Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 11 / 13./14. Januar 2014

AUFGABE 1:

Sei $\mathcal{G}$ ein Algorithmus, der eine zyklische Gruppe G der bekannten Ordnung q und einen Generator g für G erzeugt. In der Vorlesung wurde gezeigt, dass ElGamal bzgl. $\mathcal{G}$ CPA-sicher unter der DDH-Annahme ist. Zeigen Sie, dass diese Annahme auch notwendig ist, indem Sie zeigen:

$$\mathsf{ElGamal} \text{ ist CPA-sicher bzgl. } \mathcal{G} \Longrightarrow \text{Das } \mathsf{DDH}\text{-Problem ist hart bzgl. } \mathcal{G}$$

AUFGABE 2:

Sei $N = pq$ ein RSA-Modul und sei $(N, e, d) \leftarrow \mathsf{GenRSA}(1^n)$. Wir wollen für den Spezialfall $e = 3$ zeigen, dass das Berechnen von d äquivalent zum Faktorisieren von N ist. Beweisen Sie hierzu folgene Aussagen:

(a) Wenn man N effizient faktorisieren kann, so kann man d effizient berechnen.

(b) Sind $\phi(N)$ und N bekannt, so kann man p und q berechnen.

(c) Seien $e = 3$ und $d \in \mathbb{N}$ mit $ed = 1 \bmod \phi(N)$ bekannt. Zeigen Sie, dass man dann effizient p und q berechnen kann.

Bitte wenden!

AUFGABE 3:

Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine *Einwegfunktion*. Zeigen Sie, dass dann auch $g : \{0,1\}^n \to \{0,1\}^{2n}$ mit

$$g(x) := (f(x), f(f(x)))$$

eine *Einwegfunktion* ist.

AUFGABE 4:

Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine Permutation. Beweisen Sie: Wenn es ein Hardcoreprädikat $\mathsf{hc} : \{0,1\}^n \to \{0,1\}$ für f gibt, dann ist f eine *Einwegpermutation*.