Kryptographie

Von der Wahlpflicht bis zum Neigungskurs

Katrin Büttner

MS „J.W.v. Goethe“
Heidenau

katrin.buettner@arcor.de

Thomas Knapp

MS Kötzschenbroda
Radebeul

msk-knapp@gmx.de

Inhalte

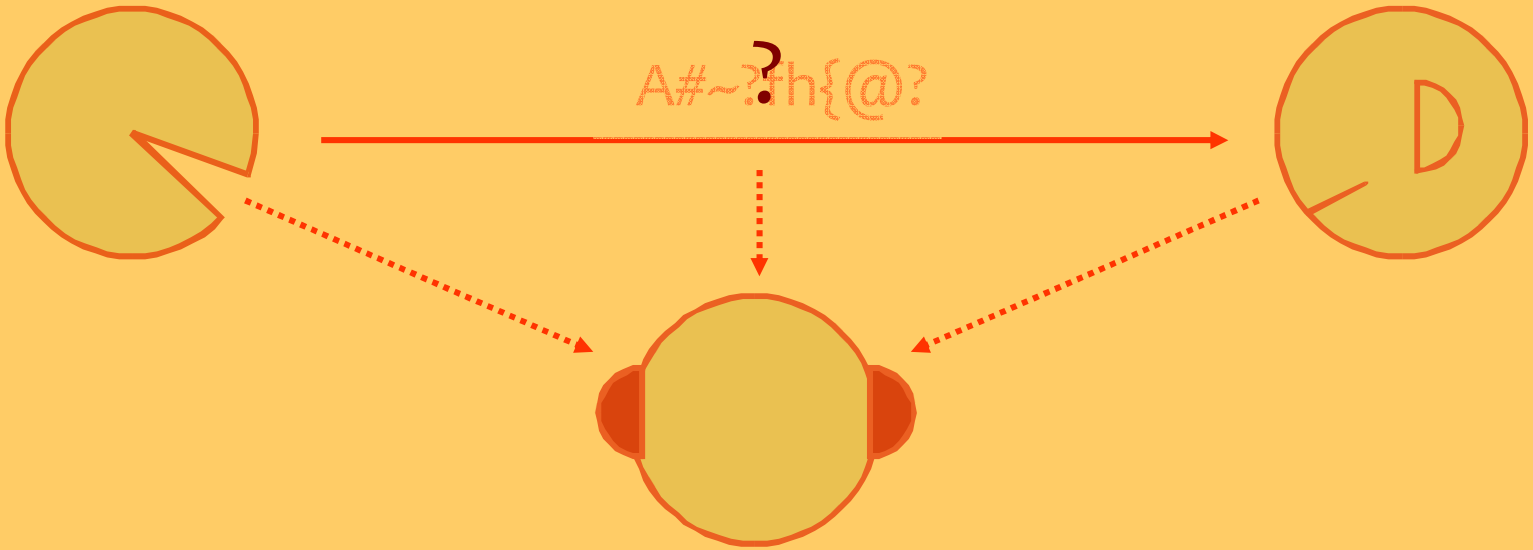
1. Grundlagen, Begriffe, Vereinbarungen
2. Wahlpflichtbereich 2
3. ein möglicher Neigungskurs

Inhalte

1. Grundlagen, Begriffe, Vereinbarungen
2. Wahlpflichtbereich 2
3. ein möglicher Neigungskurs

Grundlagen, Begriffe, …

- Sender, Empfänger
- Nachricht
- (Angreifer)



Achtung - Definition

Codieren

- Bringe die Nachricht in eine übertragbare Form.

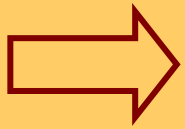
  z.B.: Brieftaube, Morsealphabet, Blindenschrift, ASCII, Englisch

Chiffrieren

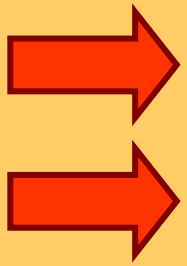
- Bringe die Nachricht in eine geheime Form.

  z.B.: Skytale, Atbash, Cäsar, Vignére, OTP

Übung Cäsar, Vignére



- Verschlüsselung
  - Verfahren (Algorithmus, öffentlich)
  - Schlüssel (geheim)
- Verfahren – Substitution
  - Atbash, Cäsar, Vignére, One-Time-Pad, …
- Verfahren – Transposition
  - Skytale, Gartenzaun, ADFX, Anagramme (Sakrileg), …



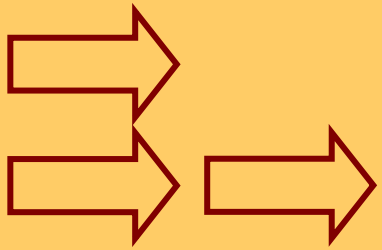
Inhalte

1. Grundlagen, Begriffe, Vereinbarungen
2. Wahlpflichtbereich 2
3. ein möglicher Neigungskurs

WP2 von KlSt 7 bis 10

siehe LP

7. Begriffe, Verfahren, Beispiele
8. mithilfe von Programmen (TK, TV)
9. Anwendung im Netz
10. Steganografie



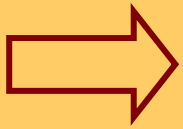
Inhalte

1. Grundlagen, Begriffe, Vereinbarungen
2. Wahlpflichtbereich 2
3. ein möglicher Neigungskurs

ein möglicher Neigungskurs

Ziele:

- Kennen Bedeutung fehlerfreier Kommunikation
- Kennen/Können Codier- und Chiffrier-Verfahren (Ausdauer, Genauigkeit, …)
- Kooperative Zusammenarbeit beim Austausch von Nachrichten
- Arbeit im Projekt (Fackeltelegraf)



Beispiele, Beispiele, …

- Fackeltelegraf (auch: Ge, Deu) ⇨
- EAN, ISBN, Kontonummer (auch: Ma, WTH, Gk) ⇨
- „Knacken“ von ⇨
  verschlüsselten Texten (Kryptoanalyse)
  Handhabung Textverarbeitung und
  Tabellenkalkulation (auch: Ma, Info, Deu)
- andere Werkzeuge
  - Steganografie (auch: Ku)
  - CrypTool