Name: Ayush Patel Enrolment 22162171038 Class B Batch 55

Practical – 5

Subject – Crypto

Aim

Alice wants to send some confidential information to Bob over a secure network. Provide encryption through Hill Cipher Method for message "Palladium Mall" and Key is "SAVE" (Consider A=1,B=2...). Also decrypt using same.

Code:

```
import numpy as np
def adjoint(matrix):
    matrix[0,0],matrix[1,1]=matrix[1,1],matrix[0,0]
    matrix[0,1]*=-1
    matrix[1,0]*=-1
    return matrix

pt=input("Please enter the plain text : ")
key=input("Please enter the key : ")

if len(pt)%2 != 0:
    pt+='x'
```

Name: Ayush Patel Enrolment 22162171038 Class B Batch 55

```
tempKeyMatrix=np.zeros((2,2), dtype=np.str_)
k=0
for i in range(2):
    for j in range(2):
        tempKeyMatrix[i,j]=key[k]
        k+=1
keyMatrix=np.matrix(tempKeyMatrix)

print('Char key matrix\n',tempKeyMatrix)

keyMatrix=np.zeros((2,2),dtype=np.int64)

for i in range(2):
    for j in range(2):
        keyMatrix[i,j]=ord(tempKeyMatrix[i,j])-96

print('Integer key matrix\n',keyMatrix)

ptList=[pt[i:i+2] for i in range(0,len(pt),2)]
ctList=[]
print()
print('Cipher')
print(ptList)
for i in ptList:
```

Name: Ayush Patel Enrolment 22162171038 Class B Batch 55

```
    # print('For',i)
    t=np.zeros((2,1),dtype=np.int64)
    t[0,0]=ord(i[0])-96
    t[1,0]=ord(i[1])-96
    cipher=np.dot(keyMatrix,t)%26
    # print(cipher)
    ctList+=[chr(cipher[0,0]+96)+chr(cipher[1,0]+96)]
    del t

del ptList
print(ctList)
print()

print('Decipher')
mod=(keyMatrix[0,0]*keyMatrix[1,1])-
(keyMatrix[1,0]*keyMatrix[0,1])
print('Determinant of key matrix',mod)

mod%=26
print('Modulus By 26 of Determinant of key matrix',mod)
kInverse=1

while (mod*kInverse)%26!=1:
    kInverse+=1
```

```
print()
print('kInverse',kInverse)
print('Adjoint of Key Matrix\n', adjoint(keyMatrix.copy()))

kInverseMatrix=((adjoint(keyMatrix.copy())%26)*kInverse)%26
print()
print('kInverseMatrix\n',kInverseMatrix)

print()
print(ctList)
ptList=[]

for i in ctList:
    # print('For',i)
    t=np.zeros((2,1),dtype=np.int64)
    t[0,0]=ord(i[0])-96
    t[1,0]=ord(i[1])-96
    decipher=np.dot(kInverseMatrix,t)%26
    # print(cipher)
    ptList+=[chr(decipher[0,0]+96)+chr(decipher[1,0]+96)]
    del t

print(ptList)
```

Name: Ayush Patel Enrolment 22162171038 Class B Batch 55

output:

```
Cipher
['pa', 'll', 'ad', 'iu', 'm ', 'ma', 'll']
['ss', 'fl', 'wp', 'jq', 'ar', 'ne', 'fl']
```

Decryption:

```
kInverseMatrix
 [[25 21]
 [20 17]]

['ss', 'fl', 'wp', 'jq', 'ar', 'ne', 'fl']
['pa', 'll', 'ad', 'iu', 'mn', 'ma', 'll']
```