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

Hausübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 4 / 04. November 2013

Abgabe: 12. November 2013, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (7 Punkte)**:**

Wir betrachten die Konstruktion „Stromchiffre" und den zugehörigen Sicherheitsbeweis aus der Vorlesung (siehe Folie 44 ff.), wobei $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ ein Pseudozufallsgenerator ist. Wir definieren ein symmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Sicherheitsparameter n für Nachrichten der Länge $\ell(n)$ wie folgt.

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

$\mathsf{Enc}_k(m)$: Zur Nachricht $m \in \{0,1\}^{\ell(n)}$ berechne $c := m \oplus \bar{G}(k)$, mit $\bar{G}(k) := G(k) \oplus 1^{\ell(n)}$.

(a) Geben Sie eine Entschlüsselungsfunktion an und zeigen Sie die Korrektheit.

(b) Zeigen Sie die KPA-Sicherheit von Π, indem Sie zeigen dass $\bar{G} : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ ebenfalls ein Pseudozufallsgenerator ist. Benutzen Sie dann den Satz „Stromchiffre" (Folie 45) aus der Vorlesung.

(c) Zeigen Sie die KPA-Sicherheit *direkt*, indem Sie den Beweis zur „Stromchiffre" (Folie 45 ff.) immitieren, d.h. aus einem KPA-Angreifer $\mathcal{A}$ auf Π einen Unterscheider $\mathcal{D}$ für G konstruieren.

Bitte wenden!

AUFGABE 2 (6 Punkte)**:**

Sei $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ein KPA-sicheres, symmetrisches Verschlüsselungsverfahren mit deterministischer Verschlüsselungsfunktion Enc und $\mathcal{M} = \mathcal{C} = \{0,1\}^{\ell(n)}$. Aus der Vorlesung wissen wir, dass Π dann nicht mult-KPA sicher sein kann. Betrachten Sie die folgende randomisierte Variante $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ von Π mit

$\mathsf{Gen}'(1^n)$: Gibt $k \leftarrow \mathsf{Gen}(1^n)$ zurück.

$\mathsf{Enc}'_k(m)$: Wählt bei Eingabe $m \in \{0,1\}^{\ell(n)-2}$ ein $r \in_R \{00, 01, 10, 11\}$ und gibt $c := \mathsf{Enc}_k(m, r)$ (die Nachricht wird mit der Zufallszahl aufgefüllt) zurück.

(a) Geben Sie eine Entschlüsselungsfunktion an und zeigen Sie die Korrektheit.

(b) Zeigen Sie, dass auch Π' nicht mult-KPA-sicher ist.

AUFGABE 3 (7 Punkte)**:**

Sei $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ ein Pseudozufallsgenerator. Wir konstruieren aus G folgendes symmetrische Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ für Nachrichten $m \in \{0,1\}^{2\ell(n)}$:

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

$\mathsf{Enc}_k(m)$: Für $m = (m_1, m_2)$ gib $c := (c_1, c_2) := (G(k) \oplus m_1, G(k \oplus 0^{n-1}1) \oplus m_2)$ zurück.

Wir verschlüsseln also den ersten Teil der Nachricht analog zur Stromchiffre, indem wir die Nachricht $m_1 \in \{0,1\}^{\ell(n)}$ auf die Ausgabe des Generators bei Eingabe k xorieren. Zusätzlich dazu verschlüsseln wir nun aber auch den zweiten Teil der Nachricht, für den wir lediglich das hinterste Bit des Seeds ändern.

(a) Geben Sie eine Entschlüsselungsfunktion an und zeigen Sie die Korrektheit.

(b) Sei $G' : \{0,1\}^{n-1} \to \{0,1\}^{\ell(n)}$ ein Pseudozufallsgenerator. Konstruieren Sie aus G' ein $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ mit $G(k) = G(k \oplus 0^{n-1}1)$ für alle $k \in \{0,1\}^n$. Zeigen Sie, dass G ein Pseudozufallsgenerator ist.

(c) Zeigen Sie, dass Π im Allgemeinen nicht KPA-sicher ist.

Hinweis: Sie dürfen für (c) den konstruierten Pseudozufallsgenerator aus (b) verwenden.