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 6 / 18./19. November 2013

AUFGABE 1:

Zeigen Sie, dass der CBC-Modus nicht CCA-sicher ist.

AUFGABE 2:

Ist der Counter-Modus CPA-sicher, falls (statt einer Pseudozufallsfunktion) eine *schwache* Pseudozufallsfunktion verwendet wird? Der Counter-Modus ist für ein $\ell \in \mathbb{N}$ und Nachrichtenraum $\mathcal{M} = \{0,1\}^{n\ell}$ definiert als $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit:

$\mathsf{Gen}(1^n)$: Gibt $k \in_R \{0,1\}^n$ zurück.

$\mathsf{Enc}_k(m)$: $\mathsf{IV} \in_R \{0,1\}^n$, $c_i := m_i \oplus F_k(\mathsf{IV} + i - 1 \bmod 2^n)$ für $1 \leq i \leq \ell$, $c := (\mathsf{IV}, c_1, \ldots, c_\ell)$.

AUFGABE 3:

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine schlüsselabhängige Funktion. Betrachten Sie die Konstruktion $\Pi_B = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ aus der Vorlesung mit $\mathcal{M} = \{0,1\}^n$ und

$\mathsf{Gen}(1^n)$: Gib $k \in_R \{0,1\}^n$ zurück.

$\mathsf{Enc}_k(m)$: Wähle $r \in_R \{0,1\}^n$ und gib $c := (r, F_k(r) \oplus m)$ zurück.

$\mathsf{Dec}_k(c)$: Für $c = (c_1, c_2)$ gib $m := F_k(c_1) \oplus c_2$ zurück.

Zeigen Sie, dass Π_B CPA-sicher ist, falls F eine *schwache* Pseudozufallsfunktion ist.