[1)]

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
- Authentizitätsprobleme

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/@maurosbicego?utm_source=unsplash&utm_medium=referral&amp

;utm_content=creditCopyText“>Mauro Sbicego on Unsplash</html>