Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Dr. Christopher Wolf
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2010

Blatt 7 / 13. und 14. Juli 2010

AUFGABE 1. Quadratische Reste I.
Sei $N = pq$ für $p \neq q$ prim und sei $y \in \mathbb{Z}_N^*$ mit $y \leftrightarrow (y_p, y_q) = (y \bmod p, y \bmod q)$. Zeigen Sie, dass

$$y \in \mathcal{QR}_N \Leftrightarrow y_p \in \mathcal{QR}_p \text{ und } y_q \in \mathcal{QR}_q \ .$$

Folgern Sie daraus, dass die Abbildung $f : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ mit $x \mapsto x^2 \bmod N$ eine k-zu-1 Abbildung ist und geben Sie k an. Wie groß ist der Anteil von quadratischen Resten in $\mathbb{Z}_N^*$?

Wir erinnern kurz an die Definition folgender Mengen: Sei

$$\mathcal{J}_N^{+1} := \left\{ x \in \mathbb{Z}_N^* : \left(\frac{x}{N}\right) = +1 \right\}$$

die Menge aller x mit Jacobi-Symbol $+1$ und

$$\mathcal{QR}_N := \left\{ y \in \mathbb{Z}_N^* : \exists x \in \mathbb{Z}_N^* \text{ mit } y = x^2 \bmod N \right\}$$

die Menge aller quadratischen Reste. Sei außerdem

$$\mathcal{QNR}_N := \mathbb{Z}_N^* \setminus \mathcal{QR}_N$$

die Menge der quadratischen Nichtreste und

$$\mathcal{QNR}_N^{+1} := \mathcal{J}_N^{+1} \setminus \mathcal{QR}_N$$

die Menge der quadratischen Nichtreste mit Jacobi-Symbol $+1$.

AUFGABE 2. Quadratische Reste II.
Sei $N = pq$ für prime, ungerade $p \neq q$. Zeigen Sie:

a) $\frac{|\mathcal{J}_N^{+1}|}{|\mathbb{Z}_N^*|} = \frac{1}{2}$

b) $\mathcal{QR}_N \subset \mathcal{J}_N^{+1}$

c) $\frac{|\mathcal{QR}_N|}{|\mathcal{J}_N^{+1}|} = \frac{1}{2}$.

AUFGABE 3. Quadratische Reste III.
Sei $N = pq$ für prime, ungerade $p \neq q$. Beweisen Sie

a) $x \in \mathcal{QR}_N \Rightarrow [x^{-1} \bmod N] \in \mathcal{QR}_N$

b) $x \in \mathcal{QNR}_N^{+1} \Rightarrow [x^{-1} \bmod N] \in \mathcal{QNR}_N^{+1}$