Prof. C. P. Schnorr Wintersemester 2008/09

Kryptographie

Blatt 10, 19.12.2008, Abgabe 09.01.2009

Aufgabe 1 Zeige: Alg. 3.39 , Handbook of Applied Cryptography, berechnet $\mathrm{sqrt}(a) \in \mathbf{Z}_p$ zur Eingabe $a \in \mathrm{QR}_p$ im Mittel in $O(\lg p)^3)$ Bitoperationen.

Aufgabe 2 Für die primen p, q gelte $p-1 = 2^{m_p}p'$, $q-1 = 2^{m_q}q'$ mit p', q' ungerade und $m_p \geq m_q$. Zeige für $N = p \cdot q$:

$$S : x \mapsto x^{2^{m_p}}, \quad \mathbb{Z}_N^* \to \mathbb{Z}_N^{*2^{m_p}}$$

ist eine $2^{m_p+m_q} : 1$ Abb.

Aufgabe 3 Sei p prim, $p = 5 \bmod 8$, $a \in \mathrm{QR}_p$. Zeige $\mathrm{sqrt}(a) \in \{\pm a^{\frac{p+3}{8}}, \pm 2a(4a)^{\frac{p-5}{8}}\}$.

Hinweis: $2 \notin \mathrm{QR}_p$, Kap. 3.5, Handbook of Applied Cryptography.