Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 2

Friday, April 26, 2019

Problem 1. *(Sequence of affine ciphers)*

Suppose you encrypt a message $m \in \mathbb{Z}_q$ using an affine cipher $e_k(m)$ with key $k = (a, b) \in \mathbb{Z}_q^* \times \mathbb{Z}_q$.

a) Compute the n-fold encryption $c = e_{k_n}(...e_{k_2}(e_{k_1}(m))...)$ for keys $k_i = (a_i, b_i)$, $i = 1, ..., n$.

b) Is there an advantage using n subsequent encryptions, rather than using a single affine cipher? Substantiate your claim.

Problem 2. *(Hill cipher)* The matrix A shall be used in a Hill cipher, i.e., $\mathbf{c} = A\mathbf{m}$.

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \in \mathbb{Z}_2^{3\times 3} = \mathbb{F}_2^{3\times 3}.$$

a) Give explicit formulae for the encryption function.

b) Does a decryption function exist? If yes, determine the decryption function.

Problem 3. *(Number of keys)* Compute the number of possible keys for the following cryptosystems.

a) Substitution cipher with the alphabet $\Sigma = \mathbb{Z}_l = \{0, \ldots, l-1\}$

b) Affine cipher with the alphabet $\Sigma = \mathbb{Z}_{26} = \{0, \ldots, 25\}$

c) Permutation cipher with a fixed blocklength L