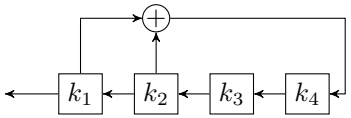
# Übungsblatt 4

**Aufgabe 15** ***mündlich***




Ein lineares Schieberegister (LSR) der Länge $m$ ist eine Anordnung von $m$ Speicherzellen $k_1, \ldots, k_m$, in denen jeweils ein Bit gespeichert ist. Seien $c_0, \ldots, c_{m-1} \in \{0,1\}$ 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

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

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

(a) 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.

(b) 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).

(a) `HSSIT OIENT THEHS AOTRE TSEHF RTEET` (*Hinweis:* Der Klartext wurde durch eine Blocktransposition mit der Blocklänge 5 verschlüsselt.)

(b) `ROYEG RHOLR EVRVN VGRHE TNKRE AACAT` (*Hinweis:* Der Klartext wurde durch eine Matrixtransposition mit einer $6 \times 5$ Matrix verschlüsselt.)

**Aufgabe 17** ***mündlich***

(a) Durch eine Häufigkeitsanalyse wurde festgestellt, dass eine affine Chiffre `E` auf `L` und `T` auf `G` abbildet. Bestimmen Sie den Schlüssel.

(b) Wie Teilaufgabe a, nur wurde `J` auf `T` und `N` auf `V` abgebildet.

**Aufgabe 18** ***mündlich***

Gegeben sei folgender mit einer Vigenère-Chiffre aus einem englischen Klartext erzeugter Kryptotext. Bestimmen Sie den zugehörigen Klartext.

```
KCCPK BGUFD PHQTY AVINR RTMVG RKDNB VFDET DGILT XRGUD DKOTF
MBPVG EGLTG CKQRA CQCWD NAWCR XIZAK FTLEW RPTYC QKYVX CHKFT
PONCQ QRHJV AJUWE TMCMS PKQDY HJVDA HCTRL SVSKC GCZQQ DZXGS
FRLSW CWSJT BHAFS IASPR JAHKJ RJUMV GKMIT ZHFPD ISPZL VLGWT
FPLKK EBDPG CEBSH CTJRW XBAFS PEZQN RWXCV YCGAO NWDDK ACKAW
BBIKF TIOVK CGGHJ VLNHI FFSQE SVYCL ACNVR WBBIR EPBBV FEXOS
CDYGZ WPFDT KFQIY CWHJV LNHIQ IBTKH JVNPI ST
```

**Aufgabe 19** ***mündlich***

(a) Seien $p_1, \ldots, p_n$ und $q_1, \ldots, q_n$ Wahrscheinlichkeitsverteilungen mit $p_1 \leq \cdots \leq p_n$. Zeigen Sie, dass $\alpha(\pi) = \sum_{i=1}^{n} p_i q_{\pi(i)}$ im Fall $q_{\pi(1)} \leq \cdots \leq q_{\pi(n)}$ einen maximalen Wert annimmt.

(b) Gegeben sei ein Kryptotext, der mit der Vigenère-Chiffre unter einem Schlüssel $k_1 \ldots k_d$ erstellt wurde. Sei $p(a)$ die bekannte Wahrscheinlichkeitsverteilung der Klartextzeichen $a \in A$ und $h_i(b)$ sei die relative Häufigkeit von $b$ unter allen Kryptotextzeichen, die mit dem Schlüsselbuchstaben $k_i$ verschlüsselt wurden. Erklären Sie, warum

$$\alpha_i(k) = \sum_{a \in A} p(a) h_i(a + k)$$

wahrscheinlich für $k = k_i$ maximal wird.

**Aufgabe 20** ***10 Punkte***

(a) Durch eine Hill-Chiffre mit unbekanntem Schlüssel wird der Klartext `CONSPIRACIES` zum Kryptotext `RPETVTZADECM` abgebildet. Bestimmen Sie die Schlüsselmatrix.

(b) Welche Matrizen verschlüsseln `CONVERSATION` zu `HIARRTNUYTUS` in der Hill-Chiffre?

(c) Bei kleiner Blocklänge $l$ kann die Hill Chiffre durch eine Häufigkeitsanalyse gebrochen werden. Im Fall $l = 2$ unterteilt man beispielsweise den Kryptotext in Bigrammblöcke und nimmt an, dass im Kryptotext häufig vorkommende Bigramme aus häufigen Bigrammen der Klartextsprache entstanden sind. Verwenden Sie diesen Ansatz, um den zu dem Kryptotext

```
LMQET XYEAG TXCTU IEWNC TXLZE WUAIS PZYVA PEWLM GQWYA
XFTCJ MSQCA DAGTX LMDXN XSNPJ QSYVA PRIQS MHNOC VAXFV
```

gehörigen englischen Klartext zu bestimmen.