Übungen zur Kryptologie 1 Wintersemester 05/06
Johannes Köbler/Olaf Beyersdorff

Übungsblatt 5

Aufgabe 18 (schriftlich, 10 Punkte)

a) Durch eine Hill-Chiffre wird der Klartext `CONVERSATION` zum Kryptotext `HIARRTNUYTUS` abgebildet. Bestimmen Sie die Schlüsselmatrix.

b) 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.

Aufgabe 19 (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 20 (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 Viginère-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.