Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 5 / 11./12. November 2013

AUFGABE 1:

Ist es möglich eine Pseudozufallsfunktion $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ aus einem Pseudozufallsgenerator $G : \{0,1\}^n \to \{0,1\}^{n+1}$ zu konstruieren?

◯ **JA**

◯ **NEIN**

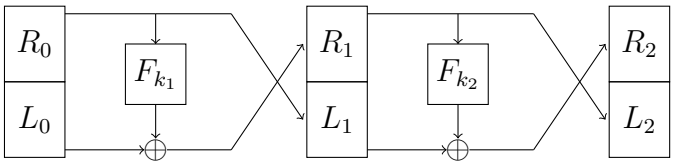
AUFGABE 2:

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion mit $F_k : \{0,1\}^n \to \{0,1\}^n$ für $k \in \{0,1\}^n$. Konstruieren Sie daraus einen Pseudozufallsgenerator $G : \{0,1\}^n \to \{0,1\}^{2n}$. Zeigen 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 3:

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Wir konstruieren aus F eine Permutation $F' : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$, die wie unten abgebildet (Feistelnetzwerk mit 2 Runden) aus der Eingabe (L_0, R_0) die Ausgabe (L_2, R_2) berechnet, wobei $k_1, k_2 \in \{0,1\}^n$ der erste bzw. zweite Teil des Schlüssels k von F' ist. Es gilt also

$$L_i = R_{i-1} \text{ und } R_i = L_{i-1} \oplus F_{k_i}(R_{i-1}).$$



Zeigen Sie, dass F' keine Pseudozufallspermutation ist.

AUFGABE 4:

Sei $F : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ eine Pseudozufallspermutation mit der Eigenschaft $F_k(x_1, x_2) \oplus F_k(x_1 \oplus k, x_2 \oplus k \oplus 1^n) = 1^{2n}$ für $x_1, x_2 \in \{0,1\}^n$.

Zeigen Sie, dass F keine *starke* Pseudozufallspermutation ist.