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 (z.B. $l = 2$) kann die Hill Chiffre durch eine Häufigkeitsanalyse gebrochen werden. Man unterteilt den Kryptotext in Bigrammblöcke und nimmt an, dass im Kryptotext häufig vorkommende Bigramme aus häufigen Bigrammen der Klartextsprache entstanden sind. Verwenden Sie diesen Ansatz bei folgendem Kryptotext, der aus einem englischem Klartext gebildet wurde:

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

Aufgabe 19

Gegeben sei folgender Kryptotext, der aus einem englischen Klartext mit einer Vigenère-Chiffre erzeugt wurde. 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

a) Seien $p_1, \dots, p_n$ und $q_1, \dots, q_n$ zwei Wahrscheinlichkeitsverteilungen, wobei $p_1 \leq \cdots \leq p_n$ ist. 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) Erklären Sie, warum der in der Vorlesung definierte Wert $\alpha_i(k)$ wahrscheinlich für $k = k_i$ maximal wird.