[1)]

# Kryptographie

- Überblick

## Einführung und klassische Verfahren

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

## 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

From:
https://info-bw.de/ -

Permanent link:
**https://info-bw.de/faecher:informatik:oberstufe:kryptographie:start?rev=1697738709**

Last update: **19.10.2023 18:05**