# Fragenkartalog Symetrische Verschlüsselung

1. Was versteht man unter symmetrischer Verschlüsselung.

2. Wie kommen die Akteure der Kryptografie zu ihren Namen?

3. Erklären sie die Begriffe Kryptografie, Kryptoanalyse, Kryptologie. Wie hängen diese Begriffe zusammen?

4. Wie funktioniert die Stabchiffre?

5. Wie funktioniert die Caesar Chiffre?

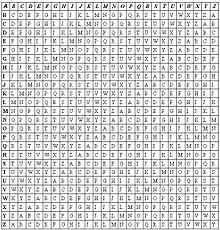
6. Warum ist eine mit Rotationschiffre verschlüsselte Nachricht leicht zu entschlüsseln?

7. Wie funktioniert die Vigenère-Chiffre? Welche Möglichkeit gibt es mit Vigenère verschlüsselte Nachrichten zu entschlüsseln?

Erstellen sie pro Frage eine kurze Erklärung bzw. wo möglich eine kleine Skizze.

1. Absender und Empfänger haben den gleichen Schlüssel
2. der Anfangsbuchstabe gibt Aufschluss über den Akteur (A = Alice,…)
3. Krypto bedeutet auf Deutsch geheim. Die Kryptografie bedeutet, dass man einen Klartext verschlüsselt, Kryptoanalyse hingegen ist das Entziffern und die Kryptologie beschäftigt sich mit beiden.
4. Der Durchmesser des Stabes ist der Schlüssel. Ein Band wird um den Stab gewickelt und wenn der Stab den richtigen Durchmesser hat, kann man die Nachricht entschlüsseln, ansonsten wären die Buchstaben verschoben.
5. Die „echte“ Caeser Chiffre (ROT-3-Verschlüsselung) funktioniert, indem man jeden Buchstaben des Alphabets um eine gewisse Anzahl verschiebt. Beim decodieren wird dieser Vorgang rückgängig gemacht.
6. Weil alle Wörter die gleiche Länge haben und Buchstaben, die in einer Sprache sehr häufig vorkommen, kommen wahrscheinlich im Chiffretext als ein anderer Buchstabe auch sehr häufig vor (es sei denn, der Chiffretext der geheimen Botschaft lautet „Fußballnationalmannschaft“, da kommt kein einziges „E“ vor…). Mit dieser Methode lässt sich auch ohne Schlüssel rückvollziehen, wie der Klartext lautet.
7. Man hat ein Schlüsselwort und verschiebt den 1. Buchstaben des Klartextes soweit, wie der 1. Buchstabe des Passwortes vom A entfernt ist. Den 2. Buchstaben des Klartextes mit dem 2. Buchstaben des Passwortes, den 3. Buchstaben um den 3. Buchstaben…

(Bild nächste Seite)



Gleiche Wortgruppen kommen oft vor und so lässt sich die Länge des Passwortes herausfinden, man teilt das Alphabet in (Länge des Passwortes) viele Gruppen und entschlüsselt mithilfe der Kasiski-Test Methode