**Information Systems Security**

**Assignment**

**Due date: (1/08/2020)**

**(4 students in each group**)

***In this assignment, you can create a group of maximum 4 students to work together. Each student is fully responsible for discussing his/her group’s project in details; each student must be able to describe/run/test and defend his/her group’s project.***

**Cryptosystem description**

In this assignment, you have to be able to implement Caesar, vigener ,transposition cipher, and play fair, and link them together in output/input relationship; that is the output of the previous cipher is the input of the next cipher. Similarly, in the decryption process, the output of the previous decoder is the input of the next decoder.

**Implementation details**

The input of your system would be a document of English text. The text will go through four main ciphers; first: Caesar, second, vigener third transposition cipher, and fourth play fair Cipher .The input text will be encrypted using : Caesar cipher The result of the Caesar cipher will be the input of the next cipher and so on. The output would be a document of ciphertext. Users should be able to pick the encryption keys for each cipher.

**Users should also be able to decrypt the ciphertext documents.**

The system’s **GUI** must show the intermediate results of each cipher (encryption/decryption). The system must also be able to read an input text file and the key or you can use a text file for the plain tect and the key for each cipher and write the final output (ciphertext in encryption and plaintext in decryption) into another text file.

Deadline to submit the assignment to [imsobeidat@hu.edu.jo](mailto:imsobeidat@hu.edu.jo) write your name group and your university numbers 1-08-2020 .

Your group will as of your university numbers

------Good luck-------