

## Übungsblatt 8

### Aufgabe 43

*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, FEFEFEFEFEFEFEFEF,**  
**1F1F1F1F0E0E0E0E, E0E0E0E0F1F1F1F1**

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

### Aufgabe 44

*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:  $\text{DES}(\overline{K}, \overline{x}) = \overline{\text{DES}(K, x)}$ . ( $\overline{x}$  ist die bitweise Negation von  $x$ .)
- (c) Zeichnen Sie das Berechnungsdiagramm des DES-Schlüsselgenerators, der die Rundenschlüssel  $K^1, \dots, K^{16}$  in der umgekehrten Reihenfolge generiert.

### Aufgabe 45

**5 Punkte**

Modifizieren Sie Ihre jeweiligen Programme aus Aufgabe 40 und Aufgabe 42, 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.

### Aufgabe 46

**5 Punkte**

- (a) Alice verschlüsselt die Klartextblöcke  $x_1, x_2, \dots, x_n$  mit einer Blockchiffre zu Kryptotextblöcken  $y_1, y_2, \dots, y_n$  und sendet sie an Bob, der sie wieder entschlüsselt. Wie viele Klartextblöcke werden durch einen bei der Übertragung von Block  $y_i$  auftretenden Fehler maximal verfälscht, wenn der ECB-, CBC-, OFB-, CFB- beziehungsweise Counter-Mode benutzt wird? Unterscheiden Sie ggf. auch unterschiedliche Segmentlängen  $t$ .
- (b) Wie wirkt sich der Verlust eines Blockes  $y_i$  bei der Übertragung auf den von Bob berechneten Klartext aus?