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

Präsenzübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 4 / 04./05. November 2013

AUFGABE 1:

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

AUFGABE 2:

Sei G ein pt-Algorithmus, der eine Funktion $\{0,1\}^n \to \{0,1\}^{\ell(n)}$ mit $\ell(n) > n$ berechnet. Wir definieren $\Pi_s = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Sicherheitsparameter n für Nachrichten der Länge $\ell(n)$ wie in der Vorlesung:

$\mathsf{Gen}(1^n)$: Gib $k \in_R \{0,1\}^n$ zurück.

$\mathsf{Enc}_k(m)$: Gib $c := G(k) \oplus m$ zurück.

$\mathsf{Dec}_k(m)$: Gib $m := G(k) \oplus c$ zurück.

Zeigen Sie, dass G ein Pseudozufallsgenerator ist, wenn Π_s KPA-sicher ist.

AUFGABE 3:

Sei $G : \{0,1\}^{n+1} \to \{0,1\}^{2n}$ ein Pseudozufallsgenerator und $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein symmetrisches Verschlüsselungsverfahren mit Nachrichtenraum $\mathcal{M} = \{0,1\}^{2n}$, sowie:

$\mathsf{Gen}(1^n)$: Gib $k \in_R \{0,1\}^n$ zurück.

$\mathsf{Enc}_k(m)$: Wähle $r \in_R \{0,1\}$ und gib $c := (c_1, c_2) = (r, G(k,r) \oplus m)$ zurück.

(a) Geben Sie einen Entschlüsselungsalgorithmus an und zeigen Sie die Korrektheit.

(b) Zeigen Sie, dass Π <u>nicht</u> mult-KPA-sicher ist.