Übungsblatt 9

Abgabe der schriftlichen Lösungen am 11. 1. 2018 bis 13.10 Uhr

Aufgabe 42 ***mündlich***

(a) Zeigen Sie, dass der Kryptotext einer Feistel-Chiffre dadurch entschlüsselt werden kann, dass man ihn nochmals verschlüsselt, wobei die Rundenschlüssel in der umgekehrten Reihenfolge benutzt werden.

(b) Beweisen Sie, dass folgende vier Schlüssel (in Hexadezimaldarstellung) die einzigen schwachen Schlüssel für den DES-Algorithmus sind:

`0101010101010101, FEFEFEFEFEFEFEFE,`
`1F1F1F1F0E0E0E0E, E0E0E0E0F1F1F1F1`

(c) Begründen Sie, dass für schwache Schlüssel K gilt: $\mathrm{DES}(K, \mathrm{DES}(K, x)) = x$.

(d) Ein DES-Schlüssel K heißt semi-schwach, falls er genau zwei verschiedene Rundenschlüssel erzeugt (d. h. falls gilt $\|\{K^1, \ldots, K^{16}\}\| = 2$). Geben Sie zwei semi-schwache Schlüssel K und K' an, für die $\mathrm{DES}(K', \mathrm{DES}(K, x)) = x$ gilt.

Aufgabe 43 ***mündlich***

(a) Ermitteln Sie den 64-Bit-Schlüsselblock, der (bei ungerader Parität) zum 56-Bit-DES-Schlüssel `01 23 45 67 89 AB CD` (Hexadezimaldarstellung) gehört.

(b) Zeigen Sie: $\mathrm{DES}(\overline{K}, \overline{x}) = \overline{\mathrm{DES}(K, x)}$. ($\overline{x}$ ist die bitweise Negation von x.)

(c) Zeichnen Sie das Berechnungsdiagramm des DES-Schlüsselgenerators, der die Rundenschlüssel $K^1, \ldots, K^{16}$ in der umgekehrten Reihenfolge generiert.

Aufgabe 44 ***10 Punkte***

Schreiben Sie ein Programm, das den in Aufgabe 41 skizzierten Angriff auf ein SPN mittels differentieller Kryptoanalyse ausführt. Testen Sie Ihr Programm mit zufällig generierten Klartext-Kryptotext-Doppelpaaren, um die Anzahl t der zur Bestimmung des korrekten Subkey benötigten Doppelpaare herauszufinden.

Aufgabe 45 ***5 Zusatzpunkte***

Modifizeren Sie Ihre jeweiligen Programme aus Aufgabe 40 und Aufgabe 44, um den exakten Bias der in Vorlesung betrachteten linearen Approximation $X_5 \oplus X_7 \oplus X_8 \oplus U_6^4 \oplus U_8^4 \oplus U_{14}^4 \oplus U_{16}^4$ (siehe auch Abbildung 4.2) und den exakten Weitergabequotienten der Differentialspur aus Beispiel 104 zu berechnen.