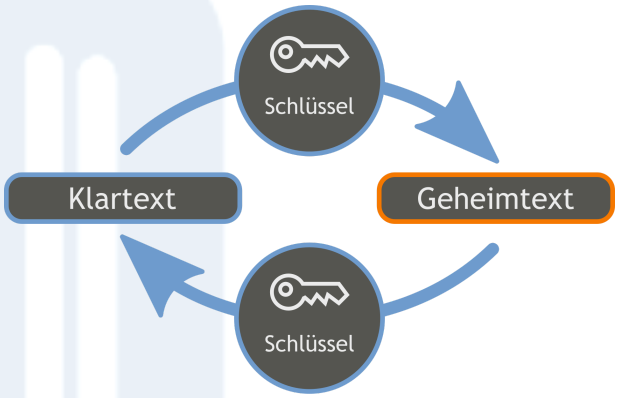
Kryptographie

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.