MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
May 4, 2007

Cryptography

Problem Sheet #3

Problem 9

Prove that a Vigenère encryption with a keyword without repeated letters is a special case of the OFB mode of a monoalphabetic substitution as defined in problem 3.

Problem 10 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 11

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

b) Suppose that $\vec{p} \in \mathcal{P}$ satisfies $p_i > 0$ for all $i \in \mathbb{Z}_m$. Show that

$$\vec{p}^{\,n} := \underbrace{\vec{p} * \ldots * \vec{p}}_{n \text{ factors}}$$

converges for $n \to \infty$ to the uniform distribution $\vec{u} \in \mathcal{P}$, cf. problem 10 b).

Hint. Define $M_n := \max\limits_{i\in\mathbb{Z}_m}\{(\vec{p}^{\,n})_i\}$ and prove that $(M_n)_{n\in\mathbb{N}}$ is monotonically decreasing.

p.t.o.

Problem 12

Let $n \geq 1$ and σ a permutation of the set $\{1, 2, \ldots, n\}$. We define a transposition cipher $T = T_{n,\sigma}$: The text is divided into blocks of n^2 letters. These letters are written as the n rows $(x_{i1}x_{i2}\ldots x_{in})$, $i = 1, 2, \ldots, n$, of an $n \times n$-matrix. The transformed block is the sequence of columns $(x_{1\sigma(j)}x_{2\sigma(j)}\ldots x_{n\sigma(j)})$, $j = 1, 2, \ldots, n$, in the permuted order. (If the last block is shorter than n^2 letters, only the upper part of the matrix is filled, and the columns become shorter.)

The following text was obtained from an English plaintext using a transposition cipher as described above with $n = 5$:

```
RNIHHCASTCPLITITYSEQYASENEEGEURNHFKISBIPOACR
```

a) Find the plaintext and the permutation σ.

b) For fixed n, let G be the set of all transpositions $T_{n,\sigma}$ as described above. Decide whether G is a group (with respect to composition of maps).

Due: Friday, May 11, 2007, 14:10 h