Homework 2 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

03.11.2009

Exercise 4.

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.

Exercise 5.

(a) Prove the following equivalence:

$$A \in \mathbb{Z}_n^{m \times m} \text{ is invertible } \iff \gcd(n, \det(\mathrm{A})) = 1.$$

(b) Is the following matrix invertible? If yes, compute the inverse matrix.

$$M = \begin{pmatrix} 7 & 1 \\ 9 & 2 \end{pmatrix} \in \mathbb{Z}_{26}^{2 \times 2}.$$

Exercise 6. The following alphabet with 29 elements

$$X = \{A, B, \ldots, Z, \#, *, -\}$$

can be identified with $\mathbb{Z}_{29} = \{0, 1, \ldots, 28\}$. Suppose the blocklength is $m = 2$. Decrypt the ciphertext **Y J G - H T** which is encrypted by a Hill cipher with

$$U = \begin{pmatrix} 3 & 13 \\ 22 & 15 \end{pmatrix} \in \mathbb{Z}_{29}^{2 \times 2}.$$