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

Hausübungen zur Vorlesung

Kryptographie I

WS 2011/2012

Blatt 3 / 7. November 2011 / Abgabe **bis spätestens Montag, 21.11.2011 16:00 Uhr**

AUFGABE 1:

Betrachten Sie folgende „zufällig“ aussehende Konstruktion, inspiriert durch `http://digicc.com/fido`:

$G : \{0..9\}^* \to \{1..9\}^*$ sei wie folgt definiert:

1. Eingabe: Eine Folge x aus n Ziffern, von 0 bis 9, aufgefasst als Dezimalzahl.
2. Permutiere die Ziffern von x (per uniformer Permutation aus S_n) und erhalte y.
3. Ziehe die grössere von der kleineren Zahl ab und erhalte $r = |x - y|$.
4. Streiche alle in r vorkommenden Nullen
5. Ausgabe $r \in \{1..9\}^*$.

Zeigen Sie, dass die Ausgabe von G nicht pseudozufällig ist, d.h. geben Sie einen ppt. Unterscheider D an mit $|\mathbf{Ws}[D(G(s)) = 1] - \mathbf{Ws}[D(u) = 1]| \neq \text{negl}$,
wobei s uniform aus $\{0..9\}^n$ und u uniform aus $\{1..9\}^{l(n)}$ für eine ihnen unbekannte zufällige Längenverteilung $l(n)$. [5 Punkte]

Hinweis: Überlegen Sie sich, dass für eine Zahl $t \in \mathbb{N}$ stets $t \equiv QS(t) \mod 9$
gilt, wobei $QS(t)$ die Quersumme von t im Dezimalsystem ist.

AUFGABE 2:

Sei $G : \{0,1\}^n \to \{0,1\}^{l(n)}$. Wir definieren die Stromchriffre $\Pi_s = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec})$ wie in der Vorlesung. Zeigen Sie, dass G ein Pseudozufallsgenerator ist, wenn Π_s KPA-sicher ist. [5 Punkte]

AUFGABE 3:

Sie $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec})$ ein symmetrisches Verschlüsselungsverfahren mit Nachrichtenraum $\mathcal{M}$ und Ciphertextraum $\mathcal{C}$.
Wir betrachten die Nachrichtenexpansion $f(n) = \frac{|\mathcal{C}|}{|\mathcal{M}|}$. Zeigen Sie, dass Π nicht *mult*-KPA-sicher sein kann, wenn $\frac{1}{f(n)}$ nicht vernachlässigbar ist. [5 Punkte]

Gehen Sie dazu beispielsweise wie folgt vor: Für $m \in \mathcal{M}$ sei $C_m \subset \mathcal{C}$ die Menge der möglichen Verschlüsselungen von m (unter festem $k \leftarrow \mathbf{Gen}$) und sei $\frac{1}{f(n)}$ nicht vernachlässigbar.

(a) Zeigen Sie, dass Π nicht *mult*-KPA-sicher ist, wenn $|C_m| = f(n)$ für alle $m \in \mathcal{M}$ und $\mathbf{Ws}[c = \mathbf{Enc}_k(m)] = \frac{1}{|C_m|}$ für jedes $c \in C_m$.

(b) Zeigen Sie, dass Π nicht *mult*-KPA-sicher ist, wenn $|C_m| = f(n)$ für alle $m \in \mathcal{M}$.

(c) Zeigen Sie, dass Π nicht *mult*-KPA-sicher ist.

Hinweise und Bemerkungen:
Es gibt mehrere Möglichkeiten, diese Aufgabe zu lösen; obige Vorgehensweise ist lediglich ein Vorschlag, und Sie dürfen auch direkt (c) zeigen.
Für (a,b) können Sie denselben Angreifer wie für deterministisches **Enc** benutzen, lediglich die Analyse ist anders.
Bei der Berechnung der Wahrscheinlichkeiten ist folgende Ungleichung möglicherweise nützlich (geht aber auch ohne):
Für $a_i > 0$ gilt: $\sqrt{\frac{\sum_{i=1}^{n} a_i^2}{n}} \geq \frac{\sum_{i=1}^{n} a_i}{n} \geq \frac{n}{\sum_{i=1}^{n} a_i^{-1}}$

AUFGABE 4:

Sei $G : \{0,1\}^n \to \{0,1\}^{n+1}$ ein PRG, der um 1 Bit expandiert.

Konstruieren Sie aus G einen neuen PRG $G' : \{0,1\}^n \to \{0,1\}^{n+2}$, der um 2 Bit expandiert und zeigen Sie mit einem Hybridargument, dass G' tatsächlich ein PRG ist. [5 Punkte]

Hinweise: Gehen Sie für die Konstruktion in wie folgt vor: G' ruft G zweimal auf. Bei Eingabe s_0 sei $G(s_0) = b_0 s_1$ für ein Bit b_0 und $s_1 \in \{0,1\}^n$. Verwenden Sie s_1 als neue Saat. Für das Hybridargument bieten sich folgende Hybride Verteilungen an:
H_0 ist gegeben als die Ausgabe von $G'(s)$ bei uniformem s.
H_1 entsteht aus H_0, indem man den 1.Aufruf von G als Unterroutine $b_0 s_1 := G(s_0)$ ersetzt durch $b_0 s_1 \in_R \{0,1\}^{n+1}$ uniform.
H_2 ist die uniforme Verteilung auf $\{0,1\}^{n+2}$