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

**Hausübungen zur Vorlesung**

# Kryptographie I

**WS 2012/13**

Blatt 2 / 25. Oktober 2012

Abgabe: Am 05. November 2012 entweder bis 12 Uhr in den Kasten NA/02 (Kasten wird um 12 Uhr geleert!) oder bis 16.15 Uhr in der Übung, NA 5/99

**AUFGABE 1** (5 Punkte)**:**

Beweisen Sie „Komposition vernachlässigbarer Funktionen" auf Folie 27 der Vorlesung:

Seien $f_1(n), f_2(n)$ zwei vernachlässigbare Funktionen. Zeigen Sie:

(a) $f_1(n) + f_2(n)$ ist vernachlässigbar,

(b) $q(n) \cdot f_1(n)$ ist für ein beliebiges Polynom $q(n) \geq 0$ vernachlässigbar.

**AUFGABE 2** (5 Punkte)**:**

Zeigen Sie in dieser Aufgabe die Äquivalenz der drei Definitionen aus der Präsenzübung. In Aufgabe 2 der Präsenzübung wurde bereits gezeigt, dass die erste Definition die zweite Definition impliziert. Zeigen Sie für einen Ringschluss:

(a) Definition 2 impliziert Definition 3,

(b) Definition 3 impliziert Definition 1.

*Hinweis:* Verwenden Sie die dritte Aufgabe der Präsenzübung.

Bitte wenden!

**AUFGABE 3** (5 Punkte)**:**

(a) Sei $G : \{0,1\}^{n/2} \to \{0,1\}^{n+1}$ ein Pseudozufallsgenerator. Sei $G' : \{0,1\}^n \to \{0,1\}^{n+1}$ definiert als $G'(s) := G(s_1, \ldots, s_{n/2})$ für einen Seed $s := (s_1, \ldots, s_n)$. Beweisen Sie, dass auch $G'$ ein Pseudozufallsgenerator ist, indem Sie aus einem Unterscheider für $G'$ einen Unterscheider für $G$ konstruieren.

(b) Sei $G : \{0,1\}^n \to \{0,1\}^{n+1}$ ein Pseudozufallsgenerator. Sei $G'' : \{0,1\}^{n/2} \to \{0,1\}^{n+1}$ definiert durch $G''(s) := G(0^{n/2}s)$ für einen Seed $s := (s_1, \ldots, s_{n/2})$. Zeigen Sie, dass $G''$ im Allgemeinen kein Pseudozufallsgenerator ist!

**AUFGABE 4** (5 Punkte)**:**

Betrachten Sie ein symmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Nachrichtenraum $\mathcal{M} \in \{0,1\}^n$. Die *Paritätsfunktion* $\mathsf{parity} : \{0,1\}^n \to \{0,1\}$ sei definiert als $\mathsf{parity}(x) = \sum_i x_i \bmod 2$. Sei $\mathcal{A}$ ein ppt Algorithmus mit

$$\mathsf{Ws}[\mathcal{A}(\mathsf{Enc}_k(m)) = \mathsf{parity}(m)] = \frac{1}{5},$$

wobei $k \leftarrow \mathsf{Gen}(1^n), m \in_R \mathcal{M}$ zufällig und die Wahrscheinlichkeit über die Wahl von $k, m$ und die interne Randomisierung von $\mathcal{A}$ gebildet wird. Zeigen Sie, dass $\Pi$ nicht KPA-sicher ist, indem Sie einen KPA-Angreifer $\mathcal{A}'$ konstruieren, der $\mathcal{A}$ benutzt.

*Anmerkungen:*

- Sie sollen diese Aufgabe mittels einer Reduktion lösen. Für diese Aufgabe dürfen Sie daher den Satz über die Nicht-Berechenbarkeit von Funktionen aus der Vorlesung nicht zitieren. Sich den Beweis dieses und des vorherigen Satzes genau anzusehen kann hilfreich sein.
- Beachten Sie, dass Sie $\mathcal{A}$ als Unterroutine mit der richtigen Eingabeverteilung aufrufen, d.h. $\mathcal{A}$ sollte $\mathsf{Enc}_k(m)$ für zufällig, gleichverteiltes $m$ erhalten, da die Annahme an die Erfolgswahrscheinlichkeit von $\mathcal{A}$ nur für diesen Fall sicher gewährleistet ist.