Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Homework Sheet 5
Version 10.06.2020

Homework 1.

Find all involutoric keys of the affine cryptosystem over an alphabet of $q = 15$ letters.

Homework 2.

At Cambridge University, Prof. Crypto Graph now dabbles in encrypting some of his own secrets using Scytales. Thinking about his time at Oxford University, he designs the cryptograms

1. `TSYTOABHORDEREEFPNHREOCOETASDRET` and
2. `OTWHANDESTSTSITIRERHYAEHEROMEM`.

Restore the plain texts.

Homework 3.

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 Vigenère's autokey cipher with key `COGITO`. This procedure resulted in the cipher text: `JLOFMYEFFKXBQMEEIWQSPRBRU`. Restore the associated plain text.

Homework 4.

In order to encrypt a plain text over the $q = 26$ capital letters of the Latin alphabet, an affine cryptosystem with parameter $a := 25$ and unknown parameter $b \in \mathbb{Z}_{26}$ has been applied. Afterwards, the resulting string has been encrypted with the aid of Hill's cryptosystem based on the key

$$K := \begin{pmatrix} 9 & 1 & 15 \\ 21 & 0 & 9 \\ 19 & 3 & 20 \end{pmatrix}.$$

The associated cryptogram reads as `TELFON`. Restore the underlying plain text.