Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 4 / 29. November 2010 / Abgabe 13. Dezember, 16 Uhr, Kasten NA 02

AUFGABE 1. Zufallspermutationen I. (5 Punkte)
Beweisen Sie, dass jede Pseudozufallspermutation eine Pseudozufallsfunktion ist (siehe Satz auf Folie 82).

Gehen Sie hierbei wie folgt vor: Zeigen Sie, dass kein Unterscheider $\mathcal{D}$ eine echte Zufallsfunktion $f \in_R \mathsf{Func}_n$ von einer echten Zufallspermutation $g \in_R \mathsf{Perm}_n$ unterscheiden kann, d.h. zeigen Sie

$$\left| \mathbf{Ws}\left[\mathcal{D}^{f(\cdot)}(1^n) = 1\right] - \mathbf{Ws}\left[\mathcal{D}^{g(\cdot)}(1^n) = 1\right] \right| \leq \mathsf{negl}(n) \ .$$

Hierfür kann es hilfreich sein, ein Ereignis Coll zu betrachten, dass $\mathcal{D}$ zwei Werte $x \neq y$ bei seinem Orakel $\mathcal{O}$ anfragt mit $\mathcal{O}(x) = \mathcal{O}(y)$. Benutzen Sie dann, dass Coll höchstens mit Wahrscheinlichkeit $\frac{q(n)^2}{2^n}$ auftritt, wenn $\mathcal{O}(\cdot) = f(\cdot)$ ist und $q(n)$ die Anzahl der Orakelanfragen bezeichnet. Was passiert für $\mathcal{O}(\cdot) = g(\cdot)$?

AUFGABE 2. Selbstinvers. (5 Punkte)
Wir nennen eine Permutation $F_k : \{0,1\}^n \to \{0,1\}^n$ *selbstinvers*, falls $F_k(F_k(x)) = x$ für alle $x \in \{0,1\}^n$ gilt, d.h. $F_k = F_k^{-1}$. Wir bezeichnen die Familie aller selbstinversen Funktionen $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ mit $\mathsf{SelfInvers}_n$. Konstruieren Sie einen Unterscheider $\mathcal{D}$, der zufällige Elemente aus $\mathsf{SelfInvers}_n$ von Zufallspermutationen unterscheidet.

AUFGABE 3. Verschlüsselung. (5 Punkte)
Sei F eine Pseudozufallsfunktion. Betrachten Sie das folgende Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ für Nachrichten $m \in \{0,1\}^{2n}$.

- $\mathsf{Gen}(1^n)$ gibt zufälliges $k \in_R \{0,1\}^n$ aus.
- $\mathsf{Enc}_k(m)$ berechnet $c = (m_0 \oplus F_k(0^n), m_1 \oplus F_k(1^n))$ wobei wir $m = (m_0, m_1)$ in zwei gleichlange Teilnachrichten $m_0, m_1 \in \{0,1\}^n$ unterteilen.
- $\mathsf{Dec}_k(c)$ berechnet $m = (c_0 \oplus F_k(0^n), c_1 \oplus F_k(1^n))$ mit $c = (c_0, c_1)$.

Ist das Verfahren KPA-sicher? Ist das Verfahren CPA-sicher? Beweisen Sie Ihre Aussagen.

AUFGABE 4. Schlechte Initialisierung. (5 Punkte)
Betrachten Sie den CBC Modus. Dieser wird so modifziert, dass der Initialisierungsvektor IV jedes Mal, wenn eine Nachricht verschlüsselt wurde, um 1 erhöht wird, d.h. für die nächste Nachricht wird $IV + 1$ verwendet. Hierbei ist die gewöhnliche Addition über den ganzen Zahlen $\mathbb{Z}$ gemeint, d.h. man fasst $IV \in \{0,1\}^n$ in kanonischer Weise via $\sum_{i=0}^{n} (IV)_i 2^i$ als ganze Zahl auf.

Beweisen Sie, dass dieser modifizierte CBC-Modus *nicht* CPA-sicher ist, indem Sie einen Angreifer angeben.

Hinweis: Unterscheiden Sie zwischen geradem und ungeradem IV.