technische universität
dortmund

Sicherheit: Fragen und Lösungsansätze

Thomas Ruhroth | Dortmund

PA1

- Verschlüsselung

- Ziele:
  - Block- und Streamchiffren verstehen.
  - Verstehen, wann eine Verschlüsselung „knackbar“ ist.

Präsenzübung

Zweiergruppen (Person A und Person B)

- Person A ist Prüfer und stellt Person B fragen
- Hinweise für den Prüfer
  - Fragen Sie nach, wenn etwas unklar erscheint
  - Fragen Sie zusätzliche 2-3 Details aus der Antwort nach
- Hinweis für den Prüfling
  - Nutzen Sie Stift und Zettel um Sachverhalt auch optisch darzustellen
- Wenn die Zeit um ist wechseln Sie bitte die Rollen

Person A

- Was ist ein kryptographisches Verfahren?
- Erklären Sie „Blockchiffre“.
- Was sind die Vor- und Nachteile einer Blockchiffre?

Person B

- Was ist ein One-Time-Pad?
- Erklären Sie „Stromchiffre“.
- Was sind die Vor- und Nachteile einer Stromchiffre?

Caesar-Verschlüsselung

```
Klar:    a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheim:  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

$$encrypt_{K(P)} = (P + K) \bmod 26$$

$$decrypt_{K(P)} = (P - K) \bmod 26$$

- Ist das Verfahren symmetrisch oder asymmetrisch?
- Ist das Verfahren sicher? Beantworten Sie die Frage bitte für alle verschiedenen Kriterien aus der Vorlesung.

Verwürfeltes Geheimalphabet

- Geheimwort
  - „Regenschirmstaender“
- Doppelte Buchstaben eliminieren:
  - REGNSCHIMTAD
- Zuordnen:
  - Erste Buchstaben zum Wort und dann Rest alphabetisch

```
Klar:   abcdefghijklmnopqrstuvwxyz
Geheim: REGNSCHIMTADBFJKLOPQUVWXYZ
```

- Ist das Verfahren symmetrisch oder asymmetrisch?
- Ist das Verfahren sicher? Beantworten Sie die Frage bitte für alle verschiedenen Kriterien aus der Vorlesung.

Atbasch

Revertiertes Alphabet:

```
  Klar: abcdefghijklmnopqrstuvwxyz
Geheim: ZYXWVUTSRQPONMLKJIHGFEDCBA
```

- Ist das Verfahren symmetrisch oder asymmetrisch?
- Ist das Verfahren sicher? Beantworten Sie die Frage bitte für alle verschiedenen Kriterien aus der Vorlesung.