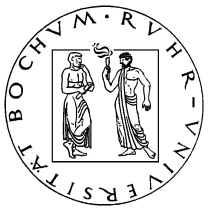
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Präsenzübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 4 / 27. November 2009

AUFGABE 1 (5 Punkte)**:**
Sei $p(n)$ die Anzahl von Permutationen auf $\{0,1\}^n$. Sei $k(n) := 2^n$, d.h. die Anzahl der möglichen Schlüssel der Länge n. Zeigen Sie, dass

$$\lim_{n\to\infty} \frac{k(n)}{p(n)} = 0$$

Was heisst das für den Anteil der durch einen Schlüssel fixer Länge "indizierbaren" Permutationen an der Gesamtmenge der Permutationen ?

AUFGABE 2 (5 Punkte)**:**
Betrachten Sie die Familie von Funktionen $F_k := \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ die durch $F_k(x) := k \oplus x$ definiert ist.

1. Ist F_k für jedes festes k eine Permutation (Bijektion) auf $\{0,1\}^n$? Beweisen Sie.
2. Konstruieren Sie einen Unterscheider, der ein Element der Familie F_k von einer Zufallspermutation unterscheidet.

AUFGABE 3 (5 Punkte)**:**
Betrachten Sie den in der Vorlesung eingeführten CTR Modus. Nehmen Sie an, Sie haben die Fähigkeit, dafür zu sorgen, dass der Initialisierungsvektor immer kleiner als 256 ist.
Ist der CTR-Modus unter dieser Annahme noch cpa-sicher ? Beweisen Sie.

AUFGABE 4 (5 Punkte)**:**
Betrachten Sie den in der Vorlesung eingeführten CBC Modus. Dieser wird nun modifiziert: Wähle Initialisierungsvektor $c_0 := IV \in_R \{0,1\}^n$. Sei $n > 16$. Für Enc gelte:

$$c_i := F_k((c_{i-1} \bmod 256) \oplus m_i) \text{ für } i = 1, \ldots, \ell$$

Für Dec gelte: Gegeben ein $c = (c_0, \ldots, c_\ell)$ berechne

$$m_i := F_k^{-1}(c_i) \oplus (c_{i-1} \bmod 256) \text{ für } i = 1 \ldots, \ell$$

Ist das resultierende Schema mult-KPA-sicher ? Beweisen Sie.