Homework 2 in Cryptography I

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

21.04.2011

Exercise 5.

(a) Prove the following equivalence:

$$A \in \mathbb{Z}_n^{m \times m} \text{ is invertible} \iff \gcd(n, \det(\mathrm{A})) = 1.$$

(b) Is the following matrix invertible? If yes, compute the inverse matrix.

$$M = \begin{pmatrix} 7 & 1 \\ 9 & 2 \end{pmatrix} \in \mathbb{Z}_{26}^{2\times 2}.$$

Exercise 6. Compute 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 7. Let e_K be one of the ciphers from the exercise above.

(a) 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.

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

(b) Compute the corresponding keys for the concatenation in all three cases.