Homework 1 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

14.04.2011

Exercise 1. The following ciphertext[1] is given:

```
Rgneidvgpewn xh iwt hijsn du bpiwtbpixrpa itrwcxfjth gtapits id phetrih du
xcudgbpixdc htrjgxin hjrw ph rdcuxstcixpaxin, spip xcitvgxin, tcixin
pjiwtcxrpixdc, pcs spip dgxvxc pjiwtcixrpixdc.
```

(a) Which classical cryptosystem is used for encryption?

(b) Decipher the given ciphertext. What is the secret key?

(c) Explain why this cryptogram is easy to decrypt.

Exercise 2. A permutation cipher with blocklength 8 revealed the following ciphertext[1]:

REXETSIH ONSICESI UCIFTFID REHTLIET

(a) Decrypt the ciphertext and explain your approach.

(b) Determine the corresponding permutations π and π^{-1}.

Exercise 3. Let $a, b, c, d \in \mathbb{Z}$. a is said to divide b if (and only if) there exists some $k \in \mathbb{Z}$ such that $a \cdot k = b$. Notation: $a \,|\, b$. Prove the following implications:

(a) $a \,|\, b$ and $b \,|\, c \quad \Rightarrow \quad a \,|\, c$.

(b) $a \,|\, b$ and $c \,|\, d \quad \Rightarrow \quad (ac) \,|\, (bd)$.

(c) $a \,|\, b$ and $a \,|\, c \quad \Rightarrow \quad a \,|\, (xb + yc) \quad \forall\, x, y \in \mathbb{Z}$.

Exercise 4. The matrix A shall be used in a Hill cipher

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

(a) Give explicit formulae for the encryption function.

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

[1] The plaintext is an English text.