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

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 4 / 6./8. Dezember 2010

In der ersten Aufgabe wollen wir die Hinrichtung aus dem Fakt über die „Existenz von Pseudozufallsfunktionen“ (Folie 73) aus der Vorlesung beweisen.

AUFGABE 1. Generator generieren.
Sei $F = \{F_k : \{0,1\}^n \to \{0,1\}^n | k \in \{0,1\}^n\}$ eine Pseudozufallsfunktion. Konstruieren Sie daraus einen Pseudozufallsgenerator $G : \{0,1\}^n \to \{0,1\}^{2n}$. Beweisen Sie, dass die von Ihnen vorgeschlagene Konstruktion ein Pseudozufallsgenerator ist, indem Sie aus einem Unterscheider $\mathcal{D}'$ für G einen Unterscheider $\mathcal{D}$ für F konstruieren.

AUFGABE 2. Zufallspermutation.
Betrachten Sie die Familie von Funktionen $F := \{F_k : \{0,1\}^n \to \{0,1\}^n | k \in \{0,1\}^n\}$ definiert durch $F_k(x) := k \oplus x$ wobei $\oplus$ das komponentenweise XOR bezeichnet.

a) Ist F_k für jedes $k \in \{0,1\}^n$ eine Permutation?

b) Zeigen Sie, dass F *keine* Pseudozufallspermutation ist, indem Sie einen Unterscheider $\mathcal{D}$ angeben, der ein F_k von einer echten Zufallspermutation $f \in_R \mathsf{Perm}_n$ unterscheidet.

AUFGABE 3. Schlechte Initialisierung.
Betrachten Sie den CBC Modus. Nehmen Sie an, ein Angreifer $\mathcal{A}$ kann dafür sorgen, dass der Initialisierungsvektor stets kleiner als 16 ist, d.h. $IV \in_R \{0,1\}^4 \times 0^{n-4}$. Ist der CBC Modus dann noch CPA-sicher?