DATE: 25-08-2022

LAB 01: Working with classical ciphers

NAME	VISHWAS M
SRN	PES2UG20CS390
SECTION	F

For the given questions, write a python code and attach the snapshots.

1.	For the given input, perform Caesar cipher encryption and decryption. Plain text: “CRYPTOGRAPHY” Key: 10
SOL	

```
plain_text="CRYPTOGRAPHY"
key=10
# ENCRYPTION
l=[]
for i in plain_text:
     l.append(i)
for i in range(0,len(l)):
    j=ord(l[i])
    j=j+key
    if(j>90):
        h=j-90
        j=64+h
    l[i]=chr(j)

print("AFTER ENCRYPTION:")
s=""
for i in l:
    s=s+i
print(s)
# DECRYPTION

d=[]
for i in l:
     d.append(i)
for i in range(0,len(d)):
    j=ord(d[i])
    j=j-key
    if(j<65):
        h=65-j
        j=91-h
    d[i]=chr(j)
print("AFTER DECRYPTION")
s=""
```

```
for i in d:
    s=s+i
print(s)
```

SCREENSHOT OF THE OUTPUT:

```
PS D:\vishwas\SEM 5\Applied Cryptograpgy\Lab1> python -u "d:\vishwas\SEM 5\Applied Cryptograpgy\Lab1\Caesar_Cipher.py"
AFTER ENCRYPTION:
MBIZDYQBKZRI
AFTER DECRYPTION
CRYPTOGRAPHY
PS D:\vishwas\SEM 5\Applied Cryptograpgy\Lab1>
```

2. For the plaintext given in question 1, apply Play Fair cipher encryption with key “WORK”.

SOL

```
plain_text="CRYPTOGRAPHY"
key="WORK"
l=[];m=[];A=[];x=0
for i in range(65,91):
    if i==74:
        continue
    if chr(i) not in key:
       A.append(chr(i))
for j in range(0,5):
    for i in range(0,5):
        if x >=len(key):
            y=0
            n=0
            for o in A:
                n=n+1
                for q in range(0,len(l)):
                  if o not in l[q]:
                    y=y+1
                if y==len(l):
                    m.append(o)
                    p=A.pop(n-1)
                    break
        else:
          m.append(key[x])
          x=x+1
    l.append(m)
    m=[]
pt=[]
s=''
for i in range(0,len(plain_text)):
    if i%2==0:
        if i!=0:
          pt.append(s)
```

```
            s=''
    s=s+plain_text[i]
pt.append(s)
def find(a,b):
    for i in range(0,5):
        for j in range(0,5):
         if l[i][j]==pt[a][b]:
            return i,j
ct=[]
for i in range(0,len(pt)):
    a,b=find(i,0)
    c,d=find(i,1)
    if a==c:
        if b+1>=5:
            b=b-5
        if d+1>=5:
            d=d-5
        ct.append(l[a][b+1])
        ct.append(l[c][d+1])
    elif b==d:
        if a+1>=5:
            a=a-5
        if c+1>=5:
            c=c-5
        ct.append(l[a+1][b])
        ct.append(l[c+1][d])
    else:
        ct.append(l[a][d])
        ct.append(l[c][b])
s=''
for i in ct:
    s=s+i
print("AFTER ENCRYPTION:")
print(s)
s=''
qq=[]
for i in range(0,len(ct)):
    if i%2==0:
        if i!=0:
          qq.append(s)
          s=''
    s=s+ct[i]
qq.append(s)
dt=[]
def find1(a,b):
    for i in range(0,5):
        for j in range(0,5):
         if l[i][j]==qq[a][b]:
```

```
            return i,j
for i in range(0,len(qq)):
    a,b=find1(i,0)
    c,d=find1(i,1)
    if a==c:
        if b-1<0:
            b=b+5
        if d-1<0:
            d=d+5
        dt.append(l[a][b-1])
        dt.append(l[c][d-1])
    elif b==d:
        if a-1<0:
            a=a+5
        if c-1<0:
            c=c+5
        dt.append(l[a-1][b])
        dt.append(l[c-1][d])
    else:
        dt.append(l[a][d])
        dt.append(l[c][b])
s=''
for i in dt:
    s=s+i
print("AFTER DECRYPTION:")
print(s)
```

SCREENSHOT OF THE OUTPUT: