Cryptography and Network Security (ECSE352L) Lab-3

1) Create a web application to implement a symmetric cryptosystem called "Vigenere Cipher" to ensure the security service known as data confidentiality. Basically, Vigenere cipher is used to encrypt the alphabetic text by using a series of different Caesar ciphers, based on the letters of a keyword.

   Encryption process

   The plaintext(P) and key(K) are added modulo 26.

   C= (P + K) mod 26

   Decryption Process

   D= (C- K+ 26) mod 26

   Expected Output:

   The web application accepts the Plaintext ("**Computer Science**") from a text field T1, cryptographic Key **("Bennett")** from a text field T2 and displays the encrypted message in the text field T3, when the **encrypt** button is pressed. Further, implement the cryptosystem for decryption process.

2) Write a program to implement "Vernam one-time pad" (Additive Cipher). The cryptographic key should exactly same as the length of message which is encrypted. The key is truly random and specially auto generated.

Encryption Process: C= K⊕P

Decryption Process: P= C⊕K

Use the given truth table and encrypt the plaintext**: 0 0 1 0 1 1 0 1 0 1 1** 1 using One-time pad (Key): **1 0 0 1 1 1 0 0 1 0 1 1**

K	P	C
0	0	0
0	1	1
1	0	1
1	1	0