NIRMA UNIVERSITY
Institute of Technology
B.Tech. Computer Science and Engineering
2CSDE54 Information and Network Security

1. Perform encryption, decryption using the following substitution techniques
   a) Ceaser cipher
   b) ROT-13
   c) Hill Cipher

Discussion: The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is named after Julius Caesar, who apparently used it to communicate with his generals. More complex encryption schemes such as the Vigenere employ the Caesar cipher as one element of the encryption process. The widely known ROT13 'encryption' is simply a Caesar cipher with an offset of 13. The Caesar cipher offers essentially no communication security, and it will be shown that it can be easily broken even by hand.

To pass an encrypted message from one person to another, it is first necessary that both parties have the 'key' for the cipher, so that the sender may encrypt it and the receiver may decrypt it. For the caesar cipher, the key is the number of characters to shift the cipher alphabet.

First we translate all of our characters to numbers, 'a'=0, 'b'=1, 'c'=2, ... , 'z'=25. We can now represent the caesar cipher encryption function, e(x), where x is the character we are encrypting, as:

$$e(x) = (x + k)(mod\ 26)$$

Where k is the key (the shift) applied to each letter. After applying this function the result is a number which must then be translated back into a letter. The decryption function is :

$$e(x) = (x - k)(mod\ 26)$$

Program Execution:

```
Enter the PLAIN TEXT for Encryption:
   >information
Enter the CAESERKEY between 0 and 25:
   >7
ENCRYPTION
CIPHER TEXT :pumvythapvu
DECRYPTION
PLAIN TEXT :information
```

What's Rot13?

Rot13 is a simple "encryption" algorithm designed to make text illegible, but very easily "decrypted". It's used on USENET to post material that may be offensive - the reader has to choose to convert it back to plain text. Rot13 simply adds 13 to the value of each character, and wraps around back to "A" when it gets to "Z". So "A" becomes "N", "B" becomes "O", and "N"

becomes "A". It works on both upper and lower case characters and leaves non-alphabetic characters as they were.

Question:

1. Crack the following plaintext TRVJRI TZGYVIJ RIV HLZKV VRJP KF TIRTB
2. What key do we need to make “CAESAR” become “MKOCKB”?
3. What key do we need to make “CIPHER” become “SYFXUH”?
4. Use the Caesar cipher to encrypt your first name
5. How can we find the decryption key from the encryption key?

Instruction: You need to take the **input.txt** file and generate the cipher text in the **output.txt**

Hill cipher: Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Input : Plaintext: ACT

Key: GYBNQKURP

Output : Ciphertext: POH

We have to encrypt the message ‘ACT’ (n=3).

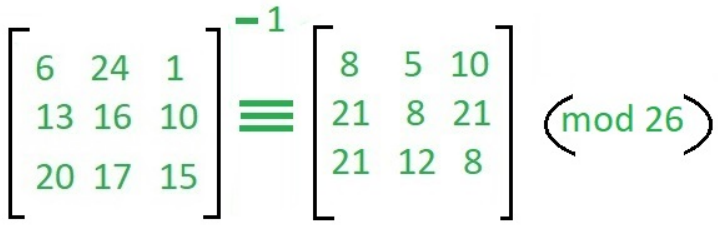
The key is ‘GYBNQKURP’ which can be written as the nxn matrix	The message ‘ACT’ is written as vector:
$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$

The enciphered vector is given as: which corresponds to ciphertext of ‘POH’

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} (\text{mod } 26)$$

Decryption :

To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).The inverse of the matrix used in the previous example is:



For the previous Ciphertext ‘POH’: which gives us back ‘ACT’.

Assume that all the alphabets are in upper case.