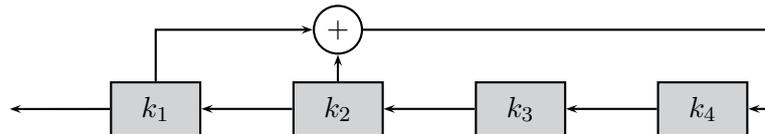


## Übungsblatt 4

### Aufgabe 15 (mündlich)



Ein lineares Schieberegister (LSR) der Länge  $m$  ist eine Anordnung von  $m$  Speicherzellen  $k_1, \dots, k_m$ , in denen jeweils ein Bit gespeichert ist. Seien  $c_0, \dots, c_{m-1} \in \{0, 1\}$  Konstanten mit  $c_0 = 1$ . Ein Rechenschritt eines LSR besteht darin, zunächst das Bit  $\ell = \bigoplus_{j=0}^{m-1} c_j \cdot k_{j+1}$  zu berechnen. Dann wird  $k_1$  ausgegeben und der Inhalt der Speicherzellen um eine Position nach links verschoben, wobei  $k_m$  den Wert  $\ell$  erhält. Die auf diese Art entstehende Bitfolge  $z_i$  mit  $z_i = k_i$ ,  $1 \leq i \leq m$ , und

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \pmod{2}, \quad i \geq 1$$

besteht aus einem sich ständig wiederholenden Muster, dessen (minimale) Länge als Periode des LSR mit dem Schlüssel  $k = (k_1, \dots, k_m, c_0, \dots, c_{m-1})$  bezeichnet wird.

- Konstruieren Sie ein LSR der Länge  $m = 5$  mit Periode 31 und zeigen Sie, dass die Periode niemals größer als  $2^m - 1$  sein kann.
- Wie kann eine auf einem LSR basierende Stromchiffre bei Kenntnis von  $2m$  aufeinanderfolgenden Klartext/Kryptotext-Bitpaaren gebrochen werden?

### Aufgabe 16 (mündlich)

Entschlüsseln Sie folgende Texte durch eine Häufigkeitsanalyse (von Bigrammen).

- HSSIT OIENT THEHS AOTRE TSEHF RTEET* (*Hinweis: Der Klartext wurde durch eine Blocktransposition, mit der Blocklänge 5 verschlüsselt.*)
- ROYEG RHOLR EVRVN VGRHE TNKRE AACAT* (*Hinweis: Der Klartext wurde durch eine Matrixtransposition mit einer  $6 \times 5$  Matrix verschlüsselt.*)

### Aufgabe 17 (schriftlich, 10 Punkte)

- Durch eine Häufigkeitsanalyse wurde festgestellt, dass eine affine Chiffre  $E$  auf  $L$  und  $T$  auf  $G$  abbildet. Bestimmen Sie den Schlüssel.
- Wie Teilaufgabe a, nur wurde  $J$  auf  $T$  und  $N$  auf  $V$  abgebildet.