANIWPIAABLPIAW QW QPAIW PTUUIW TDB BCIQW, KIW BCIAOUQLPIW, IGQN KIV CXKI FIAETUUIW, WIDW, IQWIA KIV KDWSUIW PIAAW TDE KDWSUIV CPAXW QV UTWKI VXAKXA, GX KQI BLPTCCIW KAXPW. IQW AQWN, BQI MD SWILPCIW, BQI TUUI MD EQWKIW, QWB KDWSIU MD CAIQOIW DWK IGQN MD OQWKIW QV UTWKI VXAKXA, GX KQI BLPTCCIW KAXPW.

Entschlüsselter Text

drei ringe den elbenkoenigen hoch im licht, sieben den zwergenherrschern in ihren hallen aus stein, den sterblichen, ewig dem tode verfallen, neun, einer dem dunklen herrn auf dunklem thron im lande mordor, wo die schatten drohn. ein ring, sie zu knechten, sie alle zu finden, ins dunkel zu treiben und ewig zu binden im lande mordor, wo die schatten drohn

Das Schlüsselwort ist TOLKIEN.

Unsere Vermutung $\{\texttt{a},\texttt{s},\texttt{t}\} = \{\texttt{U},\texttt{X}\}$ war übrigens falsch! Der Text ist recht kurz, was die Häufigkeitsanalyse erschwert.

Häufigkeitsanalyse - Aufgabe

Aufgabe: Knacke folgenden (monoalphabetisch verschlüsselten) Geheimtext:

```
WL PSK WBGFSE, OHK ESGYWK VWBM, BG WBGWK PWBM, PWBM WGMXWKGMWG YSESQBL...
WL ZWKKLAZM TNWKYWKDKBWY. RBW KWTWEEWG, RWKWG KSNFLAZBXXW OHG WBGWF YWZWBFWG
LMNWMVINGDM SNL SGYKWBXWG, ZSTWG BZKWG WKLMWG LBWY YWYWG RSL THWLW YSESDMBLAZW
BFIWKBNF WKKNGYWG. PSWZKWGR RWK LAZESAZM BLM WL LIBHGWG RWK KWTWEEWG YWENGYWG,
YWZWBFIESWGW NWTWK RBW STLHENMW PSXXW RWL BFIWKBNFL BG BZKWG TWLBMV VN TKBGYWG, RWG
MHRWLLMWKG, WBGW KSNFLMSMBHG, RWKWG XWNWKDKSXM SNLKWBAZM, NF WBGWG YSGVWG IESGWMWG
VN OWKGBAZMWG. OWKXHEYM OHG RWG XBGLMWKWG SYWGMWG RWL BFIWKBNFL, CSYM IKBGVWLLBG
EWBS SG THKR BZKWL LMWKGWGLAZBXXWL GSAZ ZSNLW, SEL ZNWMWKBG RWK W KTWN MWMWG IESWGW,
RBW BZK OHED KWMMWG NGR RWK YSESQBL RBW XKWBZWBM PBWRWKYWTWG DHWGGMWG...
```

Sie finden den Text und das Tool zur Häufigkeitsanalyse auf der Webseite!

Polyalphabetische Verschlüsselung

Bei der **polyalphabetischen Verschlüsselung** wird jeder Buchstabe des Klartexts mit **mehreren verschiedenen** Geheimtextbuchstaben verschlüsselt.

Polyalphabetische Verschlüsselung

Bei der **polyalphabetischen Verschlüsselung** wird jeder Buchstabe des Klartexts mit **mehreren verschiedenen** Geheimtextbuchstaben verschlüsselt.

Dazu werden **mehrere Geheimtextalphabete** benutzt.

Beispiel

Benutze vier monoalphabetische Verschlüsselungen abwechselnd:

Klartextalphabet	`a b c d e ...`
erstes Geheimtextalphabet	`H L W X D ...`
zweites Geheimtextalphabet	`U L V W A ...`
drittes Geheimtextalphabet	`N A R T I ...`
viertes Geheimtextalphabet	`D Y Z L M ...`

Der Klartext `abba` wird verschlüsselt zu `HLAD`.

Vorteil: Häufigkeiten und Muster des Klartexts sind im Geheimtext verschwunden!

Polyalphabetische Verschlüsselung

Bei der **polyalphabetischen Verschlüsselung** wird jeder Buchstabe des Klartexts mit **mehreren verschiedenen** Geheimtextbuchstaben verschlüsselt.

Dazu werden **mehrere Geheimtextalphabete** benutzt.

Beispiel

Benutze vier monoalphabetische Verschlüsselungen abwechselnd:

Klartextalphabet	`a b c d e ...`
erstes Geheimtextalphabet	`H L W X D ...`
zweites Geheimtextalphabet	`U L V W A ...`
drittes Geheimtextalphabet	`N A R T I ...`
viertes Geheimtextalphabet	`D Y Z L M ...`

Der Klartext `abba` wird verschlüsselt zu `HLAD`.

Vorteil: Häufigkeiten und Muster des Klartexts sind im Geheimtext verschwunden!

Aufgaben: Verschlüsseln Sie den Klartext `babe`.

Die Vigenére Chiffre

Die **Vigenére Chiffre** kombiniert 26 monoalphabetische Verschlüsselungen.

Die Wahl des Geheimtextalphabets erfolgt mittels **Schlüsselwort** anhand des **Vigenére Quadrats:**

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Die Vigenére Chiffre - Ein Beispiel

Wir wählen das Schlüsselwort `JAMESBOND` und schreiben es periodisch über den Klartext

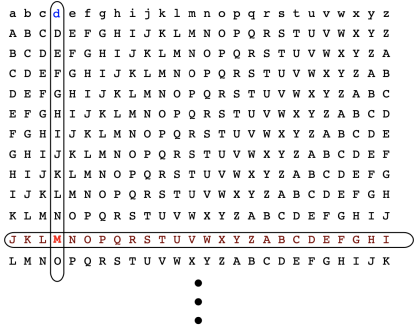
Schlüsselwort	`JAM ESBONDJAMESBON DJAME...`
Klartext	`der abgeschlossene roman...`

Die Vigenére Chiffre - Ein Beispiel

Wir wählen das Schlüsselwort `JAMESBOND` und schreiben es periodisch über den Klartext

Schlüsselwort	`JAM ESBONDJAMESBON DJAME...`
Klartext	`der abgeschlossene roman...`

Um `d` zu verschlüsseln, suchen wir den Schnittpunkt der Spalte `d` mit der Zeile `J` im Vigenére Quadrat:



Wir erhalten den Geheimtext

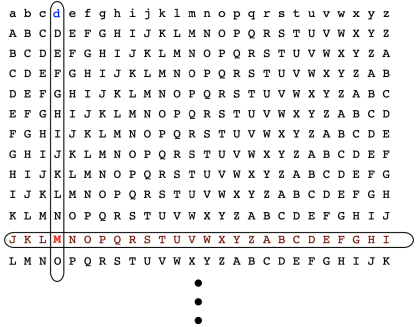
Schlüsselwort	`JAM ESBONDJAMESBON DJAME...`
Klartext	`der abgeschlossene roman...`
Geheimtext	`MED ETHSFFQLAWKFBR UXMMR...`

Die Vigenére Chiffre - Ein Beispiel

Wir wählen das Schlüsselwort `JAMESBOND` und schreiben es periodisch über den Klartext

Schlüsselwort	`JAM ESBONDJAMESBON DJAME...`
Klartext	`der abgeschlossene roman...`

Um `d` zu verschlüsseln, suchen wir den Schnittpunkt der Spalte `d` mit der Zeile `J` im Vigenére Quadrat:



Wir erhalten den Geheimtext

Schlüsselwort	`JAM ESBONDJAMESBON DJAME...`
Klartext	`der abgeschlossene roman...`
Geheimtext	`MED ETHSFFQLAWKFBR UXMMR...`

Aufgabe: Verschlüssele
`treffen im park um vier` mit Schlüsselwort `HUND`.

Sicherheit der Vigenére Chiffre

Man kann die Vigenére Chiffre brechen, wenn das **Schlüsselwort kurz** und der **Geheimtext lang** ist.

Sicherheit der Vigenére Chiffre

Man kann die Vigenére Chiffre brechen, wenn das **Schlüsselwort kurz** und der **Geheimtext lang** ist.

Beispiel

Nehmen wir an, das Schlüsselwort hat Länge 5.

Position	12345 6789...
Schlüsselwort	REGEN REGEN REGEN REGEN REGEN REGEN...
Klartext	daswe tteri stgut dieso nnesc heint...
Geheimtext	UEYAR KXKVV JXMYG UMKWB ERKWP YIORG...

Der 1.,6.,11.,16.,...Buchstabe wird mit dem **gleichen Alphabet** Caesar-verschlüsselt.
Die Weite der Verschiebung kann wieder durch Häufigkeitsanalysen ermittelt werden.

Sicherheit der Vigenére Chiffre

Man kann die Vigenére Chiffre brechen, wenn das **Schlüsselwort kurz** und der **Geheimtext lang** ist.

Beispiel

Nehmen wir an, das Schlüsselwort hat Länge 5.

Position	12345 6789...
Schlüsselwort	REGEN REGEN REGEN REGEN REGEN REGEN...
Klartext	daswe tteri stgut dieso nnesc heint...
Geheimtext	UEYAR KXKVV JXMYG UMKWB ERKWP YIORG...

Der 1.,6.,11.,16.,...Buchstabe wird mit dem **gleichen Alphabet** Caesar-verschlüsselt.
Die Weite der Verschiebung kann wieder durch Häufigkeitsanalysen ermittelt werden.

Die Schlüssellänge kann **durch Probieren** oder mittels **Kasiski-Test** gefunden werden.

Aus heutiger Sicht ist die Vigenére Chiffre daher **nicht mehr sicher**.

Aufgabe: Folgender Geheimtext wurde Vigenére-verschlüsselt. Wir vermuten, dass die Schlüssellänge 3 ist.

Geheimtext

```
LCG LQN UXX YVT YYA LCM LLD LCM OUM TYB UYZ HHS LMX LFX LCG NYG VGF LHZ SYB JBW LHL
BYL ZYG MLN LBE PHZ ZGH YAX UXB LCV OGB AAT UTX TBX YTX UAX UCX ZMX PWA ICG HFE LCG
BHW MLX BYF PWA TYB UYL SYU LHL PHW PYL LLZ LAX UXW PYY BYK ZIE JBX ZYX SYG NYL JBT
MZX UCL AQB LXB LGX PHX PWA ICG ZIZ SOX JEE PWA TYB UVX ZNX YMH NUG GCG KYF NYY BYA
SYO VHK BBB NYF KUL LCG CYK ZOG RYG KUS SFL CGL ENU MMK UKB HML LEL CWL NBJ BDV YGU
NXQ YMG NGP WAA TXP WAU YGU CVO NXP HXU MMY CVO OGK VBU HBL YBU AKV YLZ YKL LFH FXY
AXD YLL HTS MBU XBL MXU UNN YGI FBJ EXU
```

Bestimme das Schlüsselwort.

Aufgabe: Wähle ein Schlüsselwort der Länge 4, und verschlüssele einen (etwas längeren) deutschen Text mit der Vigenére-Chiffre.

Tausche den Text mit jemand anderem aus, und versuche, den erhaltenen Geheimtext zu knacken.

Achtung: Wir benutzen nur die 26 lateinischen Buchstaben. Sonderzeichen, Umlaute, etc. werden nicht verschlüsselt, und sollten ggf. umgeschrieben werden, z.b. ä als ae.

One-Time-Pad

Wir nehmen an, dass der **Klartext in Bits codiert** ist, z.B. `0110110`.

Man kann z.B. jeden Buchstaben `a`, `b` einzeln in Bits codieren:

`a`	`b`	`c`	`d`	`e`	`f`	`g`	`h`	...
00000	00001	00010	00011	00100	00101	00110	00111	...

So wird z.B. aus

`dach`

der Code

00011 00000 00010 00111.

One-Time-Pad

Wir nehmen an, dass der **Klartext in Bits codiert** ist, z.B. `0110110`.

Der Schlüssel ist ebenfalls in Bits kodiert, und **genauso lang wie der Klartext**, z.B. `0001101`.

One-Time-Pad

Wir nehmen an, dass der **Klartext in Bits codiert** ist, z.B. `0110110`.

Der Schlüssel ist ebenfalls in Bits kodiert, und **genauso lang wie der Klartext**, z.B. `0001101`.

Verschlüsselung: Schreibe
Klartext und Schlüssel untereinander und **bilde bitweise XOR**.

Entschlüsselung:
verschlüssele den Geheimtext mit **demselben Schlüssel**.

Beispiel:

Klartext	`0110110`
Schlüssel	`0001101`
Geheimtext	`0111011`

A	B	A **XOR** B
0	0	0
0	1	1
1	0	1
1	1	0

One-Time-Pad

Wir nehmen an, dass der **Klartext in Bits codiert** ist, z.B. `0110110`.

Der Schlüssel ist ebenfalls in Bits kodiert, und **genauso lang wie der Klartext**, z.B. `0001101`.

Verschlüsselung: Schreibe
Klartext und Schlüssel untereinander und **bilde bitweise XOR**.

A	B	A **XOR** B
0	0	0
0	1	1
1	0	1
1	1	0

Entschlüsselung:
verschlüssele den Geheimtext mit **demselben Schlüssel**.

Beispiel:

Klartext	`0110110`
Schlüssel	`0001101`
Geheimtext	`0111011`

Aufgabe:

1. Verschlüsseln Sie `11101001` mit dem Schlüssel `10110101`.
2. Zeigen Sie, dass es zu jedem Paar K, G zweier Bitstrings gleicher Länge einen passenden Schlüssel gibt, der K zu G verschlüsselt.