Übungen zur Kryptologie 1 Wintersemester 07/08

Johannes Köbler/Sebastian Kuhnert

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.

Aufgabe 21 (mündlich)

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 $\mathcal{H}(K|Y)$.

Aufgabe 22 (mündlich)

Zeigen Sie:

a) Ein Kryptosystem ist absolut sicher, wenn $\sum_{k:E(k,x)=y} p(k) = 1/\|M\|$ für alle $x \in M$ und $y \in C$ gilt. Im Fall $\|C\| = \|M\|$ und $p(x) > 0$ für alle $x \in M$ ist dies auch notwendig.

b) Ein Kryptosystem mit $\|K\| < \|M\|$ und $p(x) > 0$ für alle $x \in M$ ist nicht absolut sicher.

c) Ein Kryptosystem ist genau dann absolut sicher, wenn $\mathcal{H}(X|Y) = \mathcal{H}(X)$ ist.

d) Ist ein Kryptosystem mit $p(x) > 0$ für alle $x \in M$ absolut sicher, dann ist es unter allen Klartextverteilungen absolut sicher.

Aufgabe 23 (mündlich)

Für zwei Zufallsvariablen X und Y sei $\mathcal{H}(X, Y) = \sum_{x,y} p(x, y) \cdot \log(1/p(x,y))$ die (gemeinsame) Entropie von X und Y. Zeigen Sie:

a) $\mathcal{H}(X, Y) = \mathcal{H}(Y) + \mathcal{H}(X|Y) = \mathcal{H}(X) + \mathcal{H}(Y|X)$.

b) $\mathcal{H}(X, Y) \leq \mathcal{H}(X) + \mathcal{H}(Y)$, mit Gleichheit genau dann, wenn X und Y unabhängig sind.