MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
April 29, 2005

Cryptography
Problem Sheet #3

Problem 9 The following text has been obtained by an English plaintext using Vigenère encryption with a keyword of length 4. Find the keyword and decrypt the text.

```
MRFC DONE KPOL RAZN VOUT KNKS KSJV XAAV XGOV CTVE ITOR WOZG MOTC VEAR
XOUG OCOA SCHY KCJB ENAB PTOR CUIW OCAV CKHU XSAU OCVQ OBYR KKLE CTOV
CBVB UTYN MEZP BYWG YGYN ZHFS BOTV DSPA STPN VAUQ VITV DEKH CEIL DHLR
QYWG SAUF COTR POBE DHVH CEUQ IEHE CANB DOAU OTDR XTPR DHJR XTBE IWOR
BEPG ZLHL ODHP BUJV KLYB VEPA DHLB ETJB WEVS LOAU GOYY NWHE C
```

Problem 10 Let $x, y \in \mathbb{Z}_m^N$ be random texts in the alphabet $\mathbb{Z}_m$, where the letters in x have been chosen indepently according to the probability distribution $\vec{p} = (p_i)_{i\in\mathbb{Z}_m}$ and the letters in y according to the probability distribution $\vec{q} = (q_i)_{i\in\mathbb{Z}_m}$.

(a) Calculate the expectation value $\mathbb{E}\,\kappa(x, y)$ of the kappa index of x and y.

(b) Consider the special case where $q_i = p_{\sigma(i)}$ for some permutation $\sigma : \mathbb{Z}_m \to \mathbb{Z}_m$. Prove that for fixed $\vec{p}$ and variable σ the absolute maximum of $\mathbb{E}\,\kappa(x, y)$ is attained for $\sigma = \mathrm{id}_{\mathbb{Z}_m}$.

Problem 11 Let

$$\mathcal{P} := \{\vec{p} = (p_i)_{i\in\mathbb{Z}_m} \in \mathbb{R}^m : \sum_{i\in\mathbb{Z}_m} p_i = 1 \text{ and } p_i \geq 0 \text{ for all } i \in \mathbb{Z}_m\}$$

be the set of all probability distributions on $\mathbb{Z}_m$. For $\vec{p}, \vec{q} \in \mathcal{P}$ we define the convolution product $\vec{r} = \vec{p} * \vec{q}$ by

$$r_n := \sum_{i\in\mathbb{Z}_m} p_i q_{n-i}.$$

(a) Show that $\vec{p} * \vec{q}$ belongs again to $\mathcal{P}$, and that the convolution product is commutative and associative, i.e.

$$\vec{p} * \vec{q} = \vec{q} * \vec{p} \quad \text{and} \quad (\vec{p} * \vec{q}) * \vec{r} = \vec{p} * (\vec{q} * \vec{r}) \quad \text{for all } \vec{p}, \vec{q}, \vec{r} \in \mathcal{P}.$$

(b) Let $\vec{u} \in P$ be the uniform distribution, i.e. $u_i = 1/m$ for all $i \in \mathbb{Z}_m$.
Prove that $\vec{u} * \vec{p} = \vec{u}$ for all $\vec{p} \in \mathcal{P}$.

Problem 12 With texts $x, y \in \mathbb{Z}_m^N$ as in problem 10, let $z := x + y \in \mathbb{Z}_m^N$ be the text obtained by addition modulo m. Prove that the probability distribution of the letters in z is $\vec{p} * \vec{q}$.

Due: Friday, May 6, 2005, 14:10 h