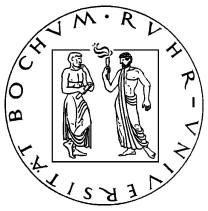
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Hausübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 3 / 14. November 2009 / Abgabe 23. November 2009, 12 Uhr

AUFGABE 1 (5 Punkte)**:**
Betrachten Sie die in der Vorlesung eingeführte Stromchiffre, die auf einem Pseudozufallszahlengenerator basiert, sowie deren Sicherheitsbeweis. Nun betrachten Sie die folgende Stromchiffre:
Sei G ein Pseudozufallsgenerator mit Expansionsfaktor $\ell(n)$ mit $\ell(n) > 4in$ für ein festes $i \in \mathbb{N}$. Wir definieren $\Pi_{s_i} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Sicherheitsparameter n für Nachrichten der Länge $\frac{\ell(n)}{i}$.

Enc: Bei Eingabe $k \in \{0,1\}^n$ und $m = (m_1, \ldots, m_{\frac{\ell(n)}{i}}) \in \{0,1\}^{\frac{\ell(n)}{i}}$ berechne

$$c := (G(k)_{ij} \oplus m_j) \text{ für } j = 1, \ldots \frac{\ell(n)}{i}$$

Dec: Bei Eingabe $k \in \{0,1\}^n$ und $c = (c_1, \ldots, c_{\frac{\ell(n)}{i}}) \in \{0,1\}^{\frac{\ell(n)}{i}}$ berechne

$$m := (G(k)_{ij} \oplus c_j) \text{ für } j = 1, \ldots \frac{\ell(n)}{i}$$

Konstruieren Sie einen Unterscheider analog zu dem in der Vorlesung, und beweisen Sie: Die so erzeugte Stromchiffre ist sicher.

AUFGABE 2 (5 Punkte)**:**
Sei Π ein nicht weiter spezifiziertes, deterministisches Verschlüsselungsschema welches Nachrichten der Länge n verschlüsselt. Aus der Vorlesung wissen wir, dass deterministisches Enc nicht mult-KPA-sicher sein kann. Wir setzen

$$\begin{aligned} \mathsf{Enc}_2(m) &:= \mathsf{Enc}(r|m) \text{ mit } r \in \{0,1\}^2 \\ \mathsf{Dec}_2(c) &:= \mathsf{Dec}(c)_2, \ldots, \mathsf{Dec}(c)_n \end{aligned}$$

Dieses Schema ist nun randomisiert. Ist es mult-KPA-sicher ? Beweisen Sie.

AUFGABE 3 (5 Punkte)**:**
Betrachten Sie das Schema aus Aufgabe 2. Konstruieren Sie einen mult-CPA-Unterscheider für dieses Schema.

AUFGABE 4 (5 Punkte)**:**
Betrachten Sie das in der Vorlesung eingeführte Π_B-Schema (Folie 62). Nehmen Sie an, es existiere ein $\mathcal{A}^{\mathsf{cpa}}$ mit nicht-vernachlässigbarem Vorteil $\epsilon(n)$. Zeigen Sie, dass F keine Pseudozufallsfunktion sein kann.