3-3 **Feistel-Chiffre**

Folgende einfache Feistel-Chiffre sei gegeben: Blocklänge = 8 Bit, 2 Runden, $k = (k1|k2)$, Rundenfunktion f: $\mathrm{S}(R_{i-1} \oplus k_i)$. Die Substitution S ist wie folgt definiert:

$\boldsymbol{x}$	0000	0001	0010	0011	0100	0101	0110	0111
$\mathrm{S}(\boldsymbol{x})$	0101	1010	0001	1001	0111	1100	0000	1111

$\boldsymbol{x}$	1000	1001	1010	1011	1100	1101	1110	1111
$\mathrm{S}(\boldsymbol{x})$	1101	0011	1000	0100	0010	1110	0110	1011

Als Schlüssel sei gegeben: $k = 11010001$. Verschlüsseln Sie den ersten Block des Klartextes $m = 1010011011001000...$ und entschlüsseln Sie das Ergebnis wieder!

3-4 **Designkriterien**

Stellen Sie die Abhängigkeitsmatrix für folgende Funktion f auf: $(y_3y_2y_1y_0) = \mathrm{f}(x_3x_2x_1x_0) = (x_1x_0x_2x_3)$. Interpretieren Sie die Abhängigkeitsmatrix (Vollständigkeit, Avalanche-Effekt, Linearität)! (Hinweis: die Matrix kann ohne Auswertung der Bitvektoren erstellt werden.)

3-5 **DES**

a) Input für die Rundenfunktion in Runde i sei $R_{i-1} = 101100110...1$, der entsprechende Rundenschlüssel $k_i = 110100011010...$ Berechnen Sie die Ausgabe der ersten beiden Substitutionsboxen!

b) Wie könnte ein Klartext-Schlüsseltext-Angriff durchgeführt werden, wenn die Rundenfunktion keine S-Boxen enthalten würde?

Ermitteln Sie die Funktionen zur Bestimmung der Schlüsselbits für folgendes Beispiel: Gegeben sei eine Feistel-Chiffre mit Blocklänge 8 Bit, 1 Runde, Rundenfunktion f: $\mathrm{P}(R_{i-1}) \oplus k_i$, P: zyklische Verschiebung nach rechts um zwei Stellen.

Bestimmen Sie mit Hilfe dieser Gleichungen den Schlüssel für das Klartext-Schlüsseltextpaar $(m, c) = (10001110, 11101010)$!

c) Zeigen Sie, dass die zweimalige Verschlüsselung mit einem schwachen Schlüssel wieder den Klartext liefert! Betrachten Sie dazu zur Vereinfachung eine auf 2 Runden reduzierte Variante des DES ohne Eingangs- und Ausgangspermutation.

d) Dem Angreifer liegt ein Klartext-Schlüsseltext-Paar vor und er möchte daraus mit vollständiger Suche den Schlüssel ermitteln. Wie lange dauert die Analyse

   – maximal
   – im Schnitt

   wenn er für die Analyse einen Rechner benutzt, der 2 Millionen Schlüssel pro Sekunde testen kann? Wie lange würde es im Vergleich dazu maximal bzw. im Schnitt dauern, wenn der Angreifer über Spezialhardware verfügt, mit der 65,28 Milliarden Schlüssel pro Sekunde getestet werden können?

e) Wie groß ist der Zeit- und Speicheraufwand, wenn der Angreifer den Schlüssel mit Hilfe einer vorab berechneten Tabelle ermitteln will?

f) Wie groß ist der ungefähre Sicherheitsgewinn von 3-DES?