

Kryptologie

The Codebreakers 1967:

Terminus Kryptologie bedeutet
sowohl Kryptografie als auch
Kryptoanalyse

Inhalt

- Überblick
- Monoalphabetische Chiffrierung
 - ▲ Transpositionschiffre
 - ▲ Verschiebechiffre
- Polyalphabetische Chiffrierung
 - ▲ Homophone Chiffren
 - ▲ Vigenère-Chiffre
- One-Time-Pad (OTP)
- Kryptoanalyse
- moderne Verfahren

Kryptologie

■ Kryptologie (Geheimschriften)

Steganografie
(gedeckte Geheimschriften)

eigentliche Kryptografie
(offene Geheimschriften)

Kryptologie



Steganografie

techn. Steganografie
(unsichtbare Geheimschriften)

linguistische Steganografie
(getarnte Geheimschriften)

Kryptologie



linguistische Steganografie

Semagramme
(sichtl. getarnte
Geheimschriften)

open code
(unersichtl. getarnte
Geheimschriften)

Kryptologie



open code

jargon code
(maskierte
Geheimschriften)

concealment cipher
(verschleierte
Geheimschriften)

Stichwort (cue)

Überblick

Kryptologie



concealment cipher

Würfel
(null cipher)

Raster
(grille)

Monoalphabetische Chiffrierung

■ Skytale von Sparta (~2500v. Chr.)

■ Klartext: HEUTE FLEXEN WIR!

■ Verschlüsselung: $Z = 3$

H E U

T E F

L E X

E N W

I R !

■ Ergebnis: H T L E I E E E N R U F X W !

Monoalphabetische Chiffrierung

■ Julius Caesar (100 - 44 v. Chr.)

■ Klartext: HALLO

■ Verschlüsselung: $Z = 3$

A B C D

d e f g

■ Ergebnis: KDOOR

Polyalphabetische Chiffrierung

■ Verschlüsselung:

A: 10 21 52 59 71

B: 20 34

C: 28 06 80

D: 04 19 70 81 87

E: 09 18 33 38 40 53 54 55 60 66 75 85 86 92 99

...

...

...

X: 44

Y: 48

Z: 64

■ Häufigkeit der Buchstaben wird verdeckt

Polyalphabetische Chiffrierung

■ Vigenère-Quadrat (~1550)

A	B	C	D	E	F	G	H	.	.	.
B	C	D	E	F	G	H	I	.	.	.
C	D	E	F	G	H	I	J	.	.	.
D	E	F	G	H	I	J	K	.	.	.
E	F	G	H	I	J	K	L	.	.	.
.
X	Y	Z	A	B	C	D	E	.	.	.
Y	Z	A	B	C	D	E	F	.	.	.
Z	A	B	C	D	E	F	G	.	.	.

■ Klartext: A F F E A F F E

■ Schlüssel: C A F E F L E X

■ Ergebnis: C F K I F Q J B

Vigenère Chiffre

Polyalphabetische Chiffrierung

■ Enigma (1. Weltkrieg 1917)



Enigma

ONE-TIME-PAD (OTP)

- Dieses Verfahren ist ABSOLUT sicher, wenn der Schlüssel:
 - ▲ genauso lange ist wie der Klartext
 - ▲ streng zufällig gewählt ist
 - ▲ nur ein einziges mal verwendet wird

Kryptoanalyse

- Brute Force Attacke
- Known Ciphertext Attacke
- Known Plaintext Attacke
- Chosen Plaintext Attacke
- Chosen Ciphertext Attacke
- Adaptive Chosen Plaintext Attacke

moderne Verfahren

symmetrische Algorithmen (secret key)

 DES (Data Encryption Standard)

 Triple DES

 RC4 (Ron`s Code 4)

 AES (Advanced Encryption Standard)

asymmetrische Algorithmen (public / private key)

 RSA (Namen: Rivest, Shamir, Adleman)

meine Idee

- Klartext mit symmetrische Chiffrierung verschlüsseln
- Geheimtext als Schlüssel für Asymmetrische Chiffrierung verwenden
- => One-Time-Pad ???

Quellen

- <http://cryptolounge.cjb.net>
- <http://www.crypto.de>
- <http://www.heise.de/ct/pgpCA>
- <http://www.tu-darmstadt.de>
- <http://senderek.de/security/schutz.html>