Perfect Secrurity

Definition: The ciphers of $\mathcal{S}$ provide perfect secrurity with respect to $\mathcal{T}$ and $\mathcal{K}$, if

$$p_k(t) = p(t)$$

holds for every cipher text $k \in \mathcal{K}$ and every plain text $t \in \mathcal{T}$.

Theorem: Let $\mathcal{S}$ be a set of keys with $\#(\mathcal{T}) = \#(\mathcal{K}) = \#(\mathcal{S})$, where all keys have the same probability and which contains, for any plain text t and any cipher text k, exactly one transformation τ with $\tau(t) = k$. Then $\mathcal{S}$ provides perfect secrurity with respect to $\mathcal{T}$ und $\mathcal{K}$.

Shift Register

Definition:

i) A shift register of length m is a sequence of m flip-flops k_1, k_2, . . . k_m; each contains in any moment t of time an element $k_i(t) \in \{0,1\}$; with each flip-flop k_i, a constant $c_i \in \{0,1\}$ and an initial value $x_i \in \{0,1\}$ is associated $(k_i(0) = x_i)$.

ii) The configuration of a shift register changes in every step according to the conditions:

– $k_1(t+1) = c_1k_1(t) \oplus c_2k_2(t) \oplus \ldots \oplus c_mk_m(t)$,
– $k_i(t+1) = k_{i-1}(t)$ für $2 \leq i \leq m,\ t \geq 0$.

iii) The output of the shift register is the sequence $k_m(0)k_m(1)k_m(2)\ldots$