Prof. C. P. Schnorr Sommersemester 2007

Kryptographie

Blatt 1, 20.04.2007, Abgabe 27.04.2007

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 $G = \langle g \rangle$ Gruppe der Ordnung p^2, p prim. Zeige, dass die Berechnung von $h \mapsto \log_g(h)$ in $O(\sqrt{p})$ Multiplikationen in G geht.

Hinweis: für $\log_g(h) = a_1 + a_2 p$, $0 \le a_1, a_2 < p$ gilt

$$a_1 = \log_{g^p}(h^p), \quad a_2 = \log_{g^p}(h g^{p^2 - a_1}).$$

Aufgabe 3. $\mathbb{Z}_{101}^*$ ist zyklisch von der Ordnung $100 = 4 \cdot 5^2$. Berechne in Anlehnung an Aufgabe 2 zu $\mathbb{Z}_{101}^*$ den Logarithmus $\log_2(3)$, zunächst modulo $4, 5, 25$ und schliesslich modulo 100.

Aufgabe 4. Sei $G = \langle g \rangle$ zyklische Gruppe der Ordnung 2^e. Zeige, dass man $h \mapsto \log_g(h)$ mit $\binom{e+2}{2}$ Multiplikationen in G berechnen kann.

Hinweis: Für $a := \log_g h (\mathrm{mod} 2)$ gilt

$$\log_g(h g^a) = 2 \log_{g^2}(h g^a) = a + \log_g h.$$

$$\log_g h (\mathrm{mod} 2) \;=\; \begin{cases} 0 & \text{falls} \quad h^{2^{e-1}} = 1_G \\ 1 & \text{falls} \quad h^{2^{e-1}} \neq 1_G \end{cases}.$$

Punktzahl pro Aufgabe 5