## 

## Security systems

Assignment No.1

**Ομάδα LAB41446304**

|  |
| --- |
| ***Τρίμας Χρήστος 2016030054*** |

## Purpose of Exercise:

Implement a few basic crypto algorithms in C, using linux environment.

## Files:

In the folder, there are four files.

**simple\_crypto.h** : Contains three functions that implement the three encryption and decryptions algorithms(One Time Pad, Caesar cipher, Vigenere cipher). It also contains every useful library that one needs to compile and run the algorithms. Finally, there are three helper functions to make life easier for the demo program.

-randomGenerator function, returns a random string equal to the size of the plaintext, that is needed for the OTP algorithm. This function utilizes the /dev/urandom file of the linux system to create that randomness.

-nonBufferedOvfInput function, returns the user input. In order to avoid buffer overflow attacks, and make my program take as input, unknown size strings, I use malloc and realloc to change the buffer size. The nonBufferedOvfInputUpper function, does the same, except that takes the input and transforms it in uppercase letters. This function is vital for the vigenere algorithm, if the user gives a lowercase symbol in his input.

**simple\_crypto.c**: This is a c file, that implements the functions of the above library.

**demo.c**: Contains the main function that one can compile and run to check the algorithms.

**Makefile**: a makefile that compiles and runs the demo file.