18 Kann-Liste Cryptografic

Peter Rutschmann

17.12.2025

Kann Liste Cryptografic

Ceasar

- Ich kann die Ceasar Verschlüsselung erklären (ZBsp. Verfahren, Prinzip, Schlüssel..)
- Ich kann eine Nachricht mit der Ceasar Verschlüsselung verschlüsseln und entschlüsseln.
- Ich kann die Sicherheit der Ceasar Verschlüsselung beurteilen.
- Ich kann eine Brute-Force-Attacke auf die Ceasar Verschlüsselung erklären und durchführen.

Vigenere

- Ich kann den Unterschied zwischen monoalphabetischer und polyalphabetischer Verschlüsselung erklären.
- Ich kann die Vigenere Verschlüsselung erklären (ZBsp. Verfahren, Prinzip, Schlüssel..)
- Ich kann eine Nachricht mit der Vigenere Verschlüsselung verschlüsseln und entschlüsseln.
- Ich kann die Sicherheit der Vigenere Verschlüsselung beurteilen.
- Ich kann eine Kasiski-Attacke auf die Vigenere Verschlüsselung erklären und durchführen.

Symmetrische Verschlüsselung

- Ich kann das Prinzip der symmetrischen Verschlüsselung erklären.
- Ich kann drei typische symmetrische Verschlüsselungsverfahren (aus der Informatik) nennen.
- Ich kann die binäre Darstellung einer Nachricht erklären.

- Ich kann den Unterschied zwischen Binär, Dezimal und Hexadezimal erklären.
- Ich kann den Zwecke von ASCII und UTF8 erklären.
- Ich kann eine Nachricht in Binär, Dezimal und Hexadezimal umwandeln und umgekehrt. (mit Hilfe einer Tabelle)
- Ich kann die XOR Verschlüssel erklären (ZBsp. Verfahren, Prinzip, Schlüssel..)
- Ich kann eine Nachricht mit der XOR Verschlüsselung verschlüsseln und entschlüsseln.
- Ich kenne den Zusammenhang von Klartext, Schlüssel und Geheimtext bei der XOR Verschlüsselung. (habe ich zwei davon, kenne ich den dritten. Egal welche zwei!)
- Ich kann die Sicherheit der XOR Verschlüsselung beurteilen.
- Ich kann mit einem umvollständigen Schlüssel eine teilweise Entschlüsselung durchführen. Und dann den Schlüssel ergänzen.
- Ich kann die AES Verschlüsselung erklären (ZBsp. Verfahren, Prinzip, Schlüssel..)
- Ich kann diese Verfahren erklären und anwenden
  - Transformation
  - Substitution
  - Transposition/Permutation
- Ich kann diese Verfahren mit einem kurzen Satz erklären
  - Diffusion
  - Konfusion
  - Rundensystem
  - Key Schedule
  - Blockchiffre
  - Stromchiffre
- Ich kann eine Nachricht mit der AES Verschlüsselung verschlüsseln und entschlüsseln (mit Hilfsmittel).
- Ich kann die Sicherheit der AES Verschlüsselung beurteilen.

Schlüsselaustausch

- Ich kann das Problem des Schlüsselaustauschs erklären.
- Ich kann die Bedetung des Schlüsselsaustausch bei HTTPS erklären.
- Ich kann das Prinzip des Deffie-Hellman Verfahrens erklären.

Asymetrische Verschlüsselung

- Ich kann das Prinzip der asymmetrischen Verschlüsselung erklären.
- Ich kann die RSA erklären (ZBsp. Verfahren, Prinzip, Schlüssel..)
- Ich kann eine Nachricht mit der RSA Verschlüsselung verschlüsseln und entschlüsseln.
- Ich kann die Sicherheit der RSA Verschlüsselung beurteilen.

Signatur

- Ich kann das Prinzip und die Funktionsweise einer digitalen Signatur erklären.
- Ich kann den Unterschied zwischen Verschlüsselung und Signatur erklären.
- Ich kann die Sicherheit einer digitalen Signatur beurteilen.
- Ich kann eine Signatur anwenden.

Informationen zur Lernkontrollen

- Lösen auf Papier ohne Hilfsmittel (Taschenrechner, Smartphone, Laptop, Internet)
- UTF8, HEX, BIN, DEC Tabellen werden zur Verfügung gestellt.
- Sie dürfen einen einseitig von Hand geschriebenen Spickzettel mitbringen.
- Zeit der Lernkontrolle: ca. 30 Minuten