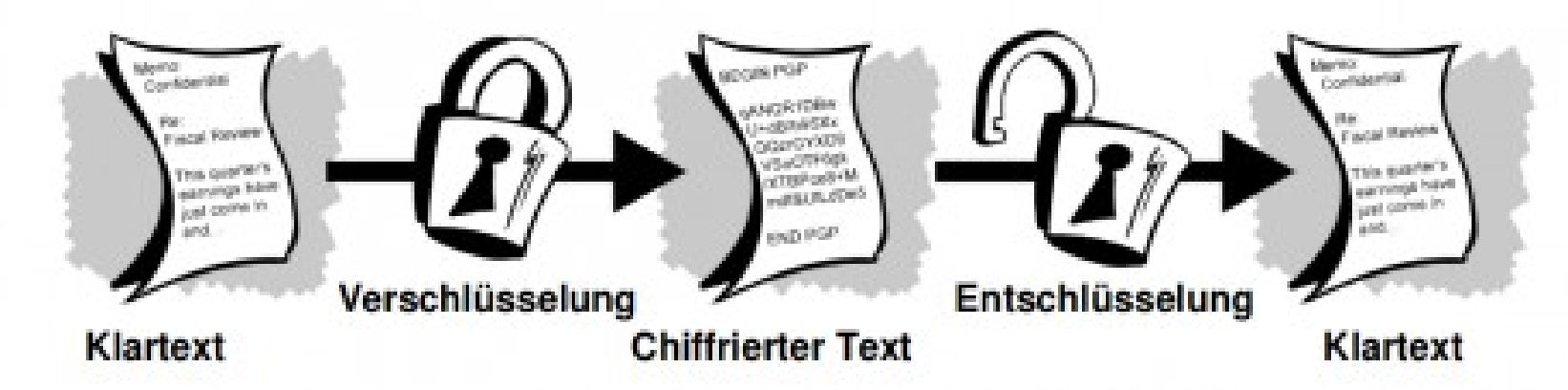
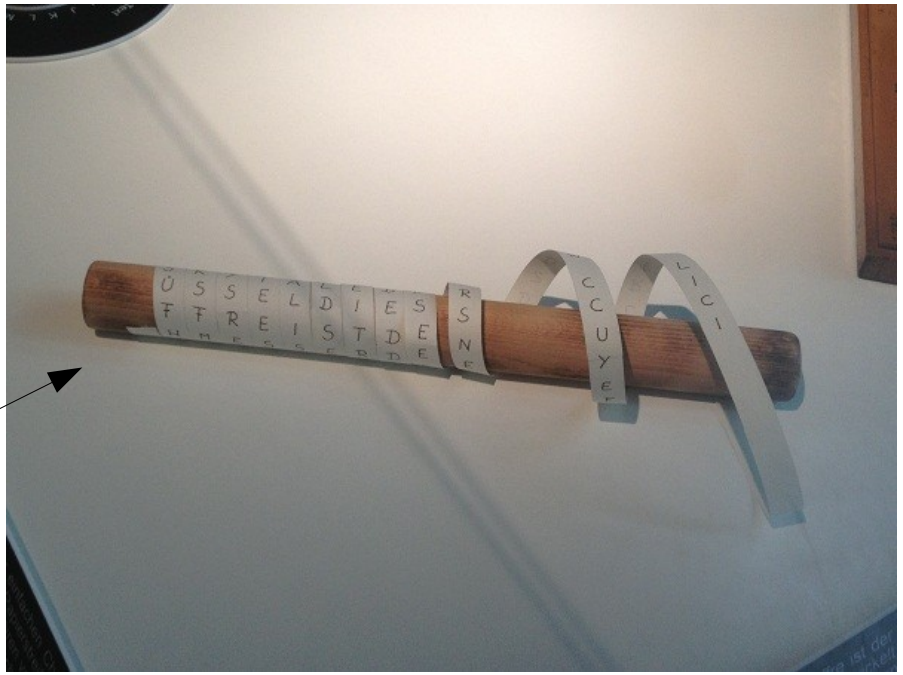
Kryptologie: Grundsätze

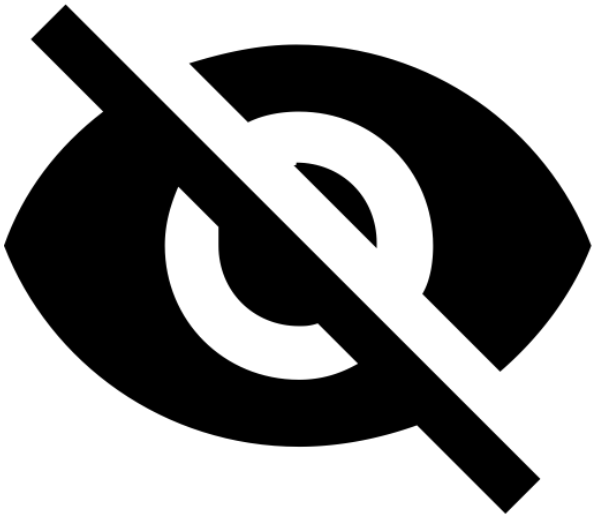


- Schlüssel
- Klartext
- Geheimtext

Skytale: Was ist was?



Kryptologie: Security ↔ Obscurity



Kerckhoff:

- **Mechanismus/Verfahren bekannt**, gut untersucht
- Sicherheit ausschließlich durch die **Kenntnis des Schlüssels**

Kryptologie: Klassische Verfahren

Monoalphabetische Substitutionsverfahren

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

MEIN NAME IST HASE

ZIXR RLZI XJK ULJI

Spezialfall: Cäsar Chiffre

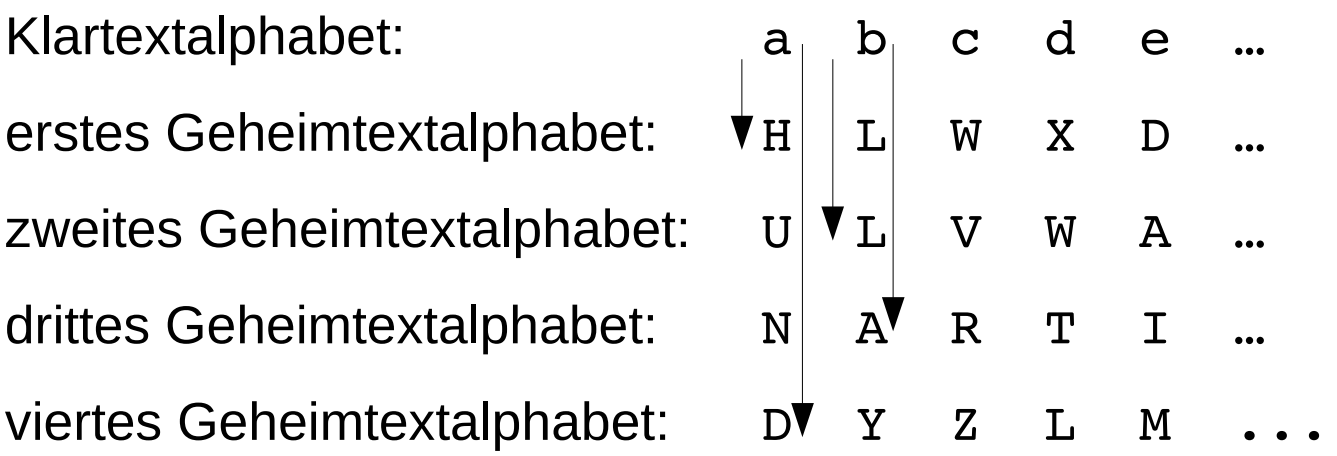
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Angriff: Häufigkeitsanalyse

Kryptologie: Klassische Verfahren

Polyalphabetische Substitutionsverfahren

Klartext `'abba'`



Geheimtext `'HLAD'`

~~**Angriff: Häufigkeitsanalyse**~~

Problem: Was ist der Schlüssel?

Kryptologie: Vigenere

Schlüsselbuchstabe

Klartextbuchstabe	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

Klartext: `Info ist voll super`
Schlüsselwort: `geheim`

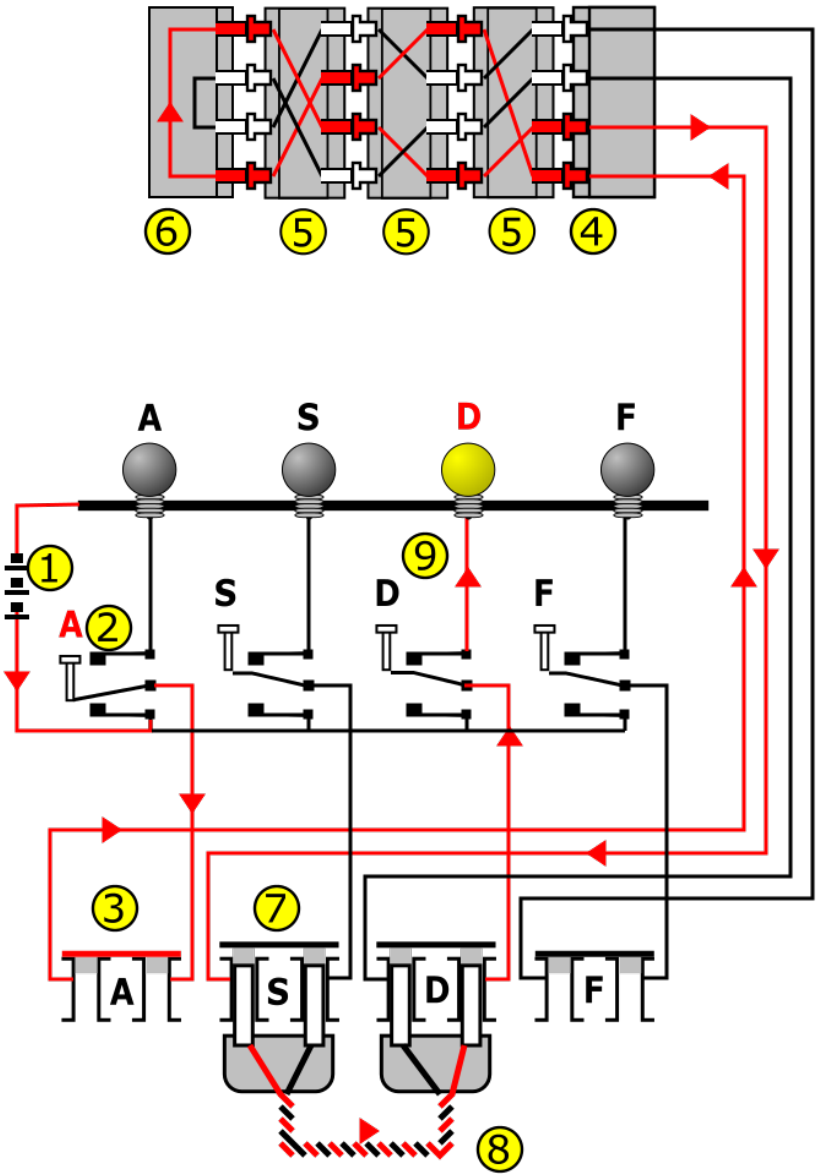
`geheimgeheimgeheim`
`Infoistvollsuper`

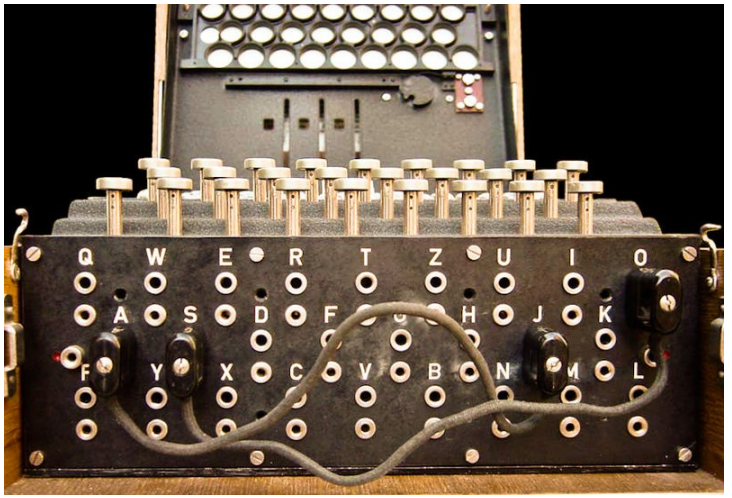
Klartextbuchstabe i

`ormsq...`

Kryptologie: Maschinen

Kryptologie: Maschinen





Von Bob Lord - German Enigma Machine, uploaded in english wikipedia on 16. Feb. 2005 by en:User:Matt Crypto, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=258976

Von MesserWoland - own work by user:HandigeHarry based on previous version based on Image:Enigma wiring kleur.png by Matt Crypto originally nl:Afbeelding:Enigma_wiring_kleur.png by nl:User:Drdefcom, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=1790479

Kryptologie: Maschinen

Die Nema ist eine Verschlüsselungsmaschine aus der Schweiz, die in den Jahrzehnten nach dem Zweiten Weltkrieg genutzt wurde. Auch sie wurde der Enigma nachempfunden, ist jedoch deutlich sicherer. Da die Schweiz nie in einen Krieg verwickelt wurde, kam es zu keinem Kriegseinsatz.

http://scienceblogs.de/klausis-krypto-kolumne/files/2013/07/Kryptologikum-NEMA.jpg

Kryptologie: Heute