

**Aufgabe 7:** (6 Punkte)

Wir betrachten Blockchiffren. Diskutieren Sie Vor- und Nachteile der im Skript beschriebenen Betriebsarten ECB, CBC, OFB und CFB in Bezug auf Sicherheit (welche Angriffe sind möglich?) und Fehlertoleranz (welche Auswirkungen haben Übertragungsfehler?).

**Aufgabe 8:** (8 Punkte)

- (a) Zeigen oder widerlegen Sie folgende Eigenschaften exemplarisch für die S-Box  $S_8$  beim DES-Algorithmus:
- (i) Behält man die beiden Bits 0 und 5 einer Eingabe  $A_j \in \{0, 1\}^6$  bei und verändert die mittleren 4 Bits, so wird jede mögliche Ausgabe  $B_j \in \{0, 1\}^4$  genau einmal erzeugt.
  - (ii) Unterscheiden sich zwei Eingaben genau in den beiden mittleren Bits, so unterscheiden sich die Ausgaben in mindestens zwei Bits.
  - (iii) Unterscheiden sich zwei Eingaben in zwei beliebigen Bits, so unterscheiden sich die Ausgaben in mindestens zwei Bits.
  - (iv) Unterscheiden sich zwei Eingaben in zwei beliebigen Bits der mittleren 4 Bits, so unterscheiden sich die Ausgaben in mindestens zwei Bits.
- (b) Zeigen Sie exemplarisch die Nicht-Linearität für eine S-Box des DES-Algorithmus. Zeigen Sie, dass alle anderen Bestandteile des DES-Algorithmus linear sind. Warum wäre der DES-Algorithmus mit linearen S-Boxen unsicherer? Beschreiben Sie einen möglichen Angriff gegen ein solches Verfahren.

**Aufgabe 9:** (8 Punkte)

- (a) Betrachten Sie eine beliebige Feistel-Chiffre  $E$ , die einen Klartextblock  $P = (L_0, R_0)$  zum Geheimtextblock  $C = (L_r, R_r)$  mit

$$L_i := R_{i-1}, \quad R_i := L_{i-1} \oplus f(R_{i-1}, K_i) \quad \text{für } i = 1, \dots, r$$

verschlüsselt. Zeigen oder widerlegen Sie: Damit  $E$  eine Chiffre ist (d.h. invertierbar ist), muss die Funktion  $f$  injektiv sein.

- (b) Für einen Bitvektor  $x \in \{0, 1\}^n$  sei  $\bar{x}$  das bitweise Komplement von  $x$ , d.h. für  $x_i = 0$  ist  $\bar{x}_i = 1$  und für  $x_i = 1$  ist  $\bar{x}_i = 0$ .

Zeigen Sie:  $\text{DES}(\bar{P}, \bar{K}) = \overline{\text{DES}(P, K)}$  für alle Klartexte  $P$  und alle Schlüssel  $K$ . Wie lässt sich mit Hilfe dieser Eigenschaft bei einem Chosen-Plaintext-Angriff die zu durchsuchende Menge von Schlüsseln verkleinern?