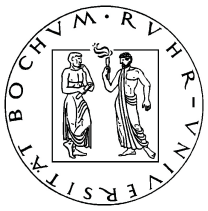
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Hausübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 4 / 27. November 2009 / Abgabe 7. Dezember 2009, 12 Uhr

AUFGABE 1 (5 Punkte)**:**

1. Betrachten Sie die Familie von Funktionen $F_k := \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ die durch $F_k(x) := kx \bmod 2^n$ definiert ist.

   Ist F_k für jedes feste k eine Permutation (Bijektion) auf $\{0,1\}^n$? Beweisen Sie.

2. Betrachten Sie die Familie von Funktionen $F_k := \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ die durch $F_k(x) := k + x \bmod 2^n$ definiert ist.

   (a) Ist F_k für ein festes k eine Permutation (Bijektion) auf $\{0,1\}^n$? Beweisen Sie.

   (b) Konstruieren Sie einen Unterscheider, der ein Element der Familie F_k von einer Zufallspermutation unterscheidet.

AUFGABE 2 (5 Punkte)**:**
Betrachten Sie die Familie von selbst-inversen Funktionen $F_k := \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$. Diese Familie habe die besondere Eigenschaft, dass $F_k \circ F_k = id$, d.h. dass $F_k = F_k^{-1}$ ist.
Konstruieren Sie einen Unterscheider, der Elemente der Familie von einer Zufallspermuation unterscheidet.

AUFGABE 3 (5 Punkte)**:**
Betrachten Sie den in der Vorlesung eingeführten CBC Modus. Angenommen, die statt echt zufälliger Wahl von IV wird eine schlechter Pseudozufallsgenerator $p : \{0,1\}^m \rightarrow \{0,1\}^{l(m)}, l(m) =: n$ verwendet. Sei D_p ein Unterscheider, der mit nicht-vernachlässigbarem Vorteil $\varepsilon(m)$ der Pseudozufallsgenerator p von echtem Zufall unterscheiden kann.
Ist der CBC-Modus mit diesem nicht-zufälligen Initialisierungsvektor noch cpa-sicher ? Beweisen Sie.

AUFGABE 4 (5 Punkte)**:**
Konstruieren Sie einen Unterscheider, der das one-time-pad im CCA-Modell bricht. Verwenden Sie hierbei *keine* Reduktion auf CPA oder mult-KPA.