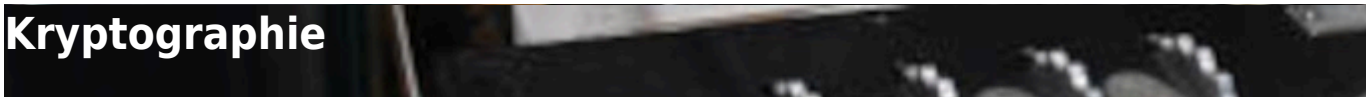
Kryptographie



[1)]

- Überblick

Einführung und klassische Verfahren

- Transpositions- und Substitutionschiffren
- Ziele der Kryptographie
- Vigenere Verschlüsselung
- Prinzipien der Kryptographie
- Einführung und klassische Verfahren
- One Time Pad & Knobeln

Mechanische Verfahren

Basierend auf zu Beginn des 20. Jahrhunderts neu aufgekommenen Technologien, wie der elektrischen Schreibmaschine und dem Fernschreiber, kamen teilweise unabhängig voneinander und nahezu zeitgleich mehrere Erfinder auf die Idee, Texte mit (elektro-)mechanischen Verschlüsselungsmaschinen zu verschlüsseln. Diese Maschinen sind inzwischen durch moderne Verschlüsselungsalgorithmen weitgehend abgelöst.

- Ein bekanntes Beispiel für eine solche Maschine war die Enigma

Moderne Verfahren

Symmetrische Verfahren

- Moderne symmetrische Verfahren
- Chiffrendesign
- AES etwas genauer

Asymmetrische Verfahren

- Warum reicht symmetrische Kryptographie nicht aus?
- Die Kryptobox als Modell
- Etwas Mathematik
- Das RSA Verfahren
- RSA Schritt für Schritt
- Hybride Verfahren
- Diffie-Hellman Schlüsselaustausch
- Hashfunktionen
- Signaturen
- Authentizitätsprobleme

- Public-Key-Infrastrukturen

Praxis

- Übungsaufgabe zur Signatur mit RSA
- GnuPG auf der Kommandozeile
- Hintergrund: Große Primzahlen- Das Miller Rabin Verfahren
- Werkzeuge zur Dateiverschlüsselung
- Verschlüsselte Mails mit Thunderbird
- Rückblick: Kontrollfragen zur Kryptographie

1)

Photo by Mauro Sbicego on Unsplash