Security of Data Lab 2 (Spring 2018)

Dr. A. V. Vasilakos

Chair Professor and Head
Lab of Networks and Cybersecurity,
Innopolis University, Russia
Email: t.vasilakos@innopolis.ru

Exercise on symmetric encryption techniques

Total marks:10

Time:02 Hours

Exercise 01

Write a program for Caesar Cipher algorithm **Marks:2.5**

Test your program with following:
plaintext: HELLO
key: 3
ciphertext: KHOOR

Exercise 02

Write a program for Hill cipher scheme **Marks:2.5**

Test your program with following:
plaintext: Mississippi
Key Matrix:

3	25
24	17

ciphertext: “CIKKGEUWEROY” corresponding to “MISSISSIPPIK”

Note that: If there are not enough letters to form blocks of 2, pad the message with some letter, say K.

Exercise 03

Write a program for Rail Fence cipher scheme

Marks:2.5

Test your program with following:
plaintext: defendhim
key (depth/level): 3
ciphertext: dehenifdm

Exercise 04

Write a program for playfair cipher scheme

Marks:2.5

Test your program with following:
plaintext: HAMMER
key (5x5 matrix): MONARCHY
ciphertext: BOAUKM