

Übungsblatt 10

Aufgabe 37 (schriftlich, 10 Punkte)

- Zeigen Sie, dass der Kryptotext einer Feistel-Chiffre dadurch entschlüsselt werden kann, dass man ihn nochmals verschlüsselt, wobei die Rundschlüssel in der umgekehrten Reihenfolge benutzt werden.
- Beweisen Sie, dass folgende vier Schlüssel (in Hexadezimaldarstellung) die einzigen schwachen Schlüssel für den DES-Algorithmus sind:

0101010101010101, FEFEFEFEFEFEFEFEFEFEF,
1F1F1F1F0E0E0E0E, E0E0E0E0F1F1F1F1

- Begründen Sie, dass für schwache Schlüssel K gilt:

$$\text{DES}(K, \text{DES}(K, x)) = x.$$

- Ein DES-Schlüssel K heißt semi-schwach, falls er genau zwei verschiedene Rundschlüssel 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 38 (mündlich)

- Ermitteln Sie den 64-Bit-Schlüsselblock, der (bei ungerader Parität) zum 56-Bit-DES-Schlüssel 01 23 45 67 89 AB CD (Hexadezimaldarstellung) gehört.
- Zeigen Sie: $\text{DES}(\overline{K}, \overline{x}) = \overline{\text{DES}(K, x)}$. (\overline{x} ist die bitweise Negation von x .)
- Zeichnen Sie das Berechnungsdiagramm des DES-Schlüsselgenerators, der die Rundschlüssel K^1, \dots, K^{16} in der umgekehrten Reihenfolge generiert.

Aufgabe 39 (mündlich)

- 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-, CFB- bzw. OFB-Mode benutzt wird.
- Wie wirkt sich der Verlust eines Blockes y_i bei der Übertragung auf den von Bob berechneten Klartext aus?