Klassische Kryptographie

- Einige einfache Kryptosysteme -

4 Regeln bei Kryptosystemen

- **Authentizität:** Es soll sichergestellt sein, dass die empfangene Nachricht vom angegebenen Sender stammt.
- **Integrität:** Es soll sichergestellt sein, dass eine Fälschung oder Manipulation der Nachricht nicht möglich ist.
- **Vertraulichkeit:** Es darf nicht möglich sein, dass Dritte mitlesen können oder Einblick haben.
- **Verbindlichkeit:** Der Absender kann später nicht leugnen, die Nachricht abgeschickt zu haben.

Block-Chiffrierung

Definition: Ein Kryptosystem ist ein Fünf-Tupel (P,C,K,E,D) mit folgenden Eigenschaften:

1. P ist eine endliche Menge von möglichen Klartexten
2. C ist eine endliche Menge von möglichen Chiffretexten
3. K ist eine endliche Menge von möglichen Schlüsseln
4. Für jedes $k \in K$ gibt es eine Chiffrierungsregel $e_K \in E$ und eine zugehörige Dechiffrierungsregel $d_K \in D$. Die Funktionen $e_K : P \rightarrow C$ und $d_K : C \rightarrow P$ müssen durch effiziente Algorithmen berechenbar sein und für jedes $x \in P$ gilt $d_K(e_K(x)) = x$.

Monoalphabetische Kryptosysteme

Kryptosystem 1.1: Verschiebungschiffre (Shift Cipher)

Sei $P=C=K=\mathbb{Z}_{26}$. Für $0 \leq K \leq 25$ definiere

$$e_K(x) = (x + K) \bmod 26$$

und

$$d_K(y) = (y - K) \bmod 26$$

$(x,y \in \mathbb{Z}_{26})$.

Kryptosystem 1.2: Substitutionschiffre (Substitution Cipher)

Sei $P = C = \mathbb{Z}_{26}$, und K sei die Menge aller Permutationen der 26 Zeichen 0,1,...,25.
Für jede Permutation $\pi \in K$ definiere

$$e_\pi(x) = \pi(x)$$

und

$$d_\pi(y) = \pi^{-1}(y)$$

wobei π^{-1} die inverse Permutation von π sei.

Kryptosystem 1.3: Affin-Lineare Chiffre (Affin Cipher)

Sei $P = C = \mathbb{Z}_{26}$, und sei $K = \{ (a,b) \in \mathbb{Z}^{26} \times \mathbb{Z}^{26} : ggT(a,26) = 1\}$.
Für $k = (a,b) \in K$ definiere

$$e_k(x) = (ax + b) \bmod 26$$

und

$$d_k(y) = a^{-1}(y - b)$$

$(x,y \in \mathbb{Z}_{26})$.

Polyalphabetische Kryptosysteme

Kryptosystem 1.4: Vigenère Chiffre (The Vigenère Cipher)

Sei m eine positive Zahl und $P = C = K = (\mathbb{Z}_{26})^m$. Für einen Schlüssel $k = (k_1,k_2,...,k_m)$ definiere

$$e_k(x_1,x_2,...,x_m) = (x_1 + k_1, x_2 + k_2,...,x_m + k_m)$$

und

$$d_k(y_1,y_2,...,y_m) = (y_1 - k_1, y_2 - k_2,...,y_m - k_m)$$

wobei alle Oparationen in $\mathbb{Z}_{26}$ ausgeführt werden.

Kryptosystem 1.5: Hill Chiffre (Hill Cipher)

Sei $m \geq 2$ eine Zahl, $P = C = (\mathbb{Z}_{26})^m$ und $K = \{m \times m$ Matrizen mit inverser Matrix über $\mathbb{Z}_{26}\}$.
Für jeden Schlüssel k definiere

$$e_k(x) = xk$$

und

$$d_k(y) = yk^{-1}$$

wobei alle Oparationen in $\mathbb{Z}_{26}$ ausgeführt werden.

Kryptosystem 1.6: Permutation-Chiffre (Permutation Cipher)

Sei m eine positive Zahl, $P = C = (\mathbb{Z}_{26})^m$ und K besteht aus allen Permutationen von {1,...,m}
Für jeden Schlüssel π definiere

$$e_\pi(x_1,x_2,...,x_m) = (x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(m)})$$

und

$$e_\pi(y_1,y_2,...,y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, ..., y_{\pi^{-1}(m)})$$

wobei π^{-1} die inverse Permutation von π sei.

Strom-Chiffrierung

Definition: Die sogenannte Stromchiffre (synchronous stream cipher) besteht aus einem Sechs-Tupel (P,C,K,L,E,D) und einer Funktion g mit folgenden Eigenschaften:

1. P ist eine endliche Menge von möglichen Klartexten
2. C ist eine endliche Menge von möglichen Chiffretexten
3. K ist eine endliche Menge von möglichen Schlüsseln
4. L ist eine endliche Menge, die "keystream"-Alphabet genannt wird
5. g ist der "keystream"-Generator. Die Funktion erhält als Eingabe einen Schlüssel k und erzeugt eine unendliche Zeichenkette $z_1z_2...$, die "keystream" genannt wird, wobei $z_i \in L$ für alle $i \geq 1$.
6. Für jedes $z \in L$ gibt es eine Chiffrierungsregel $e_z \in E$ und eine zugehörige Dechiffrierungsregel $d_z \in D$. Die Funktionen $e_z : P \rightarrow C$ und $d_z : C \rightarrow P$ müssen durch effiziente Algorithmen berechenbar sein und für jedes $x \in P$ gilt $d_z(e_z(x)) = x$

Kryptosystem 1.7: Autokey-Chiffre (Autokey Cipher)

Sei $P = C = K = L = \mathbb{Z}_{26}$. Außerdem sei $z_1 = K$ und $z_i = x_{i-1}$ für alle $i \geq 2$.
Für $0 \leq z \leq 25$ definiere

$$e_z(x) = (x + z) \bmod 26$$

und

$$d_z(y) = (y - z) \bmod 26$$

$(x,y \in \mathbb{Z}_{26})$.