20.1.2020

Allgemeine Ziele der Kryptographie

- Confidentiality: (Vertraulichkeit)
- Integrity (Daten nicht verändert worden)
  Prüfsumme
- Authentication (Genau wer)
- Nonrepudiation

Diffi, Hellman, Bruce Schneier, NSA,

RSA: Rivest, Shamir, Adleman.

Symmetrische - Verschlüsselung:

TEA, Feistel structure

AES = Advanced Encryption Standard

Asymmetrisch

RSA - Schlüssel verschlüsseln != Key entschlüsseln

Diffie - Hellmann

27.1.2020

Wiederholung