NAME TASHFEEN LATIF

ROLL NO 17P-6035(CS-A)

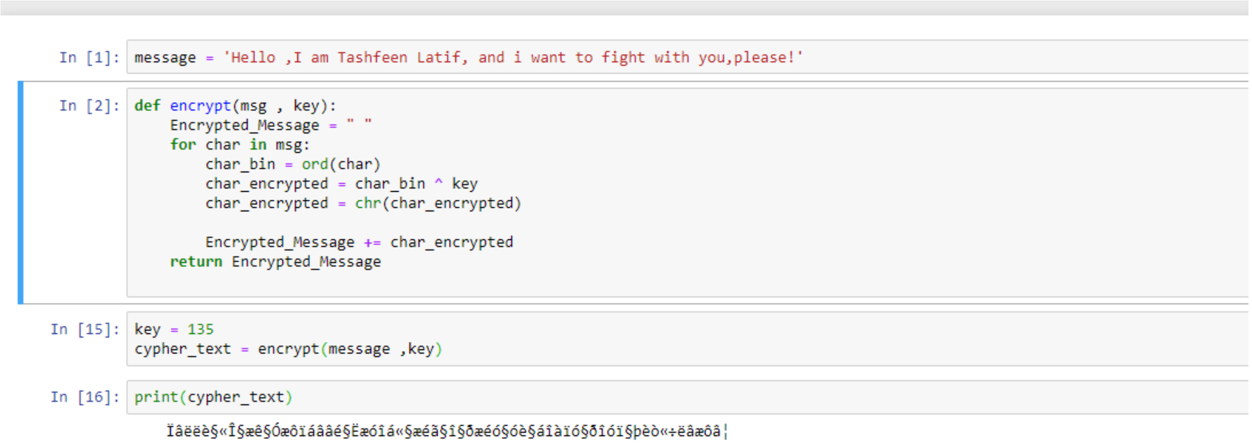
COURSE Operating System Lab

Prof Sir Usman Wajid Sahab

System Administration-:> Lab Task #1

First of all when key is symmetric I perform encryption and decryption

Encryption:



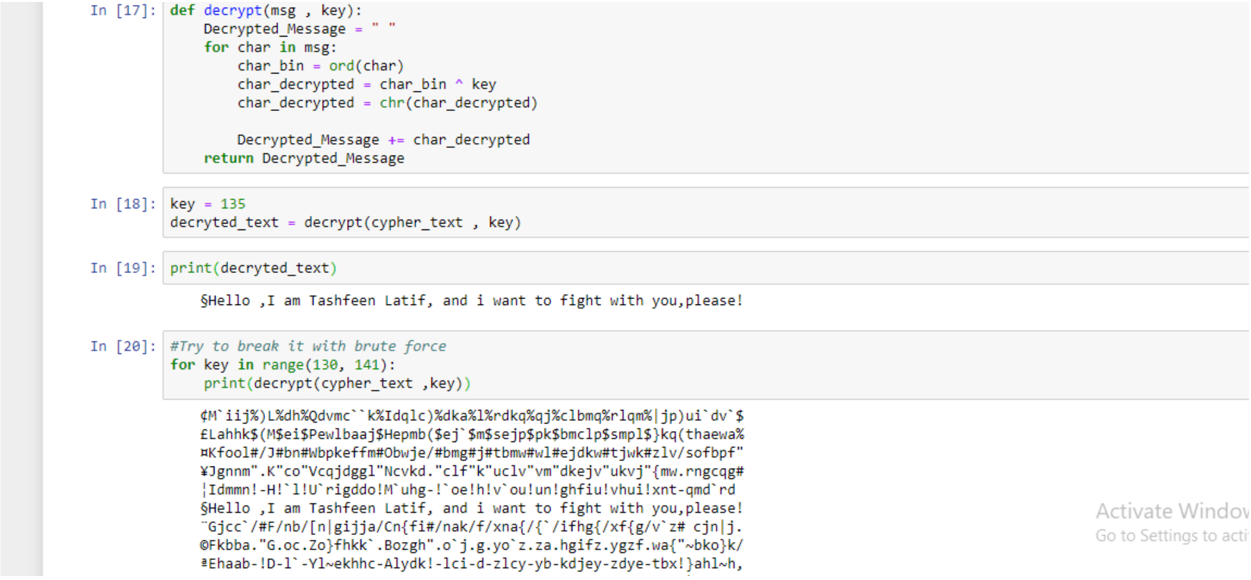
```
In [1]: message = 'Hello ,I am Tashfeen Latif, and i want to fight with you,please!'
```

```
In [2]: def encrypt(msg , key):
            Encrypted_Message = " "
            for char in msg:
                char_bin = ord(char)
                char_encrypted = char_bin ^ key
                char_encrypted = chr(char_encrypted)

                Encrypted_Message += char_encrypted
            return Encrypted_Message
```

```
In [15]: key = 135
         cypher_text = encrypt(message ,key)
```

```
In [16]: print(cypher_text)

          Ïâëëè§«Î§æê§Óæôïáââé§Ëæóîá«§æéã§î§ðæéó§óè§áîàïó§ðîóï§þèò«÷ëâæôâ¦
```

Decryption:



```
In [17]: def decrypt(msg , key):
             Decrypted_Message = " "
             for char in msg:
                 char_bin = ord(char)
                 char_decrypted = char_bin ^ key
                 char_decrypted = chr(char_decrypted)

                 Decrypted_Message += char_decrypted
             return Decrypted_Message
```

```
In [18]: key = 135
         decryted_text = decrypt(cypher_text , key)
```

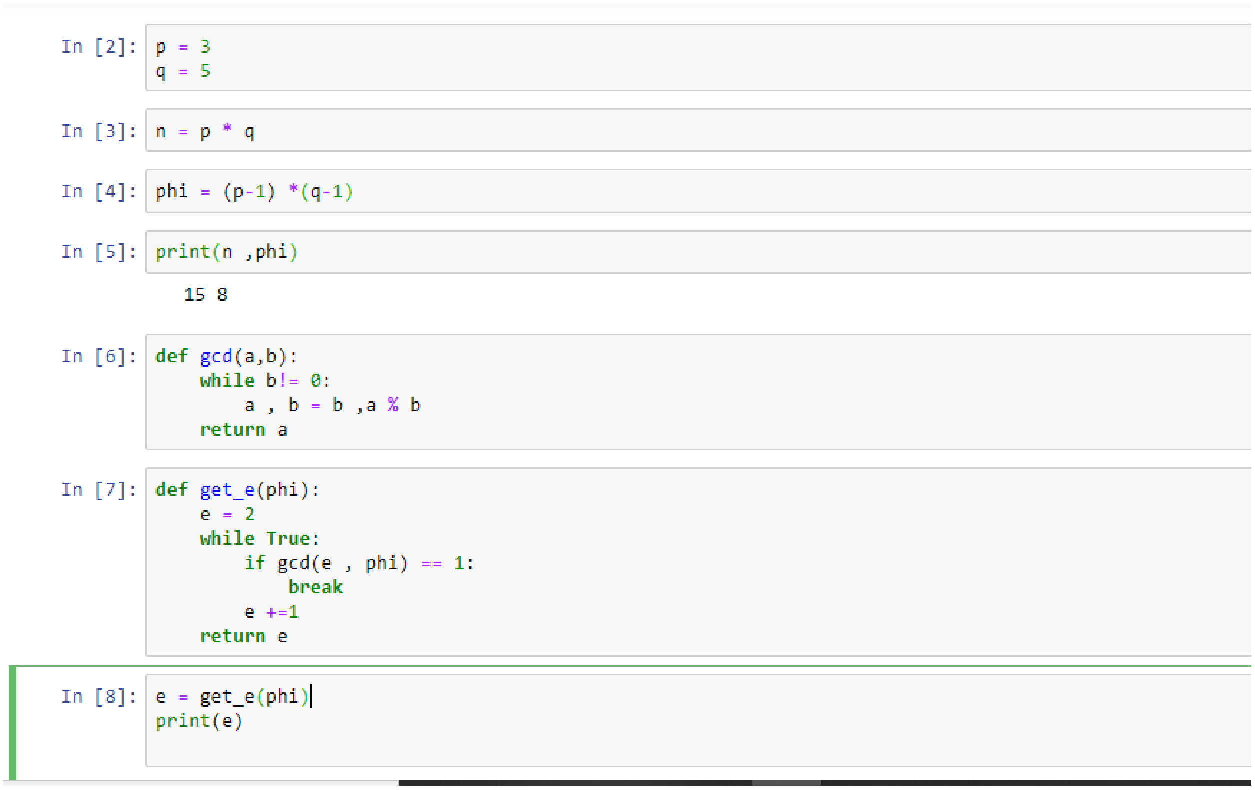
```
In [19]: print(decryted_text)

             §Hello ,I am Tashfeen Latif, and i want to fight with you,please!
```

```
In [20]: #Try to break it with brute force
         for key in range(130, 141):
             print(decrypt(cypher_text ,key))

             ¢M`iij%)L%dh%Qdvmc``k%Idqlc)%dka%l%rdkq%qj%clbmq%rlqm%|jp)ui`dv`$
             £Lahhk$(M$ei$Pewlbaaj$Hepmb($ej`$m$sejp$pk$bmclp$smpl$}kq(thaewa%
             ¤Kfool#/J#bn#Wbpkeffm#Obwje/#bmg#j#tbmw#wl#ejdkw#tjwk#zlv/sofbpf"
             ¥Jgnnm".K"co"Vcqjdggl"Ncvkd."clf"k"uclv"vm"dkejv"ukvj"{mw.rngcqg#
             ¦Idmmn!-H!`l!U`rigddo!M`uhg-!`oe!h!v`ou!un!ghfiu!vhui!xnt-qmd`rd
             §Hello ,I am Tashfeen Latif, and i want to fight with you,please!
             ¨Gjcc`/#F/nb/[n|gijja/Cn{fi#/nak/f/xna{/{`/ifhg{/xf{g/v`z# cjn|j.
             ©Fkbba."G.oc.Zo}fhkk`.Bozgh".o`j.g.yo`z.za.hgifz.ygzf.wa{"~bko}k/
             ªEhaab-!D-l`-Yl~ekhhc-Alydk!-lci-d-zlcy-yb-kdjey-zdye-tbx!}ahl~h,
```

Now its Asymmetric Key Crypto

You need to compute ‘e’ such that e is co_prime with phi

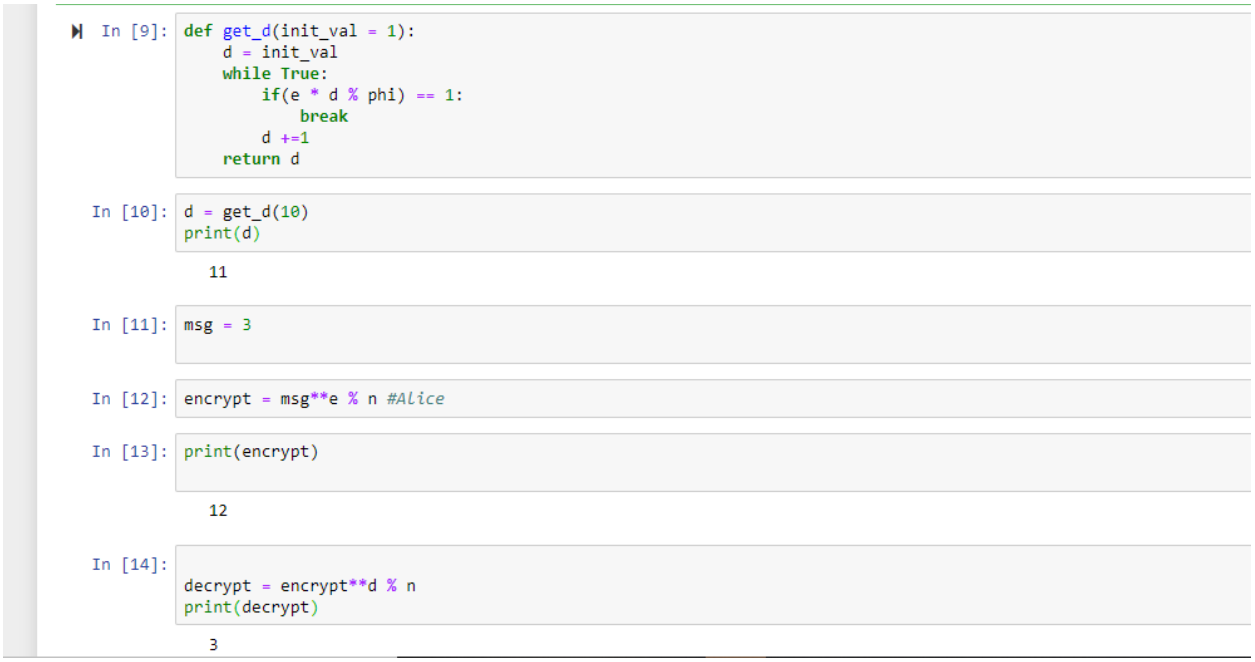
Now you can publish ‘e’ and ‘n’ public



```
In [2]: p = 3
        q = 5

In [3]: n = p * q

In [4]: phi = (p-1) *(q-1)

In [5]: print(n ,phi)

          15 8

In [6]: def gcd(a,b):
            while b!= 0:
                a , b = b ,a % b
            return a

In [7]: def get_e(phi):
            e = 2
            while True:
                if gcd(e , phi) == 1:
                    break
                e +=1
            return e

In [8]: e = get_e(phi)
        print(e)
```

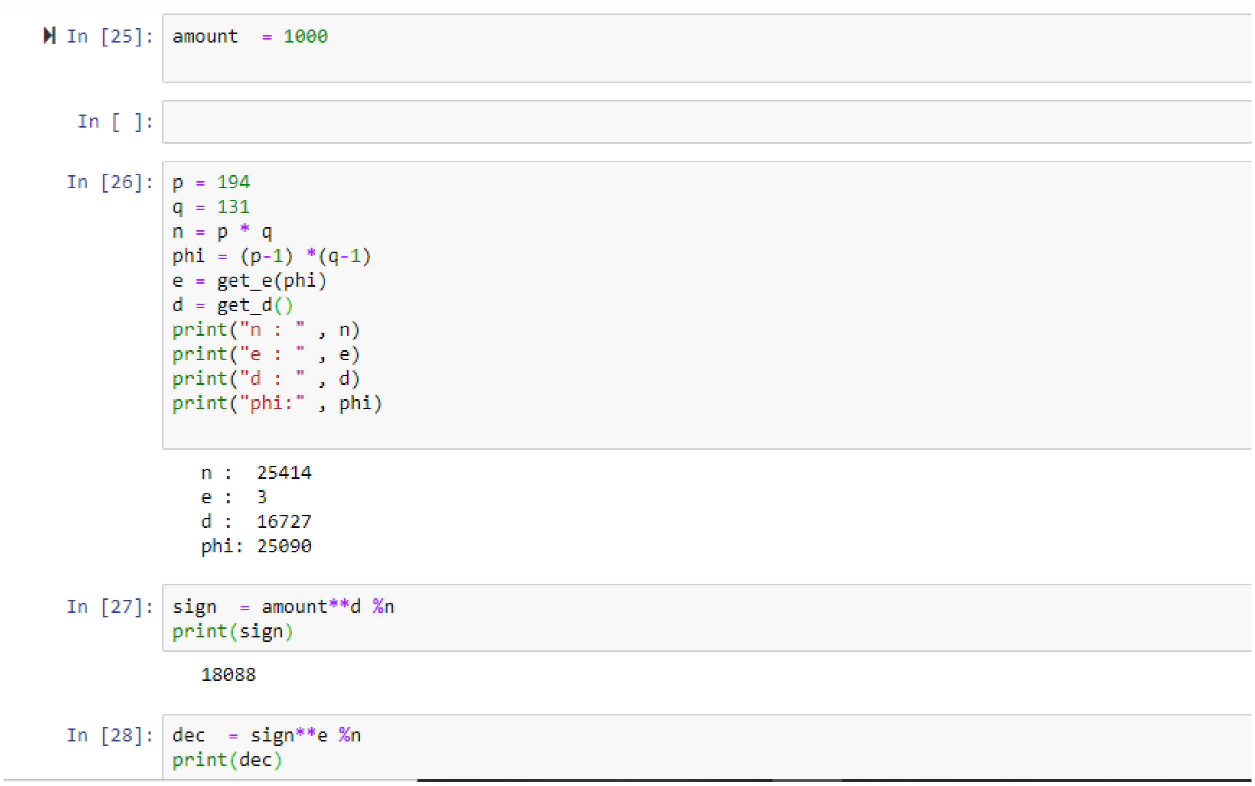
Compute d such that

e . d mod phi = 1



```
In [9]: def get_d(init_val = 1):
            d = init_val
            while True:
                if(e * d % phi) == 1:
                    break
                d +=1
            return d

In [10]: d = get_d(10)
         print(d)

           11

In [11]: msg = 3

In [12]: encrypt = msg**e % n #Alice

In [13]: print(encrypt)

           12

In [14]:
         decrypt = encrypt**d % n
         print(decrypt)

           3
```

Now according to tell you that I just written this message so I sign it now



```
In [25]: amount  = 1000
```

```
In [ ]:
```

```
In [26]: p = 194
         q = 131
         n = p * q
         phi = (p-1) *(q-1)
         e = get_e(phi)
         d = get_d()
         print("n : " , n)
         print("e : " , e)
         print("d : " , d)
         print("phi:" , phi)
```

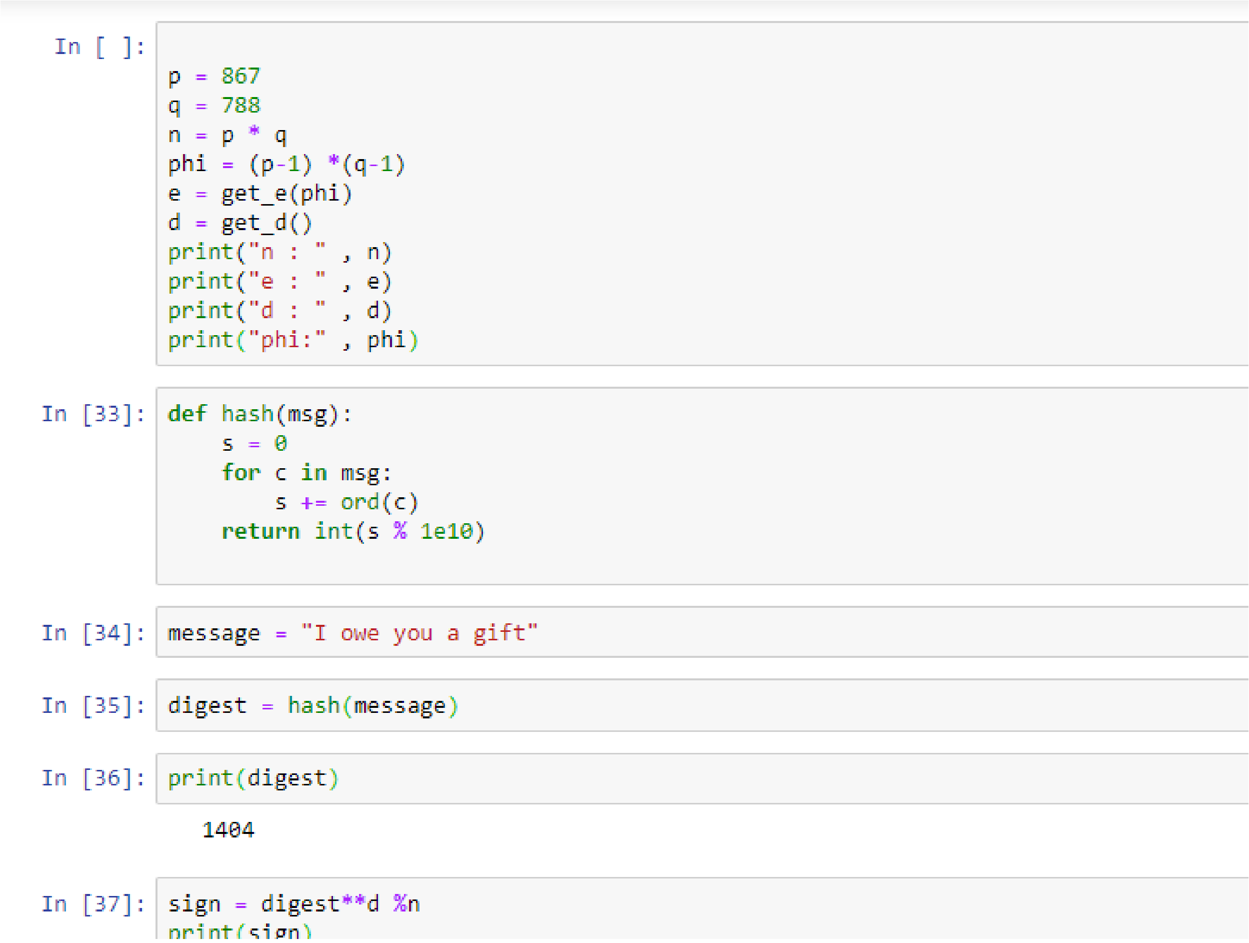
```
n :  25414
e :  3
d :  16727
phi: 25090
```

```
In [27]: sign  = amount**d %n
         print(sign)
```

```
18088
```

```
In [28]: dec  = sign**e %n
         print(dec)
```

Final Piece



In [ ]:

```

p = 867
q = 788
n = p * q
phi = (p-1) *(q-1)
e = get_e(phi)
d = get_d()
print("n : " , n)
print("e : " , e)
print("d : " , d)
print("phi:" , phi)
```

In [33]:

```
def hash(msg):
    s = 0
    for c in msg:
        s += ord(c)
    return int(s % 1e10)
```

In [34]:

```
message = "I owe you a gift"
```

In [35]:

```
digest = hash(message)
```

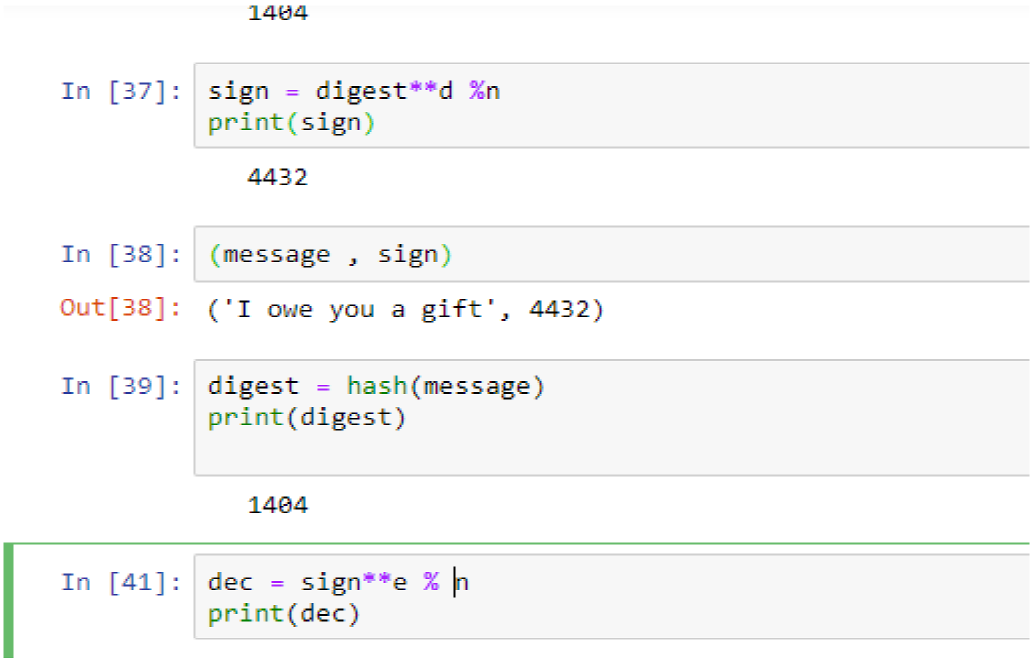
In [36]:

```
print(digest)
```

```
1404
```

In [37]:

```
sign = digest**d %n
print(sign)
```



```
1404
```

In [37]:

```
sign = digest**d %n
print(sign)
```

```
4432
```

In [38]:

```
(message , sign)
```

Out[38]:

```
('I owe you a gift', 4432)
```

In [39]:

```
digest = hash(message)
print(digest)
```

```
1404
```

In [41]:

```
dec = sign**e % n
print(dec)
```