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

Hausübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 4 / 19. November 2012

Abgabe: Am 03. Dezember 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)**:**

Betrachten Sie die folgende längenerhaltende, schlüsselabhängige Funktion F mit $F_{a,b} : \{0,1\}^n \to \{0,1\}^n$ wobei $a, b \in_R \mathbb{Z}_{2^n} := \{0, 1, \ldots, 2^n - 1\}$:

$$F_{a,b}(x) := a \cdot x + b \mod 2^n$$

Hierbei werden Elemente $x \in \{0,1\}^n$ als Zahlen von 0 bis $2^n - 1$ aufgefasst.

Zeigen Sie, dass F keine Pseudozufallsfunktion ist.

AUFGABE 2 (5 Punkte)**:**

In dieser Aufgabe wollen wir die *Hinrichtung* aus dem Fakt „Existenz von Pseudozufallsfunktionen" (Folie 73) aus der Vorlesung beweisen.

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion mit $F_k : \{0,1\}^n \to \{0,1\}^n$ für $k \in \{0,1\}^n$. Konstruieren Sie daraus einen Pseudozufallsgenerator $G : \{0,1\}^n \to \{0,1\}^{2n}$. Zeigen Sie, dass die von Ihnen vorgeschlagene Konstruktion ein Pseudozufallsgenerator ist, indem Sie aus einem Unterscheider $\mathcal{D}'$ für G einen Unterscheider $\mathcal{D}$ für F konstruieren.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

In dieser Aufgabe wollen wir zeigen, dass die Definitionen *Pseudozufallsfunktion* und *schwache Pseudozufallsfunktion* nicht äquivalent sind. Zwar ist eine *Pseudozufallsfunktion* stets auch eine *schwache Pseudozufallsfunktion* (siehe Präsenzübung, Aufgabe 3), die Rückrichtung gilt allerdings nicht. Um dies zu zeigen, geben wir eine Funktion F' an, die zwar eine *schwache Pseudozufallsfunktion* ist, aber keine *Pseudozufallsfunktion*.

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion mit $F_k : \{0,1\}^n \to \{0,1\}^n$ für $k \in \{0,1\}^n$. Sei $x = (x_1, \ldots, x_n) \in \{0,1\}^n$. Dann definieren wir eine neue Funktion $F' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ als $F'_k(x) := F_k(x_1 \ldots x_{n-1}0)$, d.h. das letzte Bit der Eingabe wird stets auf 0 gesetzt und dann F_k aufgerufen.

(a) Zeigen Sie, dass F' eine *schwache Pseudozufallsfunktion* ist.

(b) Zeigen Sie, dass F' keine *Pseudozufallsfunktion* ist.

AUFGABE 4 (5 Punkte)**:**

Seien $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ und $\Pi'' = (\mathsf{Gen}'', \mathsf{Enc}'', \mathsf{Dec}'')$ zwei Verschlüsselungssysteme mit jeweils $\mathcal{M} = \{0,1\}^n$, von denen man weiß, dass mindestens eines CPA-sicher ist. Das Problem ist, dass man nicht weiß, welches CPA-sicher ist und welches es vielleicht nicht ist. Konstruieren Sie aus Π' und Π'' ein CPA-sicheres Kryptosystem $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. Zeigen Sie die CPA-Sicherheit von Π, indem Sie aus einem Angreifer $\mathcal{A}$ auf Π einen Angreifer $\mathcal{A}'$ auf Π' bzw. $\mathcal{A}''$ auf Π'' konstruieren.

Hinweis: Konstruieren Sie aus der eingegebenen Nachricht m in Enc zwei Nachrichten m', m'' als Eingabe für Enc' bzw. Enc'', so dass jede Nachricht für sich keine Information über m enthält, man aus beiden Nachrichten zusammen aber m rekonstruieren kann.