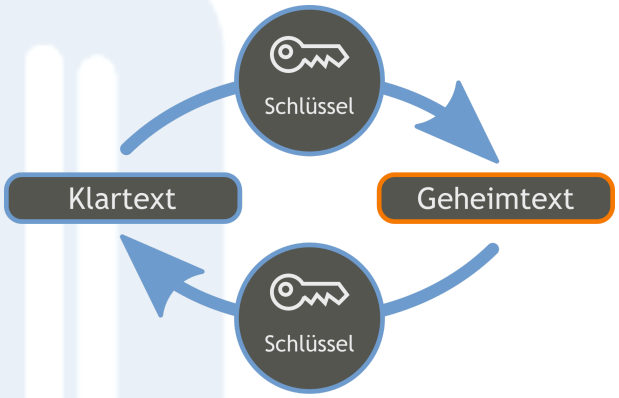
Kryptographie

Kryptographie befasst sich mit dem Thema **Informationssicherheit**, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind.

Verschlüsselungsverfahren sollen Informationen widerstandsfähig gegen unbefugtes Lesen machen.

- Beim **Verschlüsseln** wird ein **Klartext** mit Hilfe eines **Schlüssels** in einen **Geheimtext** überführt.
- Beim **Entschlüsseln** wird der **Geheimtext** mit einem **Schlüssel** in den **Klartext** zurückgeführt.



Cäsar- und **Freimaurerchiffre** sind sehr einfache Verschlüsselungsverfahren, die jedoch Funktionsweise und Angriffsmöglichkeiten gut verdeutlichen.

Aktuelle Verschlüsselungsverfahren sind als symmetrisches Verfahren der **Advanced Encryption Standard (AES**) und als asymmetrisches Verfahren der Algorithmus von **Rivest-Shamir-Adleman (RSA**).

Wo findet sich Kryptographie im Informatik-Studium?

Kryptografische Verfahren werden in verschiedenen Veranstaltungen gelehrt, z.B. in den Vorlesungen **“Foundations of Cybersecurity 1”** und **“Security”**.

Kryptographie ist Pflicht im Bachelor-Studiengang **“Cybersecurity”**.

In anderen **Bachelor-Studiengängen der Informatik** kann Kryptographie in **Wahlbereichen** belegt werden.

Cäsar-Verschlüsselung

Was ist die Cäsar-Verschlüsselung?

Die Caesar-Scheibe ist eine einfache Verschlüsselungsmethode aus der Antike, die vom römischen Kaiser Julius Caesar verwendet wurde. Sie basiert auf der Idee, jeden Buchstaben im Alphabet um eine feste Anzahl von Positionen zu verschieben. Diese Anzahl nennt man den Schlüssel.

Beispiel:
Wenn die Verschiebung 3 ist, wird aus „A“ ein „D“, aus „B“ ein „E“ und so weiter. Das Alphabet „rotiert“ also um 3 Positionen.

Die Cäsar Scheibe

Zum Verschlüsseln und Entschlüsseln nutzen wir eine sogenannte Cäsar Scheibe. Sie besteht aus einem inneren und einem äußeren Ring.Die innere (bunte) Scheibe kann gedreht werden. Damit stellt man ein, wie weit das Alphabet verschoben wird.

Man dreht die innere bunte Scheibe so oft wie es der Schlüssel angibt. Danach verändern wir die Drehung nicht mehr.

Zum Verschlüsseln sucht man den Buchstaben auf dem äußeren Ring (Klartextalphabet) und ersetzt ihn mit dem Buchstaben (Geheimtextalphabet) untendrunter.

Zum Entschlüsseln sucht man den Buchstaben im inneren Ring (Geheimtext-alphabet) und ersetzt ihn durch den oben drüber (Klartextalphabet).

Aufgabe 1: Verschlüsseln mit der Cäsar-Scheibe

1. Nutze die Caesar-Scheibe mit einem **Schlüssel von 3**, um folgende Wörter zu verschlüsseln:

   a) **C A E S A R**
   b) **K R Y P T O**

   Schreibe die verschlüsselten Wörter hier auf:

   a) __ __ __ __ __ __

   b) __ __ __ __ __ __

Aufgabe 2: Entschlüsseln mit der Cäsar-Scheibe

1. Entschlüssele die folgenden Wörter. Auch ist der **Schlüssel 3**:

   a) **L Q I R O D E**
   b) **V F K O X H V V H O**

   Schreibe die entschlüsselten Wörter hier auf:

   a) __ __ __ __ __ __ __

   b) __ __ __ __ __ __ __ __ __ __

Alle Links befinden sich auf der Webseite des InfoLab: infolab.cs.uni-saarland.de

Freimaurer-Chiffre

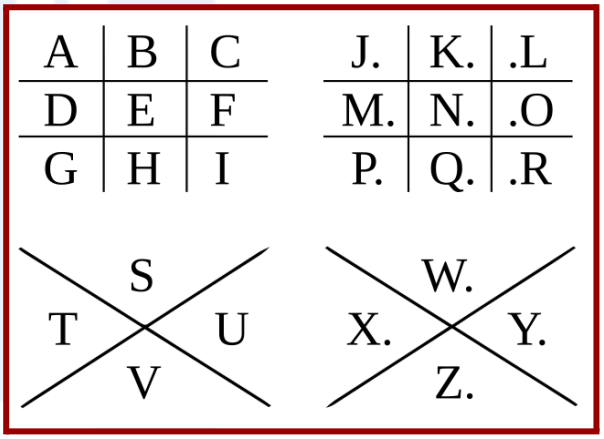
Einführung in die Freimaurer-Chiffre

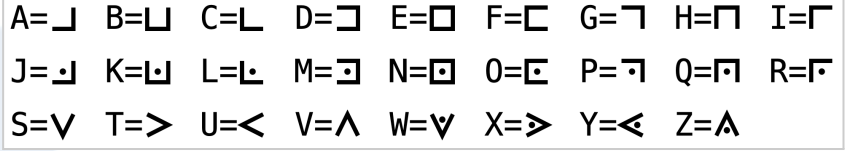
Die Freimaurer-Chiffre ist eine einfache Geheimschrift, bei der Buchstaben durch Symbole ersetzt werden. Sie wurde nicht von den Freimaurern erfunden, aber von ihnen verwendet, um Nachrichten verschlüsselt darzustellen. Die Symbole basieren auf einem einfachen Raster- und Kreuz-Schema.

So funktioniert die Freimaurer-Chiffre

1. Das Alphabet wird in zwei **Raster** und zwei **Kreuze** aufgeteilt:
   - Die ersten 9 Buchstaben des Alphabets werden in ein 3x3-Raster eingetragen.
   - Die nächsten 9 Buchstaben werden in ein weiteres 3x3-Raster geschrieben, aber dieses Mal mit einem Punkt in jedem Kästchen.
   - Die letzten 8 Buchstaben werden in zwei Kreuzstrukturen angeordnet, ebenfalls mit und ohne Punkt.
2. Für jeden Buchstaben gibt es nun ein Symbol. Es basiert auf dem Kästchen, in dem der Buchstabe steht:
   - Die Form des Kästchens bestimmt das Grundsymbol.
   - Ein Punkt im Kästchen zeigt an, dass es sich um den zweiten Buchstabensatz handelt.

Hier ist das Raster, das du für das Verschlüsseln und Entschlüsseln verwenden kannst:





Aufgaben zur Freimaurer-Chiffre

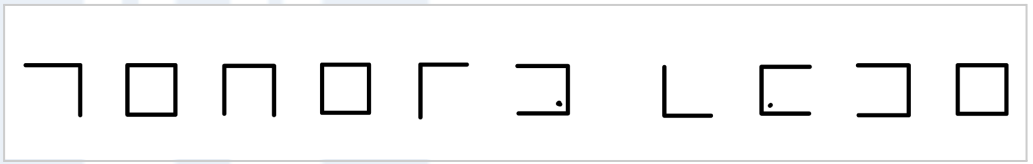
Aufgabe 1: Verschlüsseln

Verschlüssele die folgende Nachricht mit der Freimaurer-Chiffre:

INFORMATIK

Aufgabe 2: Entschlüsseln

Entschlüssele die folgende Nachricht. Sie wurde mit der Freimaurer-Chiffre verschlüsselt:



Alle Links befinden sich auf der Webseite des InfoLab:
infolab.cs.uni-saarland.de