Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Qinwei He

Exercise 2

Friday, May 5, 2017

Problem 1. *(matrix inverse)*

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.

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

Problem 2. *(sequence of affine ciphers)*

Suppose you encrypt a message $m \in \mathbb{Z}_q$ using an affine cipher $e_k(m)$ with key $k = (a, b) \in \mathbb{Z}_q^* \times \mathbb{Z}_q$.

a) Compute the n-fold encryption $c = e_{k_n}(...e_{k_2}(e_{k_1}(m))...)$ for different keys $k_i = (a_i, b_i)$ with $i = 1, ..., n$.

b) Is there an advantage using n subsequent encryptions, rather than using a single affine cipher? Substantiate your claim.

Problem 3. *(number of keys)* Compute the number of possible keys for the following cryptosystems:

a) Substitution cipher with the alphabet $\Sigma = \mathbb{Z}_l = \{0, \dots, l-1\}$

b) Affine cipher with the alphabet $\Sigma = \mathbb{Z}_{26} = \{0, \dots, 25\}$

c) Permutation cipher with a fixed blocklength L