**Applied Cryptography and Network Security**

**(CSI3002)**

**LAB ASSESSMENT – 1**

**Name : RITHIV.R**

**Reg No : 19MIC0113**

**Slot : L27+L28**

**1.Encryption and decryption using Caesar Cipher**

**CODE:**

print('RITHIV.R-19MIC0113\n')

print('Caesar Cipher')

plaintext = input('Enter the plaintext:').lower()

ciphertext = ""

decryptedtext = ""

caser = {chr(97+k):k for k in range(26)}

print('\nEncryption:\n')

for i in plaintext:

en = (caser[i]+3)%26

ciphertext = ciphertext+chr(97+en)

print("\tCiphertext:",ciphertext)

print('\nDecryption:\n')

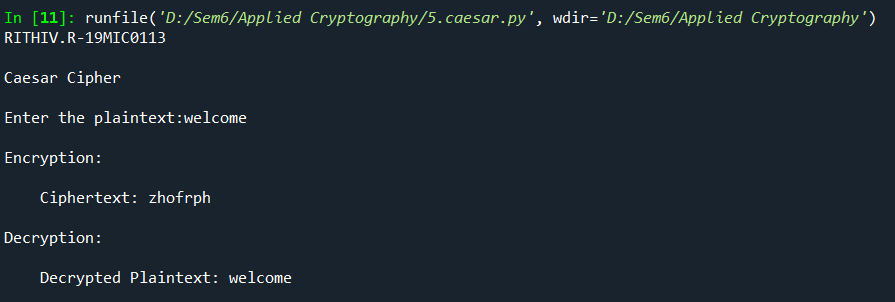
for i in ciphertext:

de = (caser[i]-3)%26

decryptedtext = decryptedtext+chr(97+de)

print("\tDecrypted Plaintext:",decryptedtext)

**OUTPUT:**



**2.Encryption by using Playfair Cipher**

**CODE:**

print('RITHIV.R-19MIC0113\n')

print('\nPlayfair Cipher - Encrpytion\n')

key = input("Enter the key:").lower().replace('j', 'i')

plaintext = input("Enter the plaintext:").lower()

array = ""

newplain = ""

ciphertext = ""

for i in key:

if(i not in array):

array = array+i

alpha = [chr(97+i) for i in range(26) if chr(97+i) not in array and chr(97+i) !='j']

for i in alpha:

array = array + i

playfair = []

for i in range(5):

x = array[i\*5:(i\*5)+5]

temp = [j for j in x]

playfair.append(temp)

print("\nPlayfair Cipher Constructed:\n")

for i in range(5):

for j in range(5):

if(playfair[i][j]!='i'):

print(playfair[i][j],end="\t")

else:

print("i/j",end="\t")

print()

for i in plaintext:

if(len(newplain)):

if(newplain[-1]!=i):

newplain = newplain+i

else:

newplain = newplain + 'x' + i

else:

newplain = newplain+i

if(len(newplain)%2!=0):

newplain = newplain + 'x'

for i in range(len(newplain)//2):

value = newplain[i\*2:(i\*2)+2]

if('j' in value):

value= value.replace('j','i')

first = -1

second = -1

for k1,i in enumerate(playfair):

for k2,j in enumerate(i):

if(j==value[0]):

first = [k1,k2]

if(j==value[1]):

second = [k1,k2]

if(first[0]==second[0]):

if(first[1]==4 or second[1]==4):

if(first[1]==4 and second[1]!=4):

first[1]=0

second[1]=second[1]+1

elif(first[1]!=4 and second[1]==4):

second[1]=0

first[1]=first[1]+1

else:

first[1]=first[1]+1

second[1]=second[1]+1

ciphertext = ciphertext+playfair[first[0]][first[1]]

ciphertext = ciphertext+playfair[second[0]][second[1]]

elif(first[1]==second[1]):

if(first[0]==4 or second[0]==4):

if(first[0]==4 and second[0]!=4):

first[0]=0

second[0]=second[0]+1

elif(first[0]!=4 and second[0]==4):

second[0]=0

first[0]=first[0]+1

else:

first[0]=first[0]+1

second[0]=second[0]+1

ciphertext = ciphertext+playfair[first[0]][first[1]]

ciphertext = ciphertext+playfair[second[0]][second[1]]

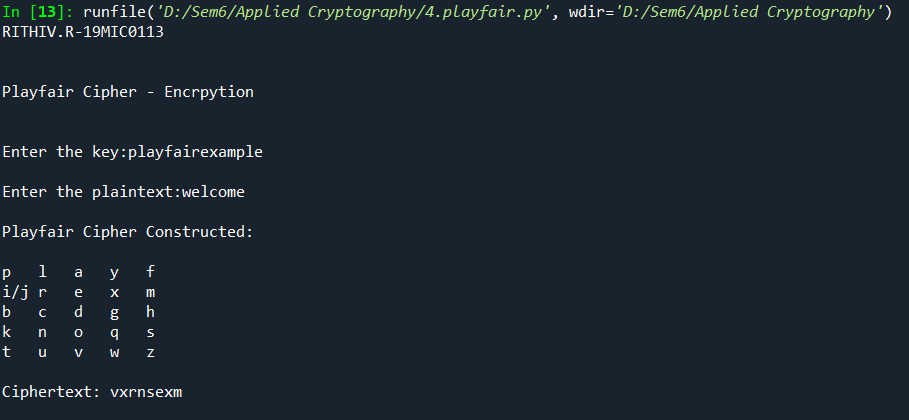
else:

ciphertext = ciphertext+playfair[first[0]][second[1]]

ciphertext = ciphertext+playfair[second[0]][first[1]]

print('\nCiphertext:',ciphertext)

**OUTPUT:**



**3.Encryption and Decryption by using Hill Cipher**

**CODE:**

print('RITHIV.R-19MIC0113-(Hill Cipher)\n')

from sympy import Matrix as mn

plaintext=input("Enter the plaintext:").lower()

n = int(input("Enter the value n:"))

key = input("Enter the key:").lower()

plainlist = []

plainvector = []

array = []

keymatrix = []

ciphertext = ""

cipherarray = []

decryptedtext = ""

val = {chr(97+i):i for i in range(26)}

val1 = {i:chr(97+i) for i in range(26)}

def mul(arr1,arr2):

global val1

m = []

for k1,i in enumerate(arr1):

sum = 0

for j,k in enumerate(i):

sum = sum + (arr1[k1][j]\*arr2[j])

x = sum%26

m.append(val1[x])

return m

for i in range(0,len(plaintext)-(len(plaintext)%n),n):

temp = []

for j in range(n):

temp.append(plaintext[i+j])

plainlist.append(temp)

if(len(plaintext)!=(len(plainlist)\*n)):

temp = [i for i in plaintext[len(plaintext)-(len(plaintext)%n):]]

for i in range(n-len(temp)):

temp.append('a')

plainlist.append(temp)

for i in plainlist:

temp = [val[j] for j in i]

plainvector.append(temp)

print("\nModified Plain Text for performing Encryption:",end = " ")

for i in plainlist:

temp = ""

for j in i:

temp = temp+j

print(temp,end=" ")

print("\n")

for i in range(len(key)//n):

value = ' '.join(key[i\*n:(i\*n)+n]).split()

array.append(value)

temp = [val[i] for i in value]

keymatrix.append(temp)

print("KeyMatrix:")

for i in keymatrix:

for j in i:

print(j,end="\t")

print()

for i in plainvector:

x = mul(keymatrix,i)

for i in x:

ciphertext = ciphertext + i

print("\nCipher Text Encrypted:",ciphertext,"\n")

for i in range(0,len(ciphertext),n):

tempor = " ".join(ciphertext[i:i+n]).split(' ')

my = []

for i in tempor:

my.append(val[i])

cipherarray.append(my)

result = mn(keymatrix)

result = result.inv\_mod(26)

myar = [[0 for j in range(n)] for i in range(n)]

counter = 0

for i in range(n):

for j in range(n):

myar[i][j] = result[counter]

counter = counter+1

print("Inversemod26 key Matrix:")

for i in myar:

for j in i:

print(j,end="\t")

print()

for i in cipherarray:

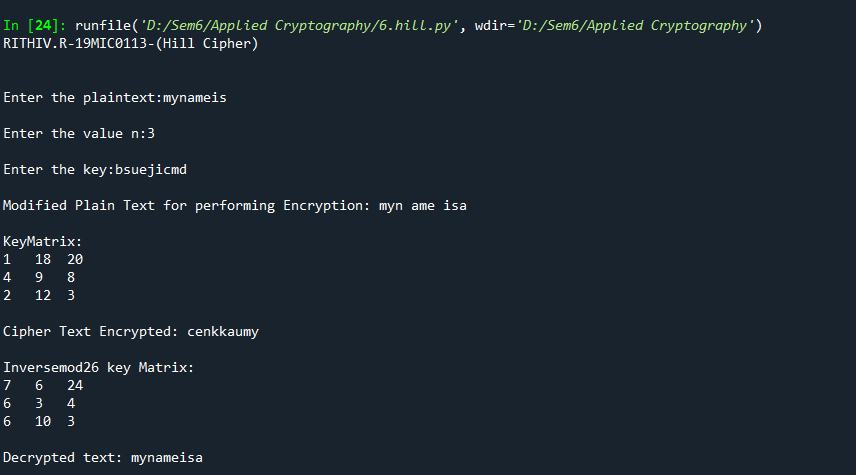
x = mul(myar,i)

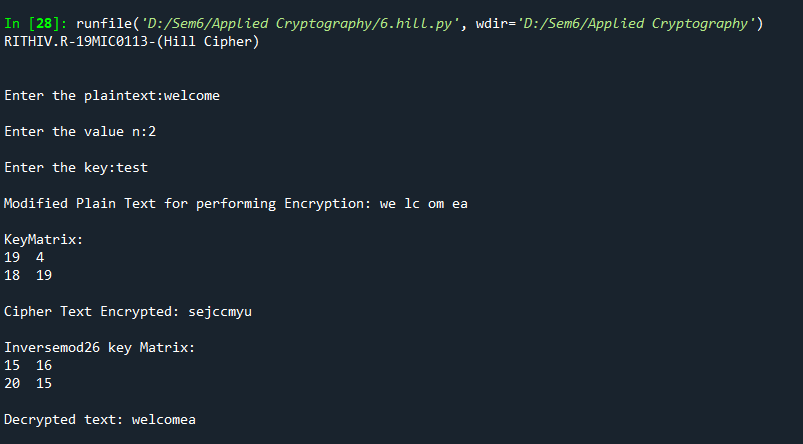
for i in x:

decryptedtext = decryptedtext + i

print("\nDecrypted text:",decryptedtext)

**OUTPUT:**





**CODE FILE UPLOADED IN GOOGLE DRIVE:**

**Caser Cipher:**

[**https://drive.google.com/file/d/18ICx4PtS33vCb1lCrzBwdTvgtRB1rvuC/view?usp=sharing**](https://drive.google.com/file/d/18ICx4PtS33vCb1lCrzBwdTvgtRB1rvuC/view?usp=sharing)

**Playfair Cipher:**

[**https://drive.google.com/file/d/1r2kTEri4AD2qdzM6HzAfJfn9hfokS3-l/view?usp=sharing**](https://drive.google.com/file/d/1r2kTEri4AD2qdzM6HzAfJfn9hfokS3-l/view?usp=sharing)

**Hill Cipher:**

**https://drive.google.com/file/d/1N9AJF1qPOc0wXRcLwyzYB-o1PaihPN6S/view?usp=sharing**