Kryptographie

Wissenschaft, die sich damit beschäftigt, wie Texte (Nachrichten) so verschlüsselt werden können, dass eine nicht authorisierte Entschlüsselung verhindert wird.

Kryptoanalyse

Wissenschaft, die sich mit dem Brechen (Knacken) vorhandener Kryptosysteme beschäftigt.

Kryptologie

Umfasst die beiden Gebiete **Kryptographie** und **Kryptoanalyse**.

Kryptosystem

Definition:

Ein Kryptosystem (oder auch Chiffre) ist ein Quintupel $\mathbf{S} = (M, C, K, \mathscr{E}, \mathscr{D})$

Zur Bedeutung der einzelnen Teile des Kryptosystems

- M, C und K sind endliche Mengen
  - M – Klartextraum (englisch: »message space«)
  - C – Schlüsseltextraum (englisch: »ciphertext space«)
  - K – Schlüsselraum (englisch: »key space«)
- $\mathscr{E} = \{E_k \mid k \in K\}$ ist eine Familie von Funktionen $E_k : M \to C$, die für die Verschlüsselung (englisch: »encrypt«) verwendet werden. $\mathscr{D} = \{D_k \mid k \in K\}$ ist eine Familie von Funktionen $D_k : C \to M$, die für die Entschlüsselung (englisch: »decrypt«) verwendet werden.
- Für jeden Schlüssel $e \in K$ gibt es einen passenden Schlüssel $d \in K$, so dass für jede Nachricht $m \in M$ folgende Gleichung zutrifft: $D_d(E_e(m)) = m$

Ein **symmetrisches** (»private-key«) Kryptosystem erfüllt die Bedingung: $d = e$
D. h. es gibt einen gemeinsamen Schlüssel, der verwendet wird, um die Nachricht zu verschlüsseln und die verschlüsselte Nachricht zu entschlüsseln.

Ein **asymmetrisches** (»public-key«) Kryptosystem erfüllt die Bedingung: $d \neq e$ **und** d praktisch(!) nicht aus e berechnet werden kann. d ist hier der private und e der öffentliche Schlüssel.

Die in diesem Informationsblatt angegebenen Elemente orientieren sich an den Einordnungen in (**Rothe2008**).