RWTH AACHEN UNIVERSITY Lehrstuhl für Theoretische Informationstechnik

Homework 2 in Advanced Methods of Cryptography

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

08.11.2013

Exercise 4. Consider a *permutation cipher* and a plaintext of n symbols divided into blocks of l symbols each such that $l \mid n$, i.e.,

$$\boldsymbol{m} = (m_1, \ldots, m_n) = (m_1, \ldots, m_l \mid m_{l+1}, \ldots, m_{2l} \mid \cdots \mid m_{n-l+1}, \ldots, m_n).$$

The key is a permutation π over the set $\{1, \ldots, l\}$. Each block of l message symbols $\hat{\boldsymbol{m}} = (\hat{m}_1, \ldots, \hat{m}_l)$ is encrypted as $\hat{\boldsymbol{c}} = (\hat{m}_{\pi(1)}, \ldots, \hat{m}_{\pi(l)})$, whereas each block of ciphertext symbols $\hat{\boldsymbol{c}} = (\hat{c}_1, \ldots, \hat{c}_l)$ is decrypted as $\hat{\boldsymbol{m}} = (\hat{c}_{\pi^{-1}(1)}, \ldots, \hat{c}_{\pi^{-1}(l)})$.
For block length $l = 8$, you intercept the following ciphertext:

```
REXETSIH ONSICESI UCIFTFID REHTLIET.
```

(a) Decrypt the ciphertext[1] and determine the permutations π and π^{-1}.

(b) Is the given cipher mono- or polyalphabetic? Substantiate your answer.

Exercise 5. The following ciphertext[1] $\mathbf{c}$ has been encrypted by a Caesar cipher (cf. lecture notes, Section 2.2.1):

```
SDSCS XCEPP SMSOX DDYZB YDOMD YEBCO VFOCG SDRVK GCGOX
OONDY ZBYDO MDYEB COVFO CGSDR WKDRO WKDSM C.
```

(a) Compute the index of coincidence $I_{\mathbf{c}}$. Is the given cipher mono- or polyalphabetic?

(b) Decrypt the ciphertext and determine the corresponding key k.
Explain your approach.

Exercise 6. Let e_K be an encryption function. Show for the Caesar cipher that subsequently encrypting a message m with a total number of n keys is the same as performing a single encryption with only one key, i.e.,

$$e_{k_n}(e_{k_{n-1}}(\ldots(e_{k_2}(e_{k_1}(m)))\ldots)) = e_k(m).$$

(a) Compute the corresponding key k resulting from the sequence of keys $k_1, \ldots, k_n$.

(b) Does the order of the sequence of keys matter? Substantiate your answer.

[1] The corresponding plaintext is an English text.