Prof. C. P. Schnorr Sommersemester 2007

Kryptographie

Blatt 9, 15.06.07 Abgabe 22.06.07

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 Berechne mit Alg. 3.39 ein $b \in \mathbf{Z}_{101}$ so dass $\left(\frac{b}{101}\right) = -1$, $\mathrm{sqrt}(-1) \bmod 101$.

Aufgabe 3 Zeige: der Algorithmus FA im Satz 3.16 führt im Fall $p - 1 \neq 0 \bmod 2^k$ nicht zum Ziel.

Es bezeichne RSA_m die Menge der RSA–Moduln $N = pq$ mit $p - 1 = 2^m \bmod 2^{m+1},\ q - 1 \neq 0 \mod 2^{m+1}$.

Aufgabe 4 Zeige für $N \in \mathrm{RSA}_m$:

a) $\mathbb{Z}_N^{*2^m} = \mathbb{Z}_N^{*2^{m+1}}$,

b) $-1 \notin \mathbb{Z}_N^{*2^m}$,

c) $x \mapsto x^2$ permutiert $\mathbb{Z}_N^{*2^m}$.