Homework 2 in Advanced Methods of Cryptography

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

23.10.2012

Exercise 4. Consider a *permutation cipher* (cf. lecture notes, Section 2.3) with plaintext of n symbols divided into blocks of k symbols each such that $k \mid n$, i.e.,

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

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

(c) Determine the index of coincidence.

Exercise 5. Let e_K be an encryption function.

(a) Show for both the Caesar cipher and the permutation 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.,

$$e_{k_n}(e_{k_{n-1}}(\ldots(e_{k_2}(e_{k_1}(m)))\ldots)) = e_k(m),$$
$$e_{\pi_n}(e_{\pi_{n-1}}(\ldots(e_{\pi_2}(e_{\pi_1}(m)))\ldots)) = e_\pi(m).$$

Compute the corresponding keys k and π respectively.
Does the order of the sequence of keys matter? Substantiate your answer.

Now, let $e_k(m)$ denote a single encryption by a Caesar cipher with a key k and $e_\pi(m)$ a single encryption by a permutation cipher with a permutation π.

(b) Show that $e_\pi(e_k(m)) = e_k(e_\pi(m))$ holds.

[1] The corresponding plaintext is an English text.

Exercise 6.

The following ciphertext[2] was encrypted by a Vigenère cipher:

```
MESSTDRHZH UWLPWCEJMY XCSWLPXFRD XCZBTVXSIS RZICVUVYIY KCGKIPCJRV
MXDCEWEWNW FHWERBQIET ISFWSQRZYE ITEUFVIGVB GRXSVRJDVQ CCEGWRISNW
QTESEVEYUQ EDJEJARQSQ KVRPSFEHNL RSRZYVEYUB VQIYZBRUMY XGJHVPXWSW
IOKCGKICRQ RRJXVBJKSL SCIHEWCSYV IOVGVUIOGC JHVQFFJLXS ZBGKIDVFVQ
KDNOFESFER GKIDKFRQKE YOAGATCZGR KZMSEQILTV EDGPSIGWLP PKRUILCZBI
XSVAQHGPZJ RGJZIOARXS VFELRRNOFP EOVWAWLPCO AGSQDCEGSC ZBGKIQZFRV
SQDCHQXOFC ZWLPUOENPZ IRFDYCFBSR VRVRVQWPTF RWEXRGGHVC ZBTWSNFBGU
SWRZYRXSVF FDROZBGRXS ZGELRRYSCR YCVRULWNII ROXJYWFPEW ZQRDROYWFZ
MWCHBGSXZB NWILCZYLJP FBRUMYXHBU YWVHUHQLCZ BQIMPCAHXS VTEHIWRBQV
SQDWQGPPVO EWLQVZYWSE YSCRAPICSW LPIWAJFFKH UHVPNSEHWZ DSJKSCVGVV
XPUOYDWERZ YLEYTSBIQP EOAGIWMSFP ECTVRGERRW AVXEYSNUQT VGBIQZIRBU
EYUCAWLPJZ BSIDFTZRYY KRBRQEYSLI SFXVGISCKV RIVPVRBPSQ DWQGPPVOEW
LGZQGRVJNO FQILIPHWXS VDBZICFTGK ICZBTFSFCR ARXMVIAGSY VWGZEDZBGK
MDDCZHRENV RQEWCVBSIS RRSDHPUHUD XTJWYGYCJC ARJEYSXLRR KCBNYAYWFI
EEYSEVWHFF QVEFICAWLP VBRPCZWHUH JCVSCHSACS FRJXZRQOIP RFGKALJRRI
ILKSQWLPIW AJTLJGRGXZ ZGVOHFIKUR LLUHULWZES PKEYTSGRHP JHERCPMWYI
SCVJRUFFKH UHLPRFGVSQ DSADVPVOFL PJTCEUYAKS QDROKVRUMY XCSSSHVFUD
WLNWYOSQZH FRAYZHOHXC RMRGMDZZQX VEFVVVHPRH UDROJCZHXS ZBTVXSRHFK
SFCRARXSRJ REIPETBUKZ KHRQAPISYR WEYWFWSCPP RFEXVZRJIY UZRJIYUPRF
EXVALWLLER SRVENCNQHL YOYIXSFIFD ROPSNUWEYS ELRRGOFVIO FIGRJLCZXQ
SHCSQJIFEH VOASVBPKEY TSPDQPZHRQ WYRFRGEYVK OHECVFGKIC ZBTFEXVHBW
LPTFRDXFIS TRPWLAJKSE FCXLXOVSCL REFHUHXFEB ROWZWHUHQT JHLPSFEHNL
RDRBQWLPIS VWGZEGHPIO YWZWLPIWAJ FCFITKXEFU BOPFDIAQEE LFNOPZEUYL
JPWCEIMGVV HQHCVRLHEC JWGSSTJCAH HSZGZLRORB QLREYSTOSZ DCSJSWCIZV
GLMSVWALZH RGHLIYAHWD TFRSXMRQXL REFHUHJZIS FWWZWHUHAZ IZQUYXFIEJ
VPNCSDWSRR BZMYKVRHED KKULWAVFFR JLEOZHPPJG SHECRBQWLP IWAJSQGCJH
VAVFPHMGVR VWWEZARKEO ECJFSXVWGD FLERBQIOXC YOYXSIGVSX VHULRRYOCS
IYVRGKEEKV RUMYXRVGRZ KWAWIYUWGZ EDGWPNIOLD OBXSVABVXF EZVNIWPQEH
EELFRLQLXW ADFWVOURFM ZHOLPMFPNJ KTEGBIXSVG ULVPWCEWLP KWZHWHZZYV
SZEQBPIHYS AKSMSWGVAT CZFKEAVHUH JZIHHQIDFT NOP
```

(a) Compute the index of coincidence.

(b) Determine the key using the Kasiski-Babbage method and explain your approach.

The above ciphertext is available as a file in the *L2P* course room and also at:
www.ti.rwth-aachen.de/teaching/cryptography/uebungen_amc_ws1213/ciphertextEx6.txt
A computer assisted evaluation is recommended.

[2]The corresponding plaintext is an English text. The relative frequency of the most frequent letter E in the English language is approximately 12.7%.