**NAME: KSHITIJA SHAMRAO JADHAV**

**PRN:2019BTECS00053**

**ASS 4: Vigenere**

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of [polyalphabetic substitution](https://en.wikipedia.org/wiki/Polyalphabetic_cipher). A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the [*Vigenère square or Vigenère table*](https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher#/media/File:Vigen%C3%A8re_square_shading.svg).

* The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible[Caesar Ciphers](https://www.geeksforgeeks.org/caesar-cipher/).
* At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
* The alphabet used at each point depends on a repeating keyword.

#include<iostream>

#include<string.h>

using namespace std;

int main(){

    char msg[] = "THECRAZYPROGRAMMER";

    char key[] = "HELLO";

    int msgLen = strlen(msg), keyLen = strlen(key), i, j;

    char newKey[msgLen], encryptedMsg[msgLen], decryptedMsg[msgLen];

    //generating new key

    for(i = 0, j = 0; i < msgLen; ++i, ++j){

        if(j == keyLen)

            j = 0;

        newKey[i] = key[j];

    }

    newKey[i] = '\0';

    //encryption

    for(i = 0; i < msgLen; ++i)

        encryptedMsg[i] = ((msg[i] + newKey[i]) % 26) + 'A';

    encryptedMsg[i] = '\0';

    //decryption

    for(i = 0; i < msgLen; ++i)

        decryptedMsg[i] = (((encryptedMsg[i] - newKey[i]) + 26) % 26) + 'A';

    decryptedMsg[i] = '\0';

    cout<<"Original Message: "<<msg;

    cout<<"\nKey: "<<key;

    cout<<"\nNew Generated Key: "<<newKey;

    cout<<"\nEncrypted Message: "<<encryptedMsg;

    cout<<"\nDecrypted Message: "<<decryptedMsg;

return 0;

}

**OUTPUT:**

