Prof. C. P. Schnorr Sommersemester 2006

Diskrete Mathematik

Blatt 6, 26.05.2006, Abgabe 02.06.2006

Aufgabe 1. **1.** Ordne den Buchstaben $A, \ldots, Z$ die ersten 26 zu $7 \cdot 19 = 133$ teilerfremden Zahlen > 1 zu.

2. Verschlüssele die Nachricht `GEHEIM` im RSA–Schema mit $N = 133$ und $e = 5$. Bestimme $\varphi(N)$, $\lambda(N)$, $e^{-1} \bmod \varphi(N)$, $e^{-1} \bmod \lambda(N)$.

Eine Blum–Zahl ist ein RSA–Modul $N = P \cdot Q$ mit P, Q prim und $P, Q = 3 \bmod 4$.

Aufgabe 2. Zeige, dass für Blum–Zahlen N gilt

1. $-1 \notin \mathrm{QR}_N = (\mathbf{Z}_N^*)^2$,
2. Jedes $x \in \mathrm{QR}_N$ hat genau eine Quadratwurzel in QR_N
3. $|\mathrm{QR}_N| = \varphi(N)/4 = 1 \bmod 2$.

Hinweis: $-1 \in \mathrm{QR}_N$ impliziert $-1 \in \mathrm{QR}_P$ und $-1^{(P-1)/2} = 1 \mod P$.

Rabin–Schema öffentl. Blum–Zahl N, geheim $\varphi(N)$

$$E : \mathrm{QR}_N \to \mathrm{QR}_N, \quad E(x) = x^2 \bmod N$$
$$D : \mathrm{QR}_N \to \mathrm{QR}_N, \quad D(x) = x^{2^{-1} \bmod (\varphi(N)/4)} \bmod N.$$

Aufgabe 3. Zeige

1. $E \circ D = D \circ E = \mathrm{id}_{\mathrm{QR_N}}$
2. Jeder Algorithmus zu D liefert die Zerlegung von N
3. Für $x \in_R \mathbf{Z}_N^*$ liefert $D(x^2)$ mit $\mathrm{Ws}_x = \frac{1}{2}$ die Zerlegung von N.

(6 Punkte pro Aufgabe)