Prof. C. P. Schnorr Sommersemester 2011

Kryptographie

Blatt 1, 15.04.2011, Abgabe 29.04.2011

Aufgabe 1. Die Gruppe $\mathbb{Z}_{71}^*$ ist zyklisch von der Ordnung 70. Bestimme zu $\mathbb{Z}_{71}^* = \langle 7 \rangle$ den Logarithmus $\log_7(3) \in [0, 69]$ mittels CRT durch zusammensetzen von $\log_7(3)$ 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 $G = \langle g \rangle$, $|G| = q$. Zeige $G \ni h \mapsto \log_g h$ geht für $h \in_R G$ mit Ws $\frac{1}{2}$ in $\sqrt{2q} + 2$ Multiplikationen in G.

Hinweis: Verkürze die Listen L_1, L_2 auf $\lceil \sqrt{q/2} \rceil$ viele Elemente.

Punktzahl pro Aufgabe 5