Verschlüsselung

Geschichtlicher Hintergrund

- Anfänge der Verschlüsselung -> Ägypter (2000 v. Chr.)
- Atbash
    - Von hebräischen Gelehrten verwendet (500 v. Chr.)
    - Buchstaben wurden umgedreht

      ```
      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
      Z Y X W V U T S R Q P O N M L K J I H G F E D C B A
      ```

    - APFEL -> ZKUVO
- Enigma
    - Verschlüsselungsmaschine des deutschen Militärs im 2. Weltkrieg
    - Stärke: Buchstabe wird abhängig von seiner Position in verschiedene Zeichen verschlüsselt -> aus A kann z. B. einmal ein B werden, an anderer Stelle ein K
    - Mit Hilfe von Alan Turing entschlüsselt

Allgemeines

- Klartext -> Schlüssel -> Geheimtext (Chiffrat)
- Symmetrische Verschlüsselung
    - Derselbe Schlüssel bei Ver- und Entschlüsselung
    - Schlüssel muss Sender und Empfänger bekannt sein und ausgetauscht werden
    - Knackbar, wenn unbefugte Person den Schlüssel herausfindet
    - Beispiel: Caesar-Verschlüsselung
- Asymmetrische Verschlüsselung
    - Unterschiedliche Schlüssel für Ver- und Entschlüsselung
    - Verschlüsselungs-Schlüssel (public key) kann öffentlich sein
    - Entschlüsselungs-Schlüssel (private key) darf nur Sender und Empfänger bekannt sein

Die Caesar-Verschlüsselung

- Symmetrische Verschlüsselung
- Wurde von Julius Cäsar für seine militärische Kommunikation verwendet
- Jeder Buchstabe wird um eine festgelegte Anzahl (= Schlüssel) an Stellen verschoben
- Einfach, aber leicht knackbar
- Beispiel:

Klartext:	APFEL
Schlüssel:	3
Geheimtext:	DSIHO

Die Vigenère-Verschlüsselung

- Der „bessere“ Cäsar
- Symmetrische Verschlüsselung
- Jeder Buchstabe wird um eine unterschiedliche Anzahl an Stellen verschoben – Anzahl an Stellen = Buchstabennummer im Alphabet
- Beispiel:

Klartext:	APFEL
Schlüssel:	abc
Geheimtext:	B (a = 1)
	R (b = 2)
	I (c = 3)
	F (a = 1)
	N (b = 2)