Diskrete Mathematik

Blatt 4, 06.05.2010, Abgabe 17.05.2010, 12.10 Uhr

Aufgabe 1. Gegeben seien drei RSA–Moduln $N_1 < N_2 < N_3$ und $x^3 \bmod N_i$ für $i = 1, 2, 3$ für ein $x \in [0, N_1[$.
Zeige, dass $x \in [0, N_1[$ in pol. Zeit berechenbar ist.
(Somit darf beim RSA–Schema mit Kodierexponent e dieselbe Nachricht x nicht mit e verschiedenen Moduln N_i kodiert werden.) **6 Punkte**

Aufgabe 2.
Ordne den Buchstaben $A, \ldots, Z$ die ersten 26 zu $7 \cdot 19 = 133$ teilerfremden Zahlen > 1 zu. Verschlüssele die Nachricht `GEHEIM` im RSA–Schema mit $N = 133$ und $e = 5$.
Bestimme $\varphi(N),\ \lambda(N),\ e^{-1} \bmod \varphi(N),\ e^{-1} \bmod \lambda(N)$. **6 Punkte**

Aufgabe 3. Sei $N \in \mathbb{N}$ ungerade mit Primfakt.zerl. $N = \prod_{i=1}^{r} p_i^{e_i}$. Zeige

1. Jedes $a \in \mathrm{Q}R_N = \{b^2 \mid b \in \mathbb{Z}_N^*\}$ hat genau 2^r Quadratwurzeln in $\mathbb{Z}_N^*$.
2. Für zufällige $x, y \in \mathbb{Z}_N^*$ mit $x^2 = y^2 \bmod N$ gilt

$$\mathrm{Ws}[\mathrm{ggT}(x \pm y, N) \neq 1] = 1 - 2^{-r+1}\ .$$

Hinweis: $\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^*$
Für alle $z \in QR_N$ gilt: $\#\{x \in \mathbb{Z}_N^* \mid x^2 = z \mod N\} = 2^r$. **6 Punkte**

Aufgabe 4. Zeige, dass im Miller-Rabin Test mindestens die Hälfte der $a \in \mathbb{Z}_N^*$ Zeugen für die Nicht-Primheit eines nicht primen N sind.
Hinweis: Knuth, Vol. 2 Aufgabe 4.5.4 (22), Crandall, Pomerance (2001), Thm. 3.4.4. **6 Punkte**