

Kryptographie

Blatt 11, 24.06.05, Abgabe 01.07.05

Sei $N \in \mathbb{N}$ beliebig und $g \in \mathbb{Z}_{N^2}^*$ habe Ordnung $\alpha N \neq 0$ mit $\text{ggT}(\alpha, N) = 1$ (α teilt $\lambda(N)$). Definiere $\text{Pail}_{N,g} : \mathbb{Z}_N \times \mathbb{Z}_N^* \rightarrow \mathbb{Z}_{N^2}^*$ durch $(m, r) \mapsto g^m r^N$.

Aufgabe 1. Zeige: $\text{Pail}_{N,g} : (\mathbb{Z}_N, +) \times (\mathbb{Z}_N^*, \cdot) \rightarrow (\mathbb{Z}_{N^2}^*, \cdot)$

ist ein Isomorphismus.

Aufgabe 2. Für $u \in \mathbb{Z}_{N^2}^* \cong [0, N^2[$ mit $u = 1 \pmod N$ sei $L(u) =_{\text{def}} \frac{u-1}{N} \pmod N \in \mathbb{Z}_N \cong [0, N[$.

Zeige für $c := \text{Pail}_{N,g}(m, r)g^m r^N$ gilt $m = \frac{L(c^\alpha \pmod{N^2})}{L(g^\alpha \pmod{N^2})} \pmod N$.

Hinweis: $c^\alpha = g^\alpha = 1 \pmod N$, o.B.d.A. sei $g = 1 + N^2$.

Aufgabe 3. Sei X Zufallsvariable auf $\{0, 1\}^n$ mit Entropie $H(X)$. Zeige

1. $0 \leq H(X) \leq n$
2. $H(X) = 0 \Leftrightarrow X = x_0$ ist konstant
3. $H(X) = n \Leftrightarrow X$ ist gleichverteilt.