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

Präsenzübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 3 / 17. Mai 2013

AUFGABE 1:

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 2:

Sei $\mathcal{G}$ ein Algorithmus, der bei Eingabe 1^n eine zyklische Gruppe G der Ordnung q mit Generator g erzeugt. Zeigen Sie, dass die Härte des *Diskreten Logarithmus Problems* bzgl. $\mathcal{G}$ die Existenz einer Familie von *Einwegpermutationen* impliziert. Konstruieren Sie dazu ein Tupel $\Pi_f = (\mathsf{Gen}, \mathsf{Samp}, f)$ und zeigen Sie die Einwegeigenschaft.

AUFGABE 3:

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*.