Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 8
Version 11.06.2020

Exercise 1.

The cipher text `ENWR ERMR ERLR` dates back to 50 B. C. and is likely to be the result of the application of a classical shift cipher to the alphabet of the $q = 26$ capital Latin letters. Restore the plain text.

Exercise 2.

The subsequently stated cryptograms have been created with the aid of different affine ciphers over the $q = 26$ capital letters of the Latin alphabet. Restore the respective plain texts and the particular key of the underlying cryptosystem exploiting the additional given information.

1. The cipher text `AREF LMRH` has been created with an affine cipher which encrypts `C` and `N` as `L` and `S`, respectively.
2. The cipher text `CBOJ PMBX` has been created with the aid of an affine cipher with $a := 9$ and unknown b.
3. The cipher text `DZWLGVP` has been created with the aid of an affine cipher with $b := 13$ and unknown a.

Exercise 3.

The cipher text `CEYV DLYV` has been obtained from a plain text over the $q = 26$ capital letters of the Latin alphabet using Vigenère's autokey cipher with key `ZEUS`. Restore the underlying plain text.

Exercise 4.

Combing through his new office at Cambridge University, Prof. Crypto Graph discovers some old Scytales together with two old cryptograms. Help him to restore the associated plain texts.

1. `XOWOATIAOSXPHABTRRSXPLOSOHIEEXEEBTUEQLRX`
2. `OTEECUUIHOIRRIQOETOLFUPINROYAOTENSEO`

Hint: Take care of letters appearing unnaturally frequent in the cryptograms.

Exercise 5.

In order to encrypt a plain text over the $q = 26$ capital letters of the Latin alphabet, a permutation cipher of block length $m = 5$ has been used. In order to enhance security even more, the resulting string has been encrypted with the aid of a one-way-key cipher with key `DIFFICULTCIPHER`. This procedure resulted in the cipher text `UCNSLKXYEINXBWE`. Restore the associated plain text.

Exercise 6.

Espionage has revealed that the cipher text `HLULPT YHANWG ODAPRE` has been created

applying Vigenère's cryptosystem to the $q = 26$ capital letters of the Latin alphabet. However, the precise block length m is still unknown. On the other hand, it has been identified that the plain text starts with `CAUT`. Restore the overall plain text and the exploited Vigenère key.

Exercise 7.

Using a substitution cryptosystem over the alphabet $A = B := \{\mathtt{A}, \mathtt{E}, \mathtt{L}, \mathtt{T}\}$, the cipher text `ELEEA TELAT` has been created. It is known that the exploited key is involutoric while changing each letter during encryption. First, determine all keys which actually satisfy these conditions. Afterwards, restore the plain text.

Exercise 8.

1. The cipher text `OMZFAS` has been created using Hill's cryptosystem over the $q = 26$ capital letters of the Latin alphabet and the key

$$K = \begin{pmatrix} 17 & 9 \\ 3 & 8 \end{pmatrix}.$$

   Restore the plain text.

2. Find all involutoric keys of Hill's cryptosystem over $\mathbb{Z}_6$ which have the particular form

$$K = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

   where $a, b, c \in \mathbb{Z}_6$ are parameters.