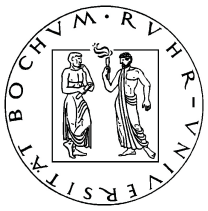
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Hausübungen zur Vorlesung

Klausuraufgaben – Kryptographie I

WS 2009

Blatt Übungsklausur / 25. Januar 2010 / Abgabe 1. Februar 2010, 12 Uhr

AUFGABE 1 (5 Punkte)**:**
Betrachten Sie das folgende Verschlüsselungsschema welches nur für eine Nachricht verwendet wird: Sei $\mathcal{M} := \mathbb{Z}_{256}$. Desweiteren sei $\mathcal{K} = \mathbb{Z}_{257}$. Nehmen Sie an, dass Gen uniform gleichverteilt aus $\mathcal{K}$ wählt. Die Verschlüsselung $\mathsf{Enc}_K(m)$ ist durch $c \leftarrow m + k \mod 256$ gegeben. Nennen Sie die Definition von *perfekter Sicherheit*. Ist das vorgeschlagene Schema perfekt sicher ? Beweisen Sie.

AUFGABE 2 (5 Punkte)**:**
Betrachten Sie die Stromchiffre aus der Vorlesung: Sei G ein Pseudozufallsgenerator mit Expansionsfaktor ℓ.

Gen Bei Eingabe von 1^n generiere $k \in_R \{0,1\}^n$

Enc Bei Eingabe von $k \in \{0,1\}^n, m \in \{0,1\}^{\ell(n)}$ gib Chiffretext $c := G(k) \oplus m$ aus.

Dec Bei Eingabe von c, k gib $m := G(k) \oplus c$ aus.

Sei nun $\mathcal{D}$ ein Unterscheider, der mit Wahrscheinlichkeit $\frac{1}{2} + \varepsilon$ eine Ausgabe von G der Länge $\frac{\ell(n)}{2}$ von echtem Zufall unterscheiden kann. Hierbei ist ε eine positive Konstante.
Konstruieren Sie hiermit einen Angreifer, der demonstriert, dass die so erzeugte Stromchiffre keine ununterscheidbaren Chiffretexte gegen KPA besitzt.

AUFGABE 3 (5 Punkte)**:**

1. Ist das one-time-pad im mult-KPA-Modell sicher ? Beweisen Sie !
2. Zeigen Sie: Jede deterministische Verschlüsselung ist im mult-KPA-Modell unsicher.
3. Zeigen Sie: Jede deterministische Verschlüsselung ist im CPA-Modell unsicher.

Geben Sie jeweils Angreifer $\mathcal{A}$ an.

AUFGABE 4 (5 Punkte)**:**
Betrachten Sie die folgende Pseudozufallsfunktionen

$$F_k : \mathbb{Z}/\langle p\rangle \to \mathbb{Z}/\langle p\rangle, x \mapsto kx \bmod p$$

Hierbei wird jeweils die kanonische Darstellung von Elementen aus $\mathbb{Z}/\langle p\rangle$ als Bitstrings benutzt. Konstruieren Sie einen Unterscheider $\mathcal{D}$, der F_k von einer echten Zufallsfunktion f unterscheidet. Tip: $\mathbb{Z}/\langle p\rangle$ ist ein Körper, man kann also Elemente invertieren !

AUFGABE 5 (5 Punkte)**:**
Sei F_k eine Pseudozufallspermutation. Zeigen Sie: Im CTR-Modus verwendet ergibt sich eine CPA-sichere Verschlüsselung.

AUFGABE 6 (5 Punkte)**:**
Zeigen Sie, dass Encrypt-and-authenticate unsicher sein kann.

AUFGABE 7 (5 Punkte)**:**
Betrachten Sie ein SPN mit komplett linearen S-Boxen. Dies bedeutet, dass jedes Chiffretextbit eine lineare Funktion der Klartext- und Schlüsselbits ist, d.h. geschrieben werden kann als:

$$\begin{aligned} c_1 &= \sum_{i\in I_1} p_i + \sum_{i\in I_1'} k_i \\ \dots &= \dots\dots \\ c_n &= \sum_{i\in I_n} p_i + \sum_{i\in I_n'} k_i \end{aligned}$$

Hierbei sind die I_j, I_j' einfache Indexmengen.
Konstruieren Sie einen Unterscheider, der dieses SPN von einer echten Pseudozufallspermutation unterscheidet.
Tip: Überlegen Sie sich, wie sich die Ausgabebits ändern, wenn man genau ein Bit der Eingabe komplementiert. Hängt diese Änderung von den anderen Eingabebits ab ?