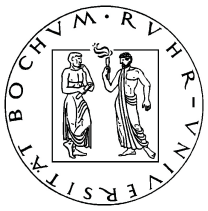
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann



Hausübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 5 / 17. Juni 2009 / Abgabe spätestens 01. Juli, 8:30 Uhr

AUFGABE 1 (5 Punkte)**:**
Sei $\mathcal{G}$ ein Polynomialzeit Algorithmus, der bei Eingabe 1^n eine Primzahl p mit $||p|| = n$ und einen Generator g von $\mathbb{Z}_p^*$ ausgibt. Man vermutet, dass das diskrete Logarithmus Problem bzgl. $\mathcal{G}$ hart ist, d.h. dass die Funktion $f_{p,g}(x) := [g^x \bmod p]$ eine Einwegfunktion ist.
Bezeichne $\mathsf{lsb}(x)$ das niederwertigste Bit von x. Zeigen Sie, dass lsb **kein** Hardcore-Prädikat für die Funktion $f_{p,g}$ ist.

AUFGABE 2 (5 Punkte)**:**
Wir betrachten *Textbook-Rabin-Verschlüsselung*, d.h. eine Nachricht $m \in \mathcal{QR}_N$ wird mit dem öffentlichen Schlüssel N durch den Chiffretext $c := [m^2 \bmod N]$ verschlüsselt (N ist dabei eine Blum-Zahl).
Geben Sie einen Chosen-Ciphertext-Angriff an, der nicht nur die Nachricht liefert, sondern sogar den privaten Schlüssel rekonstruiert.

AUFGABE 3 (5 Punkte)**:**
Sei $\Psi(N^2)$ die Menge $\{(a, 1) \mid a \in \mathbb{Z}_N\} \subset \mathbb{Z}_{N^2}^*$. Ist es schwer zu entscheiden, ob ein gegebenes Element $y \in \mathbb{Z}_{N^2}^*$ in $\Psi(N^2)$ ist ? Beweisen Sie Ihre Aussage.

AUFGABE 4 (5 Punkte)**:**
Wir wissen, dass $\mathbb{Z}_N \times \mathbb{Z}_N^* \cong \mathbb{Z}_{N^2}^*$, wobei der Isomorphismus durch $f : \mathbb{Z}_N \times \mathbb{Z}_N^* \to \mathbb{Z}_{N^2}^*$ mit

$$f(a, b) := [(1 + N)^a \cdot b^N \bmod N^2]$$

gegeben ist.
Zeigen Sie, dass f effizient umkehrbar ist, falls die Faktorisierung von N bekannt ist.