Assignments (*Computer Security and Privacy*)

Assignment #1
Submission Deadline: February 7, 2018
Maximum Marks: 30

In this programming assignment you will implement the Hill cipher in C/Python/Java. In particular you will implement and submit three independent programs

- KeyGen
- Encrypt
- Decrypt

These program shall perform the following functions:

- KeyGen: This program will take, as input, a positive integer m. It will output a random key K from the keyspace of Hill Cipher, that is a random $m \times m$ matrix K such that K is invertible over $\mathbb{Z}_{26}$. The key should be copied to a file named **key.txt**.
- Encrypt: Inputs to this program are two files - **key.txt** and **msg.txt**. The file msg.txt will contain messages over alphabet "a-z" (all in small case). No special characters are allowed. This program will implement Hill cipher encryption over the msg (in **msg.txt**) using the key (in **key.txt**) and copy the resulting ciphertext into **ciphertext.txt** file.
- Decrypt: Inputs to this program are two files - **key.txt** and **ciphertext.txt**. This program will implement Hill cipher decryption over the ciphertext (in **ciphertext.txt**) using the key (in **key.txt**) and copy the resulting message into **output.txt** file.

Important Instructions!!

- The implementation of Hill cipher requires you to build subprograms such as "gcd, modular inverse computation, matrix multiplication, matrix inversion over $\mathbb{Z}_{26}$. You cannot use libraries for these tasks. You have to implement these subprograms yourself.
- Programs that implement Hill cipher only for a fixed value of m - such as $m = 2, 3$ will not be accepted.
- 20 marks, out of 30, are for correctness. The rest 10 will account for programming efficiency and proficiency.

Assignment #2
Submission Deadline: February 11, 2018
Maximum Marks: 30

In this programming assignment you will implement a ciphertext-only attack on substitution cipher using frequency analysis. In particular you will implement and submit a KeyRecover program that will perform the following task.

- The input to KeyRecover program is an arbitrary encrypted message (encrypted using Substitution cipher) that is sufficiently large. You are then required to output the corresponding message and the secret key that used to encrypt this message. In doing so, you will take the help of KeyRecover program and an extensive manual analysis.
- **What else you will be given?** For uniformity, you will be provided with the encryption program. You can use this program to encrypt messages of your choice (key is know to you). Practice the key-recovery attack that you will be implementing.
- The input to your program will be emailed to you on February 11. You will be given sufficient time to mount your ciphertext-only attack on the input and to submit the corresponding plaintext, secret key pairs.

Important Instructions!!

- 20 marks, out of 30, are for correctness. The rest 10 will account for programming efficiency and proficiency.
- Note that, each one of you will get a different input. So it is important that you learn the frequency analysis well by your self. The method can be found in the reference book along with example analysis. Your KeyRecover program needs to automate some its components.