Klassische Chiffren

Ein erstklassiges Referat von:

Christian Ebner
Erhard Furtner

Quellenverzeichnis

- Brill, Manfred: Mathematik für Informatiker
  Hanser, ISBN 3-446-21733-9
- Sedgewick: Algorithmen und Datenstrukturen
- http://www.cryptolounge.cjb.net
- http://newmedia.idv.edu/thema/kryptographie/grundlagen.htm

Grundlegende Begriffe

- Kryptographie
- Kryptoanalyse
- Kryptoanalytiker
- Kryptologie
- Chiffrierung/Dechiffrierung
- Chiffretext
- Klartext

Anfänge der Kryptographie

- Steganographie bereits im alten Ägypten
- Entwicklung vorangetrieben von Militär, Kirchen, Geheimbünden
- Skytale
- Caesar Chiffre
- Rosenkreuzer Schablone

Schlüssel - Methode

- Probleme bisheriger Verfahren:
  Chiffre geknackt, wenn Methode bekannt wird
- also: Trennung von Schlüssel & Methode !
- Öffentliche Methode, geheimer Schlüssel
- Geheimtext nur mit entsprechendem Schlüssel dechiffrierbar

Transposition/Substitution

- Vertauschen der Zeichen im Klartext (Transp.)
- Ersetzen des Klartextalphabets durch ein Chiffrenalphabet (Subst.)
- Skytale von Sparta (Spaltentransposition):

```
SPARTAISTTOLL
```

U=3:

```
SPART
AISTT
OLL
```

Ergebnis: `SAOPILASLRTTT`

Transposition/Substitution (cont)

- Caesar-Chiffre (Additive Chiffrierung):

  k=3:

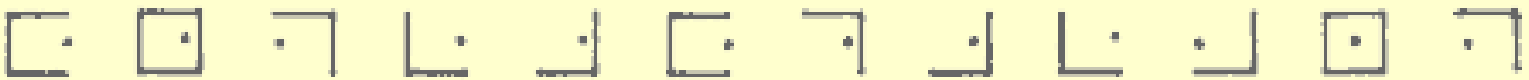
  Klartext: `VENIVIDIVICI`

  Geheimtext: `XGPKXKFKXKEK`

Monoalphabetische Substitution

- Ein einziges Chiffrenalphabet
- zB: Rosenkreuzer-Schablone

abc	def	ghi
jkl	mno	pqr
stu	vwx	yz



Polyalphabetische Substitution

- 1 Zeichen Klartext --> unterschiedliche Zeichen Geheimtext
- 1 Zeichen Geheimtext --> unterschiedliche Zeichen Klartext
- wichtig: Botschaft muss trotzdem eindeutig decodierbar sein

Polyalphabetische Substitution (cont)

- Vigenere Chiffre (Periodenanalyse):

  Klartext: `POLYALPHABETISCH`
  Schlüssel: `KRYPTOKRYPTOKRYP`
  Geheimtext: `ZFJNTZZYYQXHSJAW`

- One-Time-Pad

Polyalphabetische Substitution (cont)

- Alberti-Scheibe:

- Bringe die Ziffer 1 mit dem Buchstaben: i in Übereinstimmung.
- Dechiffriere sodann die ersten 7 Buchstaben.
- Drehe die Scheibe dann um 9 Schritte gegen den Gang der Sonne.
- Fahre fort, 13 Buchstaben zu dechiffrieren.
- .....

Anfänge Computerkryptologie

- Chiffrenzylinder
- Anfang 19. Jh. Enigma: mechanisch/elektronisch; bis zu 5 Chiffrenzylinder
- konventionelle Dechiffrierung enorm zeitaufwendig
- “brute force” Angriff erst dank Rechenmaschinen möglich

Kryptoanalyse - Einige Attacken

- Brute Force Attack
- Known Ciphertext Attack (zB. Vigenere)
- Known Plaintext Attack (Geheimtext/Klartext)
- Chosen Plaintext Attack (integrierter Schlüssel)
- Chosen Ciphertext Attack (Geheimtext)
- Adaptive Chosen Plaintext Attack
- Differentielle Kryptoanalyse (1990)

Einige Moderne Verfahren

- DES (IBM, 1977) --> EDE
- RC4
- Blowfish
- AES