

## Kryptographie

Blatt 1, 15.04.2005, Abgabe 22.04.2005

**Aufgabe 1.** Die Gruppe  $\mathbb{Z}_{77}^*$  ist zyklisch von der Ordnung 60. Bestimme zu  $\mathbb{Z}_{77}^*$  den Logarithmus  $\log_2(3) \in [0, 59]$  mittels CRT durch zusammensetzen von  $\log_2(3)$  modulo 3, 4, 5.

**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

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

**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, 20 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  $a := \log_g h(\text{mod } 2)$  gilt

$$\begin{aligned} \log_g(hg^a) &= 2 \log_{g^2}(hg^a) = a + \log_g h. \\ \log_g h(\text{mod } 2) &= \begin{cases} 0 & \text{falls } h^{2^{e-1}} = 1_G \\ 1 & \text{falls } h^{2^{e-1}} \neq 1_G \end{cases}. \end{aligned}$$

**Punktzahl** pro Aufgabe 5