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 3 / 28./29. Oktober 2013

AUFGABE 1:

Betrachten Sie folgende Modifikation des One-Time Pads, das „Double-One-Time Pad“ mit dem Nachrichtenraum $\mathcal{M} = \{0,1\}^n$, dem Chiffretextraum $\mathcal{C} = \{0,1\}^{2n}$ und dem Schlüsselraum $\mathcal{K} = \{0,1\}^{4n}$, sowie

- $\mathsf{Gen}(1^n)$: Wähle $k \in_R \{0,1\}^{4n}$.
- $\mathsf{Enc}_k(m)$: Für $k = (k_1, k_2, k_3, k_4) \in \{0,1\}^{4n}$ gib $c := (c_1, c_2) = (m \oplus k_1, m \oplus k_2)$ aus.

(a) Geben Sie eine korrekte Entschlüsselungsfunktion $\mathsf{Dec}_k(c)$ an.

(b) Zeigen Sie, dass das „Double-One-Time Pad” perfekt sicher ist.

AUFGABE 2:

Sei $a \in \mathbb{R}$ mit $a > 1$. Zeigen Sie, dass dann $\dfrac{1}{a^n}$ vernachlässigbar ist.

Hinweis: Verwenden Sie die Regel von L'Hôpital.

AUFGABE 3:

Entscheiden Sie, welche der folgenden Funktionen vernachlässigbar sind. Begründen Sie.

$$(a)\ 0.80^n, \quad (b)\ \frac{1}{2^{80}n}, \quad (c)\ \frac{1}{2^{80n}}, \quad (d)\ 2^{-\log_2(n^{80})}.$$

In der nächsten Aufgabe (und in der Hausaufgabe) wollen wir die Äquivalenz einiger Definitionen von KPA-Sicherheit zeigen. Die erste Definition ist bekannt aus der Vorlesung:

Definition 1. Ein Verschlüsselungsschema $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ besitzt *ununterscheidbare Chiffretexte gegenüber KPA*, falls für alle ppt Angreifer $\mathcal{A}$ gilt

$$\mathsf{Ws}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n)$$

Alternativ kann man definieren, dass der Betrag des *Vorteils* jedes Angreifers vernachlässigbar sein muss:

Definition 2. Ein Verschlüsselungsschema $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ besitzt *ununterscheidbare Chiffretexte gegenüber KPA*, falls für alle ppt Angreifer $\mathcal{A}$ gilt

$$\left|\mathsf{Ws}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] - \frac{1}{2}\right| \leq \mathsf{negl}(n)$$

AUFGABE 4:

Zeigen Sie, dass die erste Definition die zweite Definition impliziert.

Hinweis: Führen Sie eine Fallunterscheidung durch und betrachten Sie im zweiten Fall den Angreifer $\bar{\mathcal{A}}$, der das Gegenteil von $\mathcal{A}$ ausgibt.

AUFGABE 5:

Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit $\mathcal{M} = \mathbb{Z}_{2^n} = \{0, \ldots, 2^n - 1\}$ KPA-sicher. Sei für ein $m \in \mathcal{M}$

$$f(m) := \left\lfloor \frac{m}{2^{n-1}} \right\rfloor = \begin{cases} 0, & 0 \leq m \leq 2^{n-1} - 1 \\ 1, & 2^{n-1} \leq m \leq 2^n - 1 \end{cases}$$

Zeigen Sie, dass dann für alle ppt-Angreifer $\mathcal{A}$ gilt:

$$\mathsf{Ws}[\mathcal{A}(1^n, \mathsf{Enc}_k(m)) = f(m)] \leq \frac{1}{2} + \mathsf{negl}(n).$$

Wsraum: Wahl von $m \in_R \mathcal{M}$ und Münzwürfe von $\mathcal{A}, \mathsf{Gen}$ und Enc.