



# 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
- 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)

<html>Photo by <a href=„[https://unsplash.com/@maurosbigego?utm\\_source=unsplash&utm\\_medium=referral&utm\\_content=creditCopyText](https://unsplash.com/@maurosbigego?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)“>Mauro Sbicego</a> on <a

Last update: 31.03.2022 10:39 faecher:informatik:oberstufe:kryptographie:start <https://wiki.qg-moessingen.de/faecher:informatik:oberstufe:kryptographie:start?rev=1648715994>

---

href=„[https://unsplash.com/s/photos/cryptography?utm\\_source=unsplash&utm\\_medium=referral&utm\\_content=creditCopyText](https://unsplash.com/s/photos/cryptography?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)“>Unsplash</a></html>

From:  
<https://wiki.qg-moessingen.de/> - **QG Wiki**

Permanent link:  
<https://wiki.qg-moessingen.de/faecher:informatik:oberstufe:kryptographie:start?rev=1648715994>

Last update: **31.03.2022 10:39**

