

Kryptographie

Blatt 1, 26.04.2017, Abgabe 03.05.2017

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.

Hinweis: $\mathbb{Z}_{71}^* \cong (\mathbb{Z}_{71}^*)^{\frac{70}{2}} \times (\mathbb{Z}_{71}^*)^{\frac{70}{5}} \times (\mathbb{Z}_{71}^*)^{\frac{70}{7}}$, $\mathbb{Z}_{70} \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7$.

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 $\log_g(h) = a_1 + a_2p$, $0 \leq a_1, a_2 < p$ gilt

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

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 mittels CRT modulo 100.

Punktzahl pro Aufgabe 5