Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Eike Kiltz
Gottfried Herold

Hausübungen zur Vorlesung

Kryptographie I

WS 2011/2012

Blatt 1 / 24. Oktober 2011 / Abgabe **bis spätestens Montag, 7.11.2011 16:00 Uhr**

AUFGABE 1:

Seien $f_1(n), f_2(n) = \text{negl}(n)$ vernachlässigbare Funktionen. Beweisen oder widerlegen Sie, dass dann auch die folgenden Funktionen vernachlässigbar sind: [Je 1 Punkt]

(a) $f_1(n) + f_2(n)$

(b) $f_1(n) \cdot f_2(n)$

(c) $p(n) \cdot f_1(n)$ für ein beliebiges Polynom $p(n)$

(d) $\frac{1}{\log\left(\frac{1}{f_1(n)}\right)}$

AUFGABE 2:

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

Sei A ein ppt. Algorithmus mit

$$\mathbf{Ws}[A(\mathbf{Enc}_k(m)) = \mathbf{parity}(m)] = \frac{3}{5},$$

wobei $k \leftarrow \mathbf{Gen}(1^n), m \in_R \mathcal{M}$ zufällig und die Wahrscheinlichkeit über die Wahl von k, m und die interne Randomisierung von A gebildet wird. Zeigen Sie, dass Π nicht KPA-sicher ist, indem Sie einen KPA-Angreifer A' konstruieren, der A benutzt.[5 Punkte]

- bitte wenden (Aufgabe geht auf nächster Seite weiter)-

Bemerkung und Hinweise zu Aufgabe 2:
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 A als Unterroutine mit der richtigen Eingabeverteilung aufrufen, d. h. A sollte $\mathbf{Enc}_k(m)$ für zufällig gleichverteiltes m erhalten, da die Annahme an die Erfolgswahrscheinlichkeit von A nur für diesen Fall sicher gewährleistet ist.

AUFGABE 3:

(a) Sei $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ ein Pseudozufallsgenerator (PRG). Wir definieren $\overline{G}$ wie folgt:
Zur Saat s sei die Ausgabe von $\overline{G}$ gegeben als $\overline{G}(s) = G(s) \oplus 1^{l(n)}$, d. h. wir benutzen die Ausgabe von G und invertieren alle Bits.
Zeigen Sie, dass auch $\overline{G}$ ein PRG ist. [3 Punkte]

(b) Seien G_1, G_2 zwei verschiedene PRGs.
Wir definieren $G_1 \,||\, G_2$ als $(G_1 \,||\, G_2)(x) = G_1(x) \,||\, G_2(x)$, wobei $||$ die Konkatenation zweier Strings bezeichnet.
Zeigen Sie, dass $G_1 \,||\, G_2$ im Allgemeinen kein PRG ist. [4 Punkte]

Hinweise:
Für (a) sollten Sie zeigen, dass Sie aus einem Unterscheider für $\overline{G}$ einen Unterscheider für G konstruieren können.
Für (b) sollten Sie Teil (a) benutzen, um ein Gegenbeispiel zu finden. Geben Sie für Ihr Gegenbeispiel einen Unterscheider an und zeigen, dass dieser nicht-vernachlässigbare Erfolgswahrscheinlichkeit hat.

AUFGABE 4:

Sei $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec})$ ein symmetrisches Verschlüsselungsverfahren. Betrachten Sie folgende Modifikation des $\text{PrivK}^{\text{eav}}(n)$-Spiels:
Das Spiel $\text{PrivK}^{\text{eav-b}}_{A,\Pi}(n)$ mit $b \in \{0,1\}$ sei definiert als:

(1) $k \leftarrow \mathbf{Gen}(1^n)$
(2) $(m_0, m_1) \leftarrow A$
(3) $b' \leftarrow A(\mathbf{Enc}_k(m_b))$
(4) Ausgabe b'.

D.h. im Gegensatz zu $\text{PrivK}^{\text{eav-b}}(n)$ wird b von außen festgelegt anstatt vom Spiel selbst zufällig gewählt. Zudem ist die Ausgabe direkt das b' (und nicht, ein Bit, das sagt, ob $b' = b$ ist).

Zeigen Sie:[5 Punkte]
Π is KPA-sicher (nach der Defintion aus der Vorlesung) *genau dann* wenn für alle ppt. Angreifer A gilt, dass es eine vernachlässigbare Funktion `negl` gibt, so dass gilt:

$$\left|\mathbf{Ws}[\text{PrivK}^{\text{eav-0}}_{A,\Pi}(n) = 1] - \mathbf{Ws}[\text{PrivK}^{\text{eav-1}}_{A,\Pi}(n) = 1]\right| \leq \texttt{negl}(n)$$

Bemerkung:
Diese alternative Definition besagt, dass das „Verhalten“ (ausgedrückt durch die Wahrscheinlichkeitsverteilung seiner Ausgabe) eines beliebigen ppt. Algorithmus A bis auf einen vernachlässigbaren Fehler nicht von b abhängt. D.h. ein ppt. Algorithmus A kann die beiden Spiele $\text{PrivK}^{\text{eav-0}}$ und $\text{PrivK}^{\text{eav-1}}$ bis auf vernachlässigbaren Fehler nicht voneinander unterscheiden.