4 SP-Netze

Shannons Konstruktionsprinzipien

Nach Shannon sollen Blockchiffren folgendes leisten:

Diffusion (Durchmischung): Die Bits des Klartextblocks werden über den gesamten Block „verschmiert“. Quantitativ ausdrücken kann man das durch den „Lawinen-Effekt“ (englisch: avalanche effect):

- Jedes Bit des Geheimtextblocks hängt von jedem Bit des Klartextblocks ab.
- Bei Änderung eines Klartextbits ändern sich ca. 50% der Geheimtextbits.

Grundbausteine zur Erreichung von Diffusion sind Transpositionen.

Konfusion (Komplexität des Zusammenhangs): Die Beziehung zwischen Klartextblock und Geheimtextblock soll möglichst kompliziert sein (insbesondere hochgradig nichtlinear).

Grundbausteine hierfür sind vor allem Substitutionen.

Ähnlich komplex soll auch die Abhängigkeit des Geheimtextblocks vom Schlüssel sein.

Produktchiffren nach Shannon

Shannon schlug als Konstruktionsprinzip für starke Blockchiffren vor, Produktchiffren aus einer wechselnden Folge von **S**ubstitutionen und Transpositionen (= **P**ermutationen) zu bilden – sogenannte **SP-Netze**. Im einfachsten Fall sieht das so aus:

$$\begin{aligned} \mathbb{F}_2^n \xrightarrow{S_1(\bullet,k)} \mathbb{F}_2^n \xrightarrow{P_1(\bullet,k)} \mathbb{F}_2^n \longrightarrow \ldots \\ \ldots \longrightarrow \mathbb{F}_2^n \xrightarrow{S_r(\bullet,k)} \mathbb{F}_2^n \xrightarrow{P_r(\bullet,k)} \mathbb{F}_2^n \end{aligned}$$

abhängig von einem Schlüssel $k \in \mathbb{F}_2^l$. Dabei ist

$$\begin{aligned} S_i &= i\text{-te Substitution}, \\ P_i &= i\text{-te Permutation}, \\ P_i \circ S_i &= i\text{-te } \textbf{Runde} – \end{aligned}$$

wobei insgesamt r Runden nacheinander ausgeführt werden.

Beispiel: Lucifer I (Feistel 1973).