

Kryptographie

Blatt 2, 22.04.2005, Abgabe 29.04.2005

Aufgabe 1. Die Gruppe \mathbb{Z}_{71}^* ist zyklisch von der Ordnung 70. Bestimme zu \mathbb{Z}_{71}^* den Logarithmus $\log_2(3) \in [0, 69]$ mittels CRT durch zusammensetzen von $\log_2(3)$ modulo 2, 5, 7.

Aufgabe 2. Sei $E_{h,k} = \sum_{i=0}^{h-1} \{0, 1\}2^{ik} = \{\sum_{i=0}^{h-1} c_i 2^{ik} \mid c_i \in \{0, 1\}\}$, $hk \geq 1$. Zeige: Zu jeder Zahl $a = \sum_{i=0}^{hk-1} a_i 2^i$ mit $a_i \in \{0, 1\}$ gibt es eindeutig bestimmte $s_0, \dots, s_{k-1} \in E_{h,k}$ so dass $a = \sum_{j=0}^{k-1} s_j 2^j$.

Entwickle eine Formel für s_j in den a_i .

Hinweis: $s_j 2^j$ ist Teilsumme von $\sum_{i=0}^{hk-1} a_i 2^i$.

Aufgabe 3. (Lim-Lee, LNCS 839, p. 95–105)

Zur Gruppe $G = \langle g \rangle$, $|G| \leq 2^{hk}$, $h, k \geq 1$, sei $g^{E_{h,k}} = \{g^s \mid s \in E_{h,k}\}$ durch Vorberechnung gegeben.

Gib ein Verfahren an, das zu $a_0, \dots, a_{hk-1} \in \{0, 1\}$ $s_0, \dots, s_{k-1} \in E_{h,k}$ nach Aufg. 1 bestimmt (so dass $a = \sum_{i=0}^{hk-1} a_i 2^i = \sum_{j=0}^{k-1} s_j 2^j$) und $(g, a) \mapsto g^a = \prod_{j=0}^{k-1} (g^{s_j})^{2^j}$ in $2k - 2$ Mult. in G berechnet.

Aufgabe 4. Sei $G = \langle g \rangle$, $q = p_1 \cdots p_t$. Es bezeichne $M(p_1, \dots, p_t)$ die Anzahl der Multiplikationen in G zur Berechnung $g \mapsto g^{q/p_1}, \dots, g^{q/p_t}$.

Zeige: $M(p_1, \dots, p_t) = O(\lg q \lg t)$.

Hinweis: $M(p_1, \dots, p_t) \leq 2 \lg q + M(p_1, \dots, p_{t/2}) + M(p_{t/2+1}, \dots, p_t)$.