3-2 **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.)

3-3 **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 **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) Warum liefert eine zweimalige Verschlüsselung mit einem schwachen Schlüssel wieder den Klartext?

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

Demonstrieren Sie den beschriebenen Angriff an folgendem vereinfachten 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 den Schlüssel für das Klartext-Schlüsseltextpaar $(m, c) = (10001110, 11101010)$!

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