RWTH AACHEN UNIVERSITY

Lehrstuhl für Theoretische Informationstechnik

Homework 2 in Cryptography I

Prof. Dr. Rudolf Mathar, Markus Rothe, Milan Zivkovic

08.05.2014

Exercise 4. 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
pjiwtcixrpixdc, pcs spip dgxvxc pjiwtcixrpixdc.
```

- Which classical cryptosystem is used for encryption?
- Decipher the given ciphertext. What is the secret key?
- Explain why this cryptogram is easy to decrypt.

Exercise 5. A permutation cipher with block length 8 revealed the following ciphertext[2]:

```
REXETSIH ONSICESI UCIFTFID REHTLIET.
```

a) Decrypt the ciphertext and explain your approach.

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

Exercise 6. 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 an 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.

[2] The plaintext is an English text.

Exercise 7.

(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 8. Compute the number of possible keys for the following cryptosystems:

(a) Substitution cipher,

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

(c) Permutation cipher with a fixed blocklength k.