## Name: Muhammad Rafiq

## Seat No: B17101061

## Course: Network Security & Cryptography (NS'21 Lab)

## Assignment : Assignment # 3 ( Vigenere Cipher)

## Section: A

## Modulus Algorithm

In [21]:
```
def modulo(a, m)->int:
    R = abs(a) % m
    if a>= 0:
        R =R
    elif a < 0 and R != 0:
        R = m - R
    elif a < 0 and R == 0:
        R = 0
    return R
```

## 1- Task 1: Write a program for Vigenère Cipher that can encrypt and decrypt it. Using your preferable working platform.

## Vigenere Cipher

In [22]:

```
''' A = 0 ... Z = 25'''

def vigenere_encrypt(my_string,K,m) -> str:
    enc_string = ""
    my_string = my_string.upper()
    for i in range(len(my_string)):
        enc_string += chr(modulo((ord(my_string[i])-65 + ord(K[i % len(K)])-65), m) + 65)
    return enc_string

def vigenere_decrypt(my_string,K,m)->str:
    dec_string = ""
    for i in range(len(my_string)):
        dec_string += chr(modulo((ord(my_string[i]) - 65 - ord(K[i % len(K)])-65), m) + 65)
    return dec_string

def vigenere_cipher(choice):
    if choice == 'e':
        my_input = input("Enter the text to be encrypted: ")
        K = input("Enter the key: ")
        enc_string = vigenere_encrypt(my_input.replace(" ", "").upper(),K.upper(),26)
        print("Encrypted String is: " + enc_string)
    elif choice == 'd':
        enc_string = input("Enter the text to be decrypted: ")
        K = input("Enter the key: ")
        my_string = vigenere_decrypt(enc_string.replace(" ", "").upper(), K.upper(),26)
        print("Original String after decryption is: " + my_string)

    else:
        my_input = input("Enter the text to be encrypted: ")
        K = input("Enter the key: ")
        enc_string = vigenere_encrypt(my_input.replace(" ", "").upper(),K.upper(),26)
        print("Encrypted String is: " + enc_string)
        my_string = vigenere_decrypt(enc_string, K % 26,26)
        print("Original String after decryption is: " + my_string)

```

**Task 2: Decode the cipher text "OZELNVUXTGWHVUBJLVTYDKURVDVFKPNA" using your program and find the hidden text.**

In [23]:
```
1 vigenere_cipher('d') # d for decrypt
```

```
Enter the text to be decrypted: OZELNVUXTGWHVUBJLVTYDKURVDVFKPNA
Enter the key: tryhard
Original String after decryption is: VIGENERECIPHERISNOTHARDTODECRYPT
```

## Task 3: Decode the cipher text "XCECKVJSLKOUHTXIIYEXBOGRTIEEBXJIG" using key "Practice". without using your program

In [24]:
```
1 vigenere_cipher('d') # d for decrypt
```

```
Enter the text to be decrypted: XCECKVJSLKOUHTXIIYEXBOGRTIEEBXJIG
Enter the key: Practice
Original String after decryption is: ILEARNHOWTOSOLVETHEVIGENERECIPHER
```