Übungsblatt 4

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 6×5 Matrix verschlüsselt.)

Aufgabe 17 ***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 18 ***mündlich***

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

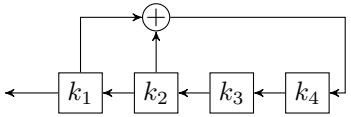
(b) Wie Teilaufgabe a, nur wurde `J` auf *T* und `N` auf *V* abgebildet.

Aufgabe 19 ***mündlich***

Es liege ein durch ein Autokey-System mit Klartextschlüsselstrom erzeugter Kryptotext y vor. Führen Sie die Analyse dieser Chiffre auf die Analyse der Vigenère-Chiffre zurück (die Schlüssellänge d kann als bekannt vorausgesetzt werden).

Hinweis: Entschlüsseln Sie y mit einem beliebigen Schlüsselwort (z.B. $k = A \dots A$) und betrachten Sie den resultierenden »Klartext«.

Aufgabe 20 ***mündlich***



Ein lineares Schieberegister (LSR) der Länge m ist eine Anordnung von m Speicherzellen $k_1, \dots, k_m$, in denen jeweils ein Bitgespeichert 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 ℓ erhält. Die auf diese Art entstehende Bitfolge z_i mit $z_i = k_i$, $1 \le i \le m$, und

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

besteht (abgesehen von einem Anfangsstück) aus einem sich ständig wiederholenden Muster, dessen (minimale) Länge als Periode des LSR mit dem Schlüssel $k = (k_1, \dots, k_m, c_0, \dots, c_{m-1})$ 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 21 ***mündlich***

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

(b) Gegeben sei ein Kryptotext, der mit der Vigenère-Chiffre unter einem Schlüssel $k_1 \dots k_d$ 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 22 ***10 Punkte***

Gegeben sei ein Kryptosystem mit Klartextraum $M = \{a, b\}$, wobei $p(a) = 1/4$ und $p(b) = 3/4$, Schlüsselraum $K = \{k_1, k_2, k_3\}$, wobei $p(k_1) = 1/2$ und $p(k_2) = p(k_3) = 1/4$ und dem Kryptotextraum $C = \{1, 2, 3, 4\}$, sowie nebenstehender Verschlüsselungsfunktion.

E	a	b
k_1	1	2
k_2	2	3
k_3	3	4

(a) Berechnen Sie die (bedingten) Wahrscheinlichkeiten $p(y)$ und $p(x|y)$ für alle Klartexte $x \in M$ und Kryptotexte $y \in C$.

(b) Berechnen Sie die Entropie $\mathcal{H}(X)$ der Klartexte, die Entropie $\mathcal{H}(K)$ des Schlüssels und die Entropie $\mathcal{H}(Y)$ der Kryptotexte, sowie die bedingte Entropie $\mathcal{H}(K|Y)$.