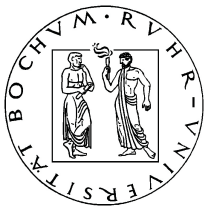
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann



Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 4 / 10. Juni 2009

AUFGABE 1:
Sei $N = pq$, wobei p und q verschiedene ungerade Primzahlen sind. Geben Sie einen ppt. Algorithmus an, der eine zufälliges Element aus $\mathcal{QNR}_N^{+1}$ ausgibt, falls die Faktorisierung von N bekannt ist. Der Algorithmus darf eine vernachlässigbare Fehlerwahrscheinlichkeit haben.

AUFGABE 2:
Sei $N = pq$, wobei p und q verschiedene ungerade Primzahlen sind. Zeigen Sie,

- falls $x \in \mathcal{QR}_N$, dann $[x^{-1} \bmod N] \in \mathcal{QR}_N$
- falls $x \in \mathcal{QNR}_N^{+1}$, dann $[x^{-1} \bmod N] \in \mathcal{QNR}_N^{+1}$.

AUFGABE 3:
Sei GenModulus ein ppt. Algorithmus, der bei Eingabe 1^n ein Tupel (N, p, q) ausgibt mit $N = pq$ und p, q n-bit Primzahlen. Angenommen das Unterscheiden von Quadratischen Resten ist hart bzgl. GenModulus. Zeigen Sie, dass dann auch das Unterscheiden eines zufälligen Elements aus $\mathcal{QR}_N$ von einem zufälligen Element aus $\mathcal{J}_N^{+1}$ hart ist.
Hinweis:

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