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

Hausübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 3 /
Abgabe: 31. Mai 2013, 10 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

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

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

eine *Einwegpermutation* ist.

AUFGABE 2 (5 Punkte)**:**

Sei $\mathsf{hc} : \{0,1\}^n \to \{0,1\}$ ein *Hardcoreprädikat* für eine Permutation $f : \{0,1\}^n \to \{0,1\}^n$. Zeigen Sie, dass dann hc *erwartungstreu (auch unbiased)* ist, d.h.

$$\left|\mathsf{Ws}_{x\in_R\{0,1\}^n}[\mathsf{hc}(x)=0] - \mathsf{Ws}_{x\in_R\{0,1\}^n}[\mathsf{hc}(x)=1]\right| \leq \mathsf{negl}(n)$$

gilt.

Bitte wenden!

AUFGABE 3 (10 Punkte)**:**

Sei $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ eine *Einwegfunktion*. Zeigen Sie, dass dann im Allgemeinen die Funktion $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ definiert durch $f'(x) := f(x) \oplus x$ keine *Einwegfunktion* ist. Gehen Sie wie folgt vor:

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

$$f(x) = f(x_1, x_2) := (g(x_1) \oplus x_2, x_2)$$

eine *Einwegfunktion* ist. Hierbei teilen wir die Eingabe $x \in \{0,1\}^{2n}$ in zwei gleichgroße Hälften $x_1, x_2 \in \{0,1\}^n$ auf.

Hinweis: Beim Nachweis der Einwegeigenschaft kann es hilfreich sein, zunächst die Mengengleichheit $f^{-1}(a,b) = g^{-1}(a \oplus b) \times \{b\}$ zu zeigen. Hierbei bezeichnet $f^{-1}(a,b) := \{(x_1, x_2) \in \{0,1\}^{2n} \mid f(x_1, x_2) = (a,b)\}$ das *Urbild* von (a,b) unter f.

(b) Benutzen Sie das in (a) konstruierte f und betrachten Sie das entsprechende f'. Zeigen Sie, dass dieses f' keine *Einwegfunktion* sein kann.