**Crypto Homework 1: Classical ciphers**

**Hadi Abu-Maruf – 301188504**

Deadline: **23.04.2017**. Submit the homework assignment on the course website, not on email. The solutions from pairs are accepted.

Submit a single file in **zip** format (only!) that contains:

- For each exercise a source file (\*.c) and function files. Each source file starts at q\_ and his exercise number (for example, q\_1, function files q1\_encrypt, q1\_decrypt).

- Word document led by two task names and ID numbers (should work in pairs only), followed, solutions and examples of input/output for every problem - as required.

A type of symmetric block cipher **Door** is given as follow:

**Plane space** X = {0…25}

**Cipher space** Y = {0…25}

**Key space values** The key is a *m* × *m* matrixA whose elements are integers in *Ζ*26.

The Encryption function defined by repeated encryption ER(x0) is given by the following way:

**x1 = x0 \*A%N,**

**xR = (xR-1 \*A+ xR-2)%N**, for each R>=2.

For example, for **R=1** the Encryption function is defined by: **E1(x0) = x0 \*A %N**,

for **R=2**: **E2(x0) = (x1 \*A+ x0) %N = (x0 \* A2 + x0**) **%N=(x0 \* (A2 + I)**) **%N,**

where I is the identical matrix.

**Exercise 1**

1. Describe the decryption function for R = 3 and R=4.
2. How many different possible keys exist for m = 3 and R=3?

We use the function we learn in lecture 3 that say:

1. Write a procedure in C to encrypt a given plain text by mean of the cipher **Door** for m=2 and R=3 with the **input parameters**: plain text and encryption key, **output**: the cipher text. The function prototype: **door\_encryption(ptext, key).**

Comment: a plain text is a string of the length between 2 and 20 characters, a key is a string given by a matrix 2X2. For example: key = "road" = "r, o, a, d" = 17, 14, 0, 3;

A = r o = 17 14

a d 0 3

Encrypt yours names. When choosing a key, check (calculate and display) if it is admissible. Give example of input/output – plain text, key, cipher text.

1. Write a procedure in C to decrypt a cipher text for m=2 and R=3 with the input parameters: the cipher text and encryption key matrix, output: the plain text.

The function prototype: **door\_decryption(ctext, key).** Give example of input/output – cipher text, encryption key, plain text.

**Exercise 2**

Write a procedure in C performing the iterative attack against the algorithm **Door** with the parameters: R=3, m=2, and decrypting the message. Use the function **door\_encryption(text, key)** from Ex.1. How many iterations does it take? Give example of input/output – cipher text, encryption key, plain text.

***Have* a pleasant vacation *and successful* work*!***