Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 2 / 25. Oktober 2010 / Abgabe 15. November, 16 Uhr, Kasten NA 02

AUFGABE 1. Vernachlässigbares I. (5 Punkte)
Es seien $f_1(n), f_2(n) = \mathsf{negl}(n)$ vernachlässigbar. Beweisen oder widerlegen Sie folgende Aussagen:

a) $f_1(n) + f_2(n) = \mathsf{negl}(n)$

b) $p(n) \cdot f_1(n) = \mathsf{negl}(n)$ für ein beliebiges Polynom $p(n) \geq 0$

c) $\frac{1}{\log\left(\frac{1}{f_1(n)}\right)} = \mathsf{negl}(n)$

AUFGABE 2. Vernachlässigbares II. (5 Punkte)
Beweisen Sie die Äquivalenz der folgenden Definitionen für *vernachlässigbar*!

Definition 1. Eine Funktion $f : \mathbb{N} \to \mathbb{N}$ heißt *vernachlässigbar*, wenn für jedes Polynom $p \neq 0$ ein $N = N(p) \in \mathbb{N}$ existiert, so dass $f(n) < \frac{1}{p(n)}$ für alle $n > N$ gilt.

Definition 2. Eine Funktion $f : \mathbb{N} \to \mathbb{N}$ heißt *vernachlässigbar*, wenn für jede Konstante $c \in \mathbb{R}, c > 0$ ein $N = N(c) \in \mathbb{N}$ existiert, so dass $f(n) < n^{-c}$ für alle $n > N$ gilt.

AUFGABE 3. Definitionssache. (5 Punkte)
Zeigen Sie die fehlende Richtung aus Aufgabe 2 aus der Präsenzübung, d.h. beweisen Sie, dass die Definition *ununterscheidbarer Chiffretexte unter KPA* aus der Vorlesung (siehe Folie 31) die Definition 2 vom Präsenzübungsblatt impliziert. Hierbei dürfen Sie die Zwischenergebnisse aus der Präsenzübung benutzen.

Hinweis: Um die Betragsstriche formal in den Griff zu bekommen, kann es hilfreich sein, einen Angreifer $\tilde{\mathcal{A}}$ zu betrachten, der stets das Gegenteil von $\mathcal{A}$ ausgibt.

AUFGABE 4. Paripari. (5 Punkte)
Betrachten sie ein symmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit $\mathcal{K} = \{0,1\}^n$. Die *Paritätsfunktion* $\mathsf{parity} : \{0,1\}^n \to \{0,1\}$ ist definiert als

$$\mathsf{parity}(x) := \sum_{i=1}^{n} x_i \bmod 2 \ ,$$

d.h. $\mathsf{parity}(n) = 1$ genau dann wenn x eine ungerade Anzahl von 1en enthält.
Nehmen Sie nun an, dass es einen Algorithmus $\mathcal{A}'$ gibt mit

$$\mathbf{Pr}\left[\mathcal{A}'(\mathsf{Enc}_k(m)) = \mathsf{parity}(m)\right] = \frac{3}{4}$$

wobei die Wahrscheinlichkeit über die zufällige Wahl von m, k (und die Randomisierung von $\mathcal{A}'$) gebildet wird. Zeigen Sie, dass Π nicht KPA-sicher ist, indem Sie einen KPA-Angreifer $\mathcal{A}$ konstruieren, welcher $\mathcal{A}'$ benutzt.

Hinweis: Achten Sie darauf, dass $\mathcal{A}$ bei Aufruf von $\mathcal{A}'$ die richtige Eingabeverteilung für $\mathcal{A}'$ gewährleistet, d.h. $\mathcal{A}'$ sollte $\mathsf{Enc}_k(m)$ für zufälliges $m \in_R \mathcal{M}$ als Eingabe erhalten.

AUFGABE 5. Pseudozufall. (5 Punkte)

a) Sei G ein Pseudozufallsgenerator. Wir definieren $\overline{G}$ wie folgt: Zum Seed s berechne $w = G(s)$ und bilde das bitweise Komplement $\overline{w}$, d.h. $\overline{w}_i := w_i \oplus 1$ für alle i. Beweisen Sie, dass $\overline{G}$ auch ein Pseudozufallsgenerator ist, indem Sie aus einem Unterscheider $\overline{D}$ für $\overline{G}$ einen Unterscheider D für G konstruieren.

b) Seien G_1 und G_2 zwei unterschiedliche Pseudozufallsgeneratoren. Betrachten Sie den Pseudozufallsgenerator $G(s) := G_1(s)||G_2(s)$ wobei $x||y$ die Konkatenation von zwei Bitstrings bezeichnet. Zeigen Sie, dass G im Allgemeinen *kein* Pseudozufallsgenerator ist.

Hinweis: Zur Lösung von Teil b) ist es hilfreich, Teil a) zu verwenden.