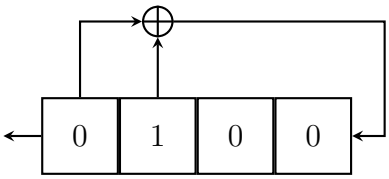
Aufgabe 1 V

Zeigen Sie, dass der Vigenère leicht brechen lässt, wenn ein Klartext-Chiffrat-Paar bekannt ist (*Known-Plaintext-Attack*). Wie viel bekannten Klartext benötigt man?

Aufgabe 2 K

Gegeben Sie das folgende linear rückgekoppelte Schieberegister mit der angegebenen Startbelegung:



Berechnen Sie die Ausgabe dieses linear rückgekoppelten Schieberegisters, bis es sicht wieder im Ausgangszustand befindet, und bestimmen Sie die Periode.

Aufgabe 3 K

Gegeben sei die folgende Blockchiffre mit Blocklänge $n = 4$ für einen gegeben Schlüssel k durch die folgende Tabelle:

Klartext		Chiffrat	Klartext		Chiffrat	Klartext		Chiffrat	Klartext		Chiffrat
0000	↔	0010	0100	↔	1010	1000	↔	0011	1100	↔	0100
0001	↔	0101	0101	↔	1001	1001	↔	1101	1101	↔	0001
0010	↔	1111	0110	↔	0000	1010	↔	1110	1110	↔	1000
0011	↔	0111	0111	↔	0110	1011	↔	1100	1111	↔	1011

Gegeben sei außerdem der Klartext: 0110 1010 0000 1010

Aufgabe 3.1

Verschlüsseln Sie den Klartext mit der angegebenen Chiffre im ECB-Modus.

Aufgabe 3.2

Verschlüsseln Sie den Klartext mit der angegebenen Chiffre im CBC-Modus. Nutzen Sie dafür den $IV = 1000$.

Aufgabe 4 V

Berechnen Sie für die folgenden Szenarien jeweils den Aufwand.

Aufgabe 4.1

Sie möchten einen DES-Schlüssel mit 56 Bit Länge durch Brute-Force brechen. Dazu besitzen Sie Spezialhardware, die $768 \cdot 10^9$ Schlüssel pro Sekunde prüfen kann. Wie lange brauchen Sie im schlimmsten Fall für das Finden des korrekten Schlüssels?

Aufgabe 4.2

Sie möchten einen AES-Schlüssel mit 128 Bit Länge brechen. Es gibt diesem Zweck spezielle Schaltungen, von denen jedes Exemplar $5 \cdot 10^8$ Schlüssel pro Sekunde ausprobieren kann. Jedes Exemplar kostet 100 € in der Anschaffung und dann 1 € pro Jahr im Betrieb. Bestimmen Sie die minimalen Kosten für das Brechen des 128 Bit Schlüssels. Ignorieren Sie dabei das Mooresche Gesetz und zukünftige Entwicklungen.