MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
May 9, 2007

Cryptography

Problem Sheet #4

Problem 13

Let M be a finite set with $m \geq 2$ elements. As defined in problem 8, an involution of M is a map $\sigma : M \to M$, different from the identity, with $\sigma \circ \sigma = \mathrm{id}_M$.

a) Prove: If m is odd, then every involution σ of M has at least one fixpoint, i.e. there exists an $x \in M$ with $\sigma(x) = x$.

b) Let $m = 2k$ be even. Determine the number of involutions of M without fixpoints.

Problem 14

Let $\sigma : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ be an involution without fixpoints. Determine the number of permutations $\pi : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ such that

$$\pi^{-1}\sigma\pi = \sigma.$$

Problem 15

Let $N = 2n$ be an even positive integer and $\mathcal{P} = \mathcal{C} = \mathbb{Z}_2^N$. Let $\mathcal{K} = S_N$ be the group of all permutations of the set $\{1, 2, \ldots, N\}$. For $\pi \in \mathcal{K}$ define the encryption $E_\pi : \mathcal{P} \to \mathcal{C}$ in the obvious way by letting π permute the components of a plaintext vector $x \in \mathbb{Z}_2^N$. Set $D_\pi = (E_\pi)^{-1}$. Let $\mathbb{P}_{key}$ be the uniform probability distribution on $\mathcal{K}$ and let $\mathbb{P}_{plain}$ be an arbitrary probability distribution with $\mathbb{P}_{plain}(x) > 0$ for all $x \in \mathcal{P}$.

a) Show that the cipher system $(\mathcal{P}, \mathcal{C}, \mathcal{K}, E, D, \mathbb{P}_{plain}, \mathbb{P}_{key})$ does not provide perfect secrecy.

b) Consider the following subsystem: Let $\mathcal{P}_1 = \mathcal{C}_1$ be the set of all vectors $x = (x_1, \ldots, x_N) \in \mathbb{Z}_2^N$ such that exactly n of the components x_i are zero. Prove that the cipher system $(\mathcal{P}_1, \mathcal{C}_1, \mathcal{K}, E, D, \mathbb{P}_{plain1}, \mathbb{P}_{key})$ provides perfect secrecy. Here $\mathbb{P}_{plain1}$ is any probability distribution on $\mathcal{P}_1$ with $\mathbb{P}_{plain1}(x) > 0$ for all $x \in \mathcal{P}_1$.

Problem 16

A sequence $x_i \in \mathbb{Z}_{25}$, $i \geq 0$, has been generated by a linear congruential generator

$$f : \mathbb{Z}_{25} \to \mathbb{Z}_{25}, \quad x \mapsto (ax + b) \bmod 25,$$

with an initial element $x_0 \in \mathbb{Z}_{25}$ and recursion relation $x_{i+1} = f(x_i)$.
We identify $\mathbb{Z}_{25}$ with the alphabet `A` ... `Z` without the letter `J`. The following ciphertext has been obtained from an English plaintext by adding the sequence (x_i) modulo 25.

```
LHHBLADYTXIUCZDDKPKVTLZXNEG
```

The beginning of the plaintext was `THE`. Calculate a, b and the plaintext.

Due: Wednesday, May 16, 2007, 14:10 h