Kontrollfragen: Klassische

Verschlüsselungsverfahren

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de, Raum 149B
Version: 1.0.0

1. Allgemeine Fragen

Kontrollfragen

1.1. Was ist der Unterschied zwischen Kryptoanalyse und Kryptologie?

1.2. Welche Aussage über den Brute-Force-Angriff ist korrekt?

- Ein Brute-Force-Angriff erfordert keinerlei Wissen über den Klartext.
- Im Durchschnitt muss beim Brute-Force-Angriff die Hälfte aller möglichen Schlüssel ausprobiert werden.

1.3. Was unterscheidet einen „Chosen Plaintext"-Angriff von einem „Known Plaintext"-Angriff?

1.4. Warum ist ein großer Schlüsselraum allein keine hinreichende Bedingung für ein sicheres Verschlüsselungsverfahren?

1.5. Was ist der wesentliche Unterschied zwischen einer Substitutions- und einer Transpositions-Chiffre?

1.6. Welchen grundlegenden Nachteil haben alle klassischen Transpositions-Chiffren gemeinsam?

1.7. Worin besteht der Vorteil der Steganografie gegenüber der Verschlüsselung – und wo liegt ihre größte Schwäche?

1.8. Was sind die zwei grundlegenden Voraussetzungen für den sicheren Einsatz eines symmetrischen Verschlüsselungsverfahrens?

2. Chiffren

Kontrollfragen

2.1. Ist die Cäsar-Chiffre bedingungslos sicher oder „nur“ rechnerisch sicher?

2.2. Was ist das Grundprinzip der Playfair-Chiffre, und warum ist sie schwerer zu brechen als eine einfache monoalphabetische Substitution?

2.3. Welche der folgenden Eigenschaften treffen auf das One-Time-Pad zu?

- Es bietet nachweislich perfekte Geheimhaltung.
- Der Schlüssel darf kürzer als die Nachricht sein, wenn er wiederholt wird.
- Es ist praktisch für den Einsatz in stark genutzten Kommunikationssystemen geeignet.
- Der Schlüssel muss wirklich zufällig sein.

2.4. Warum ist die Vigenère-Chiffre stärker als eine monoalphabetische Substitutions-Chiffre?

2.5. Welchen Vorteil bietet das Vigenère-Autokey-System gegenüber der klassischen Vigenère-Chiffre – und welche Schwäche bleibt?

2.6. Warum ist die Rail-Fence-Chiffre keine Substitutions-Chiffre?

2.7. Ein Angreifer kennt nur den Geheimtext einer mit der Cäsar-Chiffre verschlüsselten Nachricht. Um welche Art von Angriff handelt es sich, und wie viele Versuche sind im schlechtesten Fall nötig?