Homework 2 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

04.11.2008

Exercise 4. Determine 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.

Exercise 5. Let e_K be one of the ciphers from Exercise 4. Show that encrypting a message m with key K_1 and the result afterwards with the key K_2 is the same as doing one encryption with a different key K_3, i. e.

$$e_{K_2}(e_{K_1}(m)) = e_{K_3}(m).$$

Compute the corresponding keys for the concatenation in all three cases.

Exercise 6.

a) Prove the following statement.
A matrix $A \in \mathbb{Z}_m^{n \times n}$ is invertible, if and only if $\gcd(m, \det(A)) = 1$.

b) The alphabet

$$X = \{A, B, \dots, Z, \#, *, -\}$$

with 29 elements can be identified with $\mathbb{Z}_{29} = \{0, 1, \dots, 28\}$. Suppose the blocklength is $m = 2$. Decrypt the ciphertext **Y J G - H T** which is encrypted by a Hill cipher with

$$U = \begin{pmatrix} 3 & 13 \\ 22 & 15 \end{pmatrix} \in \mathbb{Z}_{29}^{2\times 2}.$$