RWTHAACHEN UNIVERSITY Lehrstuhl für Theoretische Informationstechnik

Homework 3 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Naehrig

05.11.2007

Exercise 7. The permutation $\pi = (2, 11, 5, 8)(3, 6, 7, 4)(9, 10)$ defines a permutation cipher with block length $k = 11$. Determine the number of character sequences of length 11 over the usual alphabet with 26 letters, whose cryptogram does not differ from the plaintext.

Exercise 8. Consider the matrix

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

It shall be used in a Hill cipher. Why is this possible? Give explicit formulae for the encryption function and determine the decryption function.

Exercise 9. Given a permutation π of the numbers $1, \ldots, 8$ and a bit sequence $k = (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8) \in \mathbb{Z}_2^8$ of length 8. Consider the following function:

$$E : \mathbb{Z}_2^8 \to \mathbb{Z}_2^8, (m_1, \ldots, m_8) \mapsto (m_{\pi(1)} \oplus k_1, \ldots, m_{\pi(8)} \oplus k_8).$$

Here $\oplus$ denotes addition modulo 2.

(a) Show, that E can be used as an encryption function. Determine plaintext space and ciphertext space.

(b) What is the key space and what is its cardinality?

(c) Determine the decryption function.