



Kryptographie

- Überblick

Einführung und klassische Verfahren

- Transpositions- und Substitutionschiffren
- Ziele der Kryptographie
- Vigenere Verschlüsselung
- Prinzipien der Kryptographie
- Einführung und klassische Verfahren

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
- Authentizität

Praxis

- GnuPG auf der Kommandozeile
- 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=1648719049>

Last update: **31.03.2022 09:30**

