Kryptologie

Gymnasium Kirchenfeld

Geheime Mitteilungen

Friedrich der Grosse und Voltaire

$$\frac{p}{Venez}\ \text{à}\ \frac{ci}{Sans}\,!$$

Venez sous p
à *Sans sous ci*!

Venez souper
à Sanssouci!

Antwort

G a !

'G' grand 'a' petit!

J'ai grand appetit!

Wichtige Begriffe

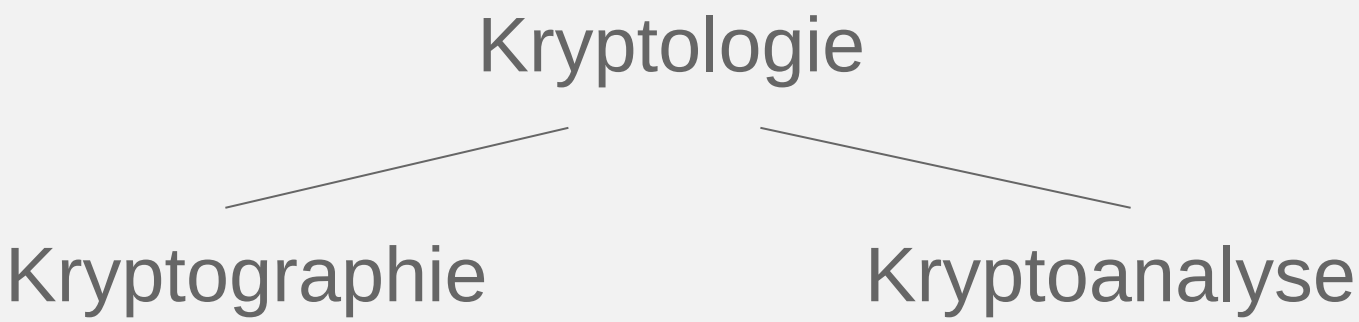
- **Kryptologie**

  kryptós = verborgen
  logos = Lehre, Kunde

- **Kryptographie**

  gráphein= schreiben

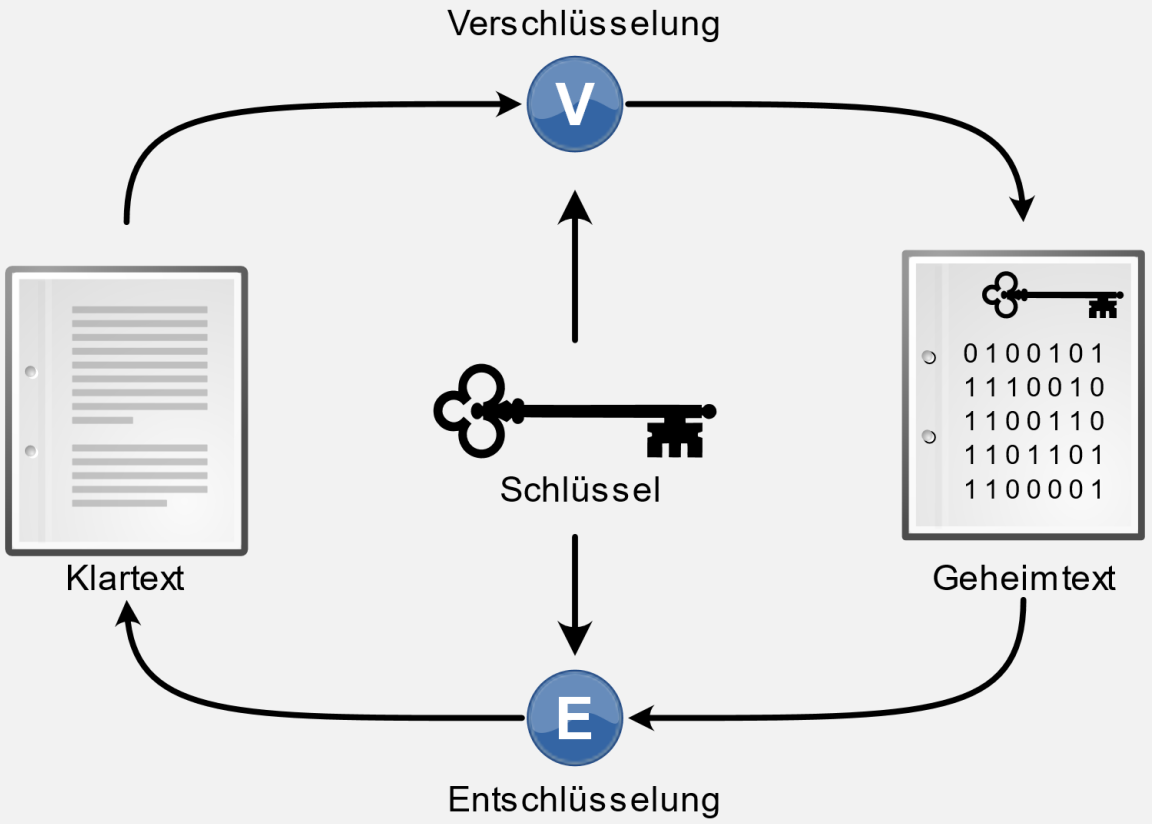
Wichtige Begriffe



Wichtige Begriffe

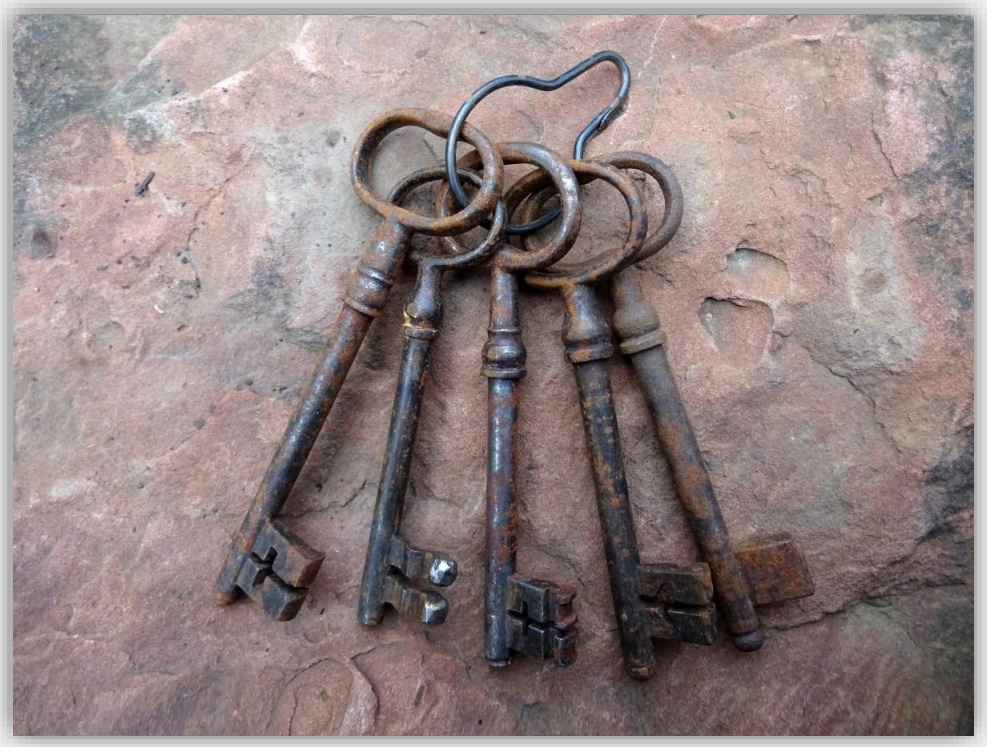
Deutsch	Englisch	Abkürzung
Klartext	Plaintext	p
Geheimtext	Ciphertext	c
Schlüssel	Key	k

Verschlüsselung/Entschlüsselung



Schlüsselraum

Die Menge aller möglichen Schlüssel



Verschlüsselte Texte

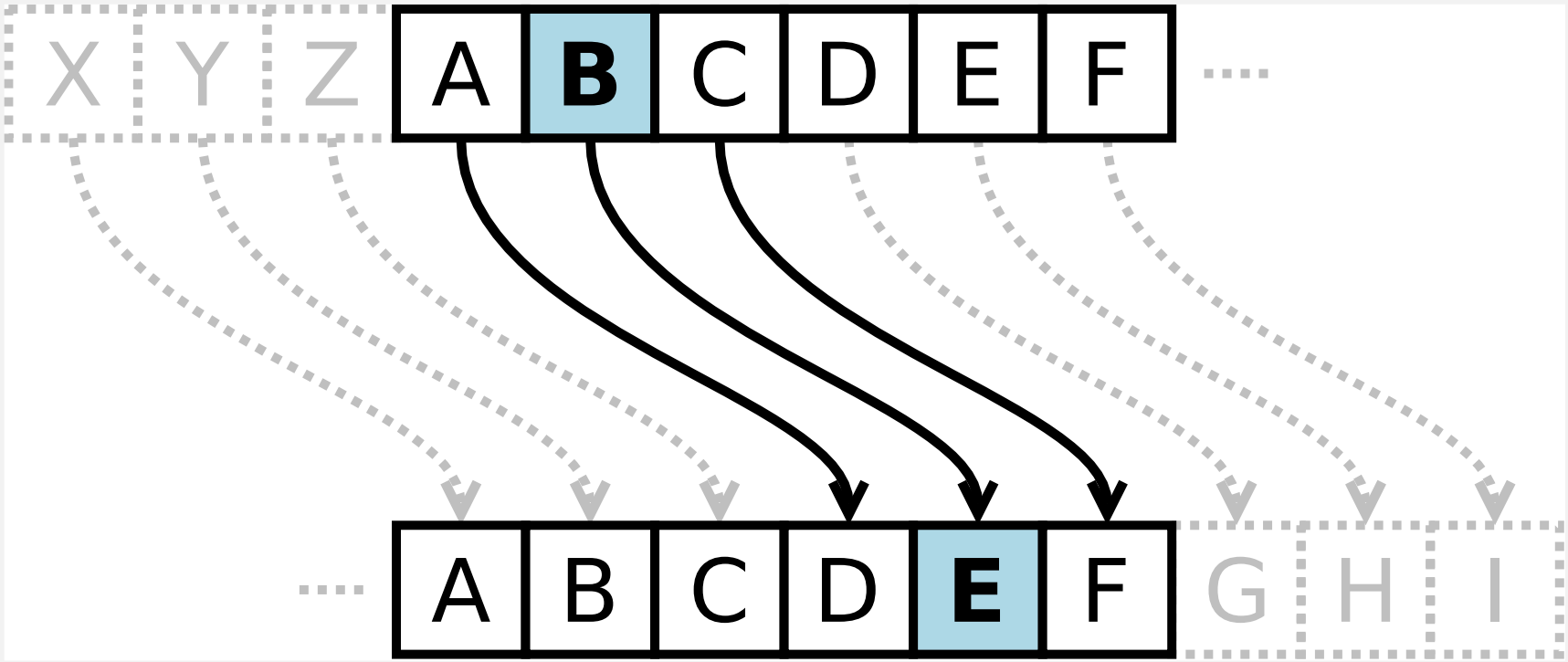
- Was haben Sie herausgefunden?
- Wie sind Sie vorgegangen?

Skytale

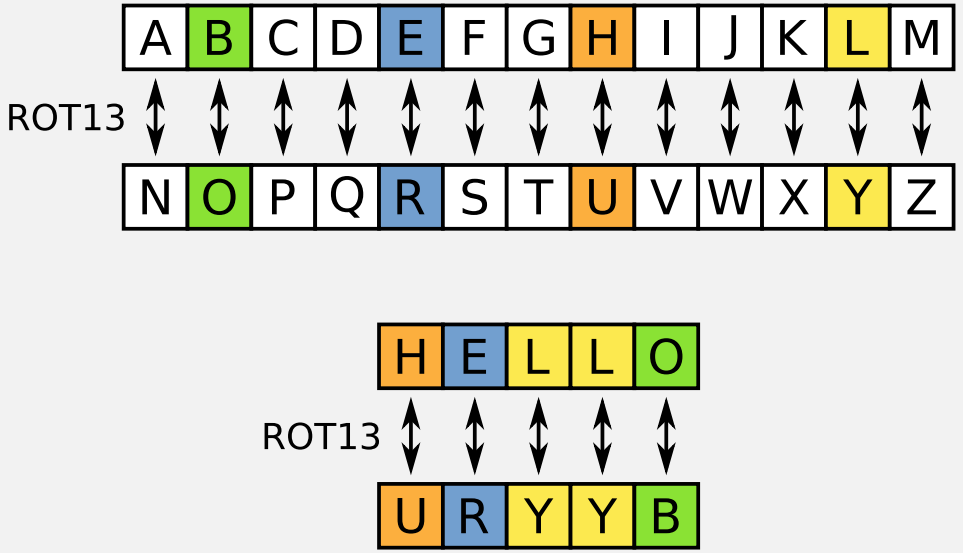
Polybios

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

Caesar-Chiffre



ROT13



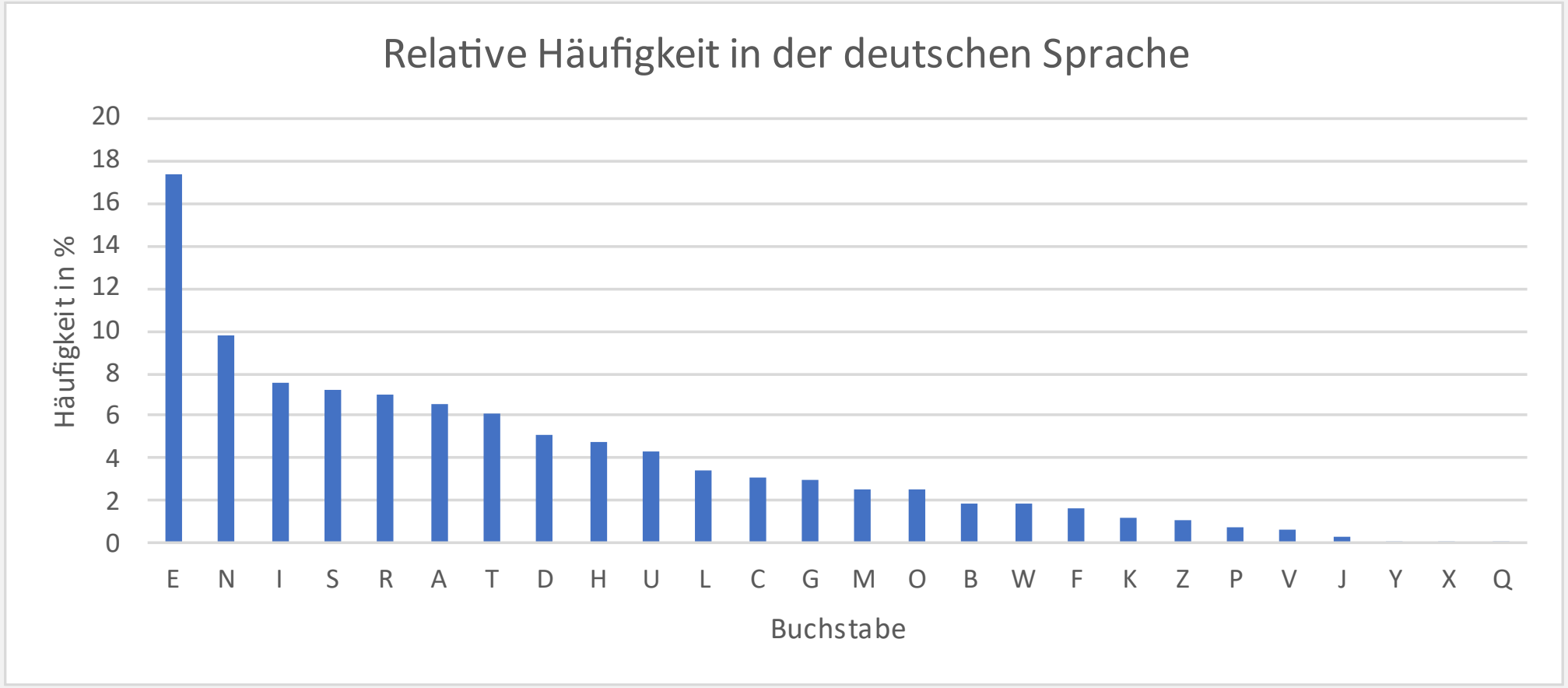
Atbash

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

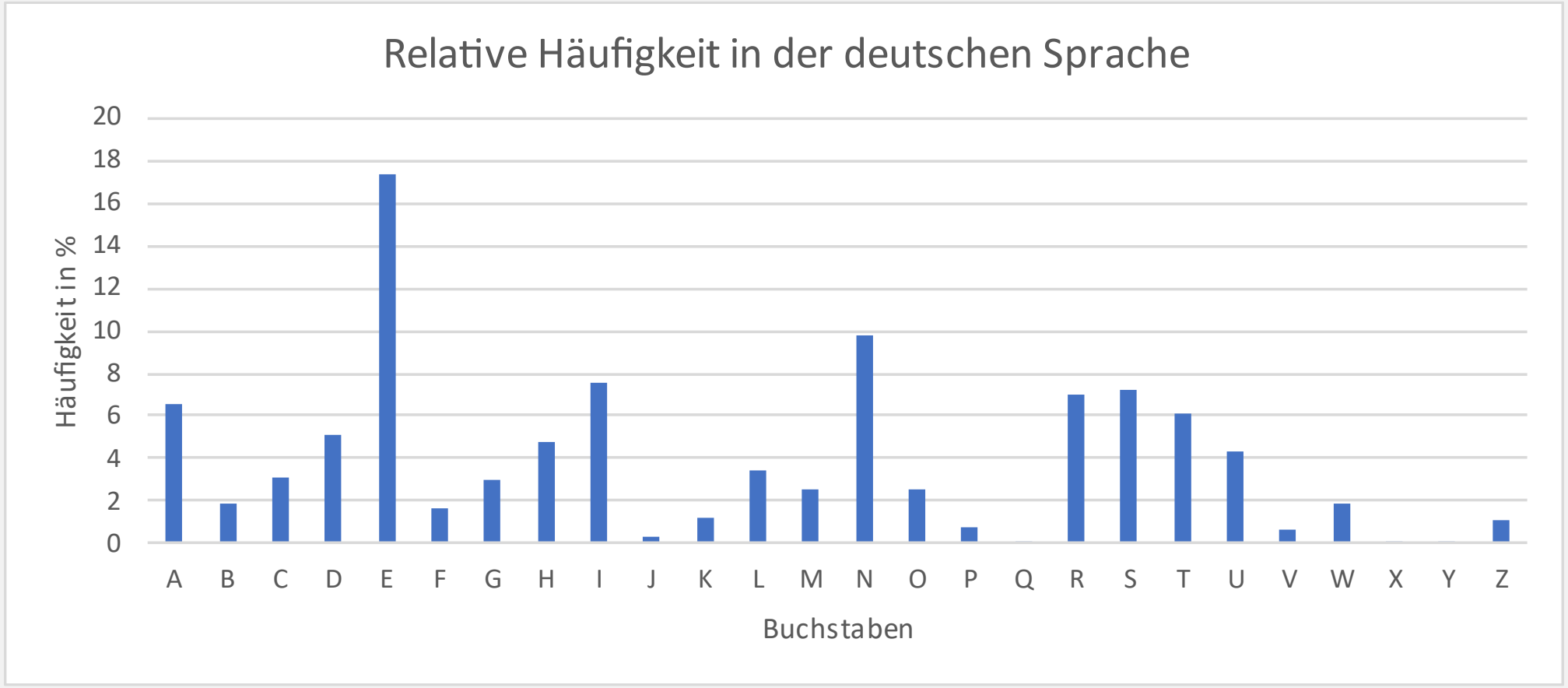
Allgemeine monoalphabetische Substitution

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

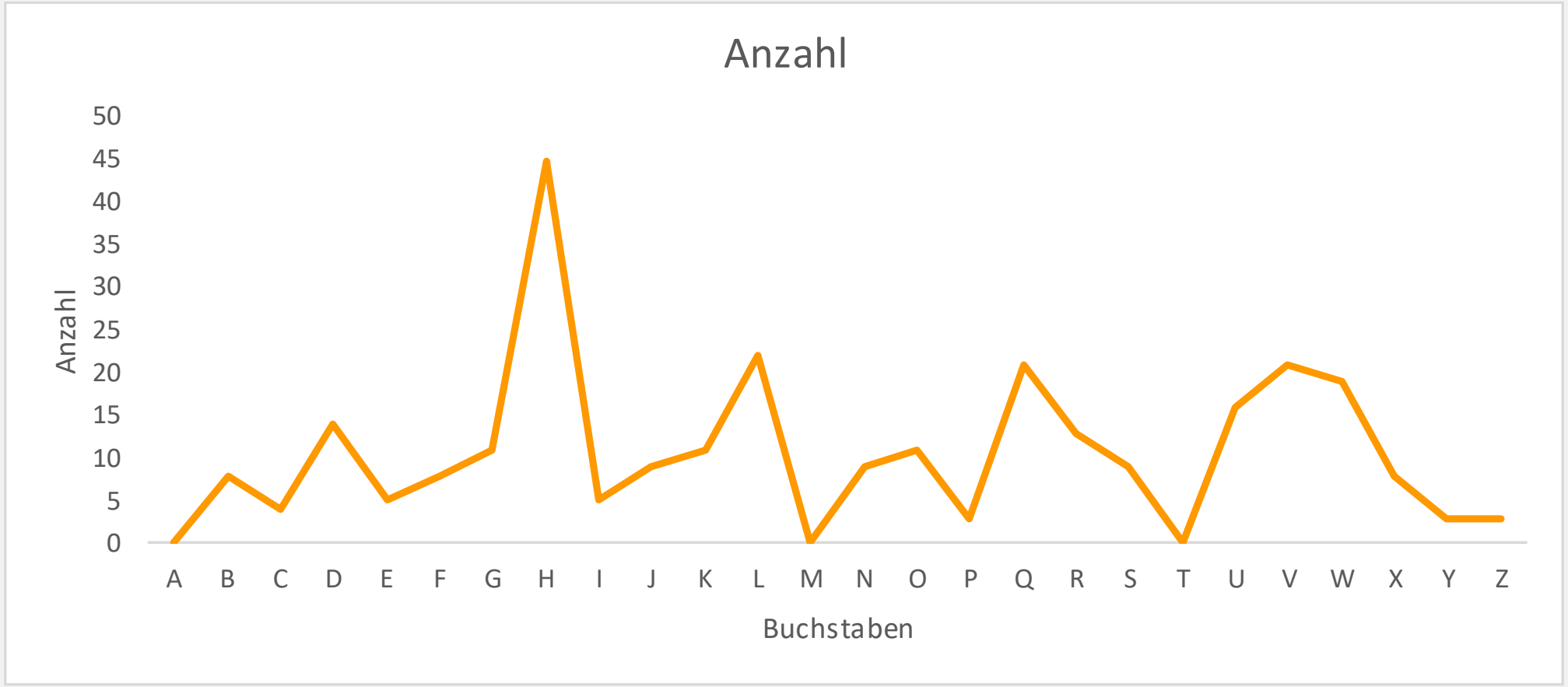
Buchstabenhäufigkeit (Deutsch)



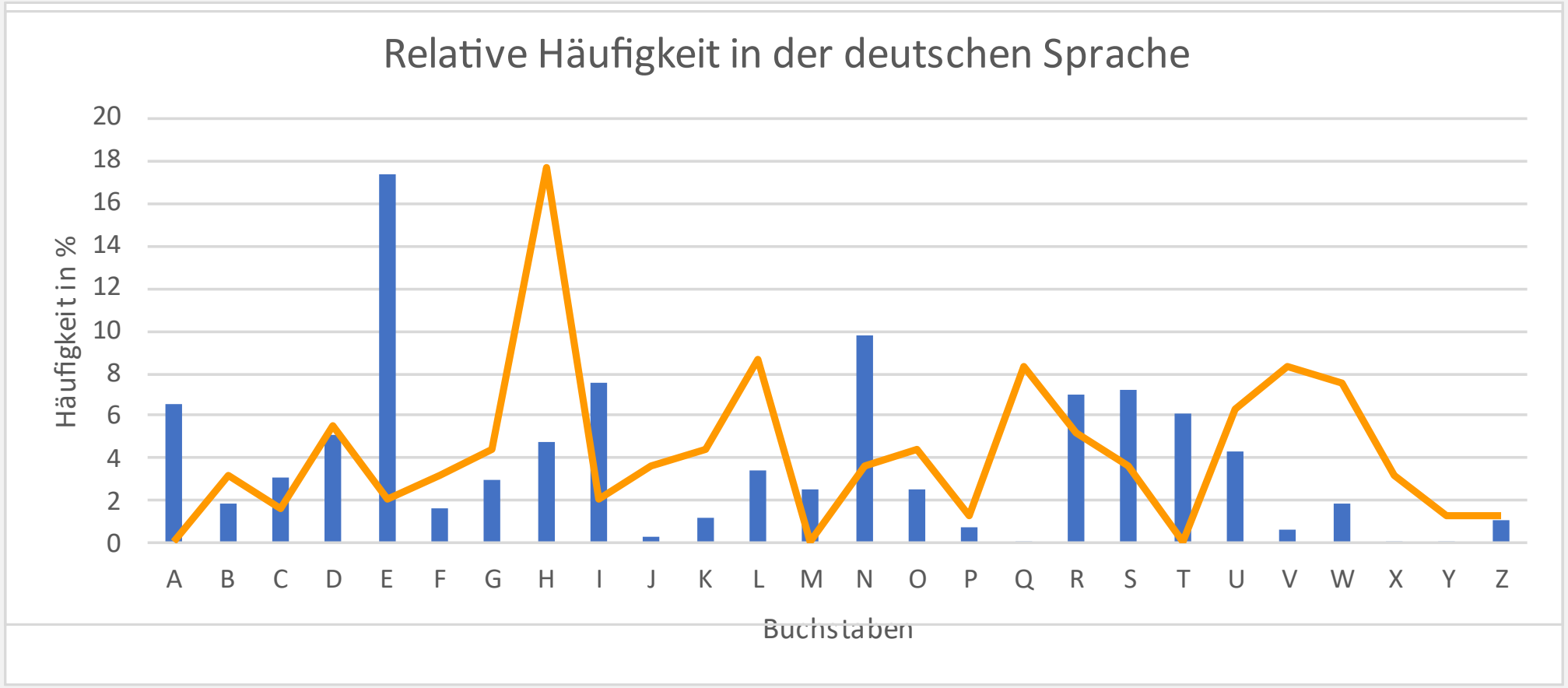
Buchstabenhäufigkeit (Deutsch)



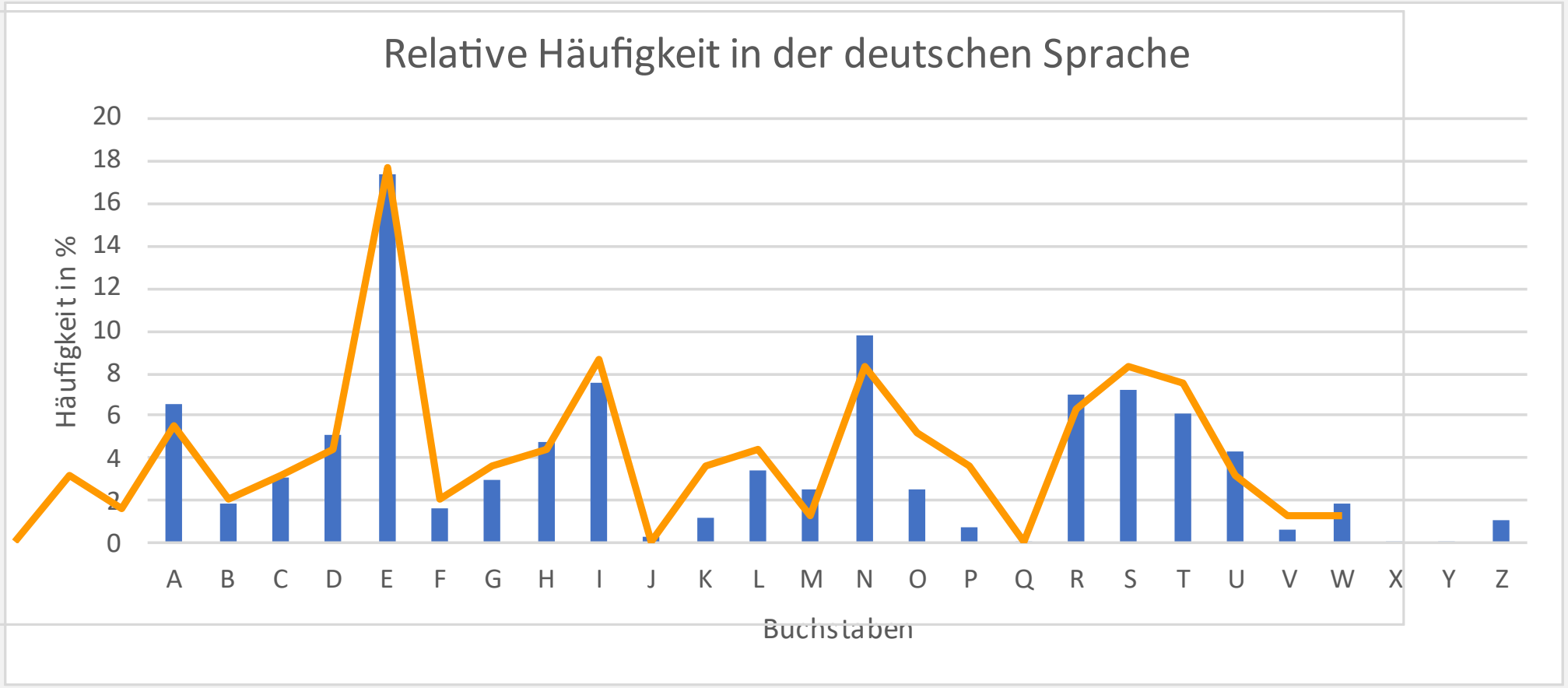
Anzahl Buchstaben im Caesar-Text



Überlagerung



Überlagerung



Vigenère-Chiffre

- Mehrere Alphabete → polyalphabetisch
- Schlüssel bestimmt Anzahl

Schlüssel \ Klartext-Alphabet	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

Geheimtext

Schlüssel:	AKEY								
Klartext:	G	E	H	E	I	M	N	I	S
Schlüssel:	A	K	E	Y	A	K	E	Y	A
Geheimtext:	G	O	L	C	I	W	R	G	S

Schlüsselraum antiker Verfahren?

- Skytale
- Caesar
- ROT13 / Atbash
- Monoalphabetische Substitution
- Polybios
- Vigenère
  - Schlüsselwort mit 6 Zeichen
  - Schlüsselwort mit 8 Zeichen

Schlüsselraum antiker Verfahren?

• Skytale	ein, zwei Dutzend
• Caesar	26
• ROT13 / Atbash	1
• Monoalphabetische Substitution	$26! > 4*10^{26}$
• Polybios	$25! > 1.5*10^{25}$
• Vigenère	Je nach Schlüsselwort
• Schlüsselwort mit 6 Zeichen	$26^6 =$ 308’915’776
• Schlüsselwort mit 8 Zeichen	$26^8 =$ 208’827’064’576

Achtung!

Der Schlüsselraum alleine
sagt nichts über die
Sicherheit des
Verfahrens
aus!

Wieso?