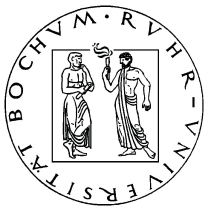
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Präsenzübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 3 / 14. November 2009

AUFGABE 1:
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 $\ell(n) > 4n$. Wir definieren $\Pi_{s_2} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ mit Sicherheitsparameter n für Nachrichten der Länge $\frac{\ell(n)}{2}$.

Enc: Bei Eingabe $k \in \{0,1\}^n$ und $m = (m_1, \ldots, m_{\frac{\ell(n)}{2}}) \in \{0,1\}^{\frac{\ell(n)}{2}}$ berechne

$$c := (G(k)_{2i} \oplus m_i) \text{ für } i = 1, \ldots \frac{\ell(n)}{2}$$

Es wird also nur mit der Hälfte der Ausgabebits des Zufallszahlengenerators verschlüsselt.

Dec: Bei Eingabe $k \in \{0,1\}^n$ und $c = (c_1, \ldots, c_{\frac{\ell(n)}{2}}) \in \{0,1\}^{\frac{\ell(n)}{2}}$ berechne

$$m := (G(k)_{2i} \oplus c_i) \text{ für } i = 1, \ldots \frac{\ell(n)}{2}$$

Es wird also nur mit der Hälfte der Ausgabebits des Zufallszahlengenerators entschlüsselt.

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

AUFGABE 2:
Betrachten Sie die Stromchiffre aus der Vorlesung. Nehmen Sie an, jeder Nachricht wird vor dem Verschlüsseln ein zuälliger 2-Bit-String vorgehangen. Konstruieren Sie einen Unterscheider, der dieses Schema im mult-KPA-Modell bricht.

AUFGABE 3:

Betrachten Sie das Schema aus Aufgabe 2. Konstruieren Sie einen CPA-Unterscheider für dieses Schema.

AUFGABE 4:
Beweisen Sie: Pseudozufallsfunktionen existieren $\Rightarrow$ Pseudozufallsgeneratoren existieren.