ANJUMAN-I-ISLAM'S KALSEKAR TECHNICAL CAMPUS

School of Engineering & Technology

Affiliated to : University of Mumbai, Recognised by : DTE (Maharashtra) & Approved by : AICTE (New Delhi)

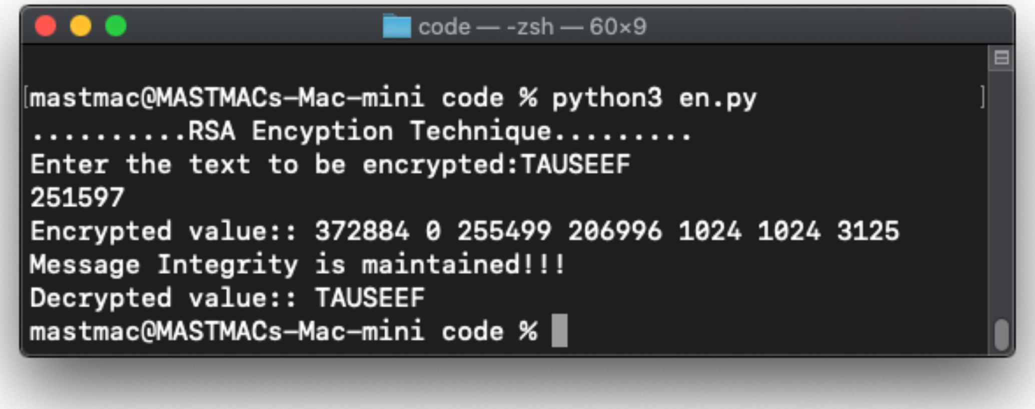
Course Code : CSL604	**Course Name : System Security Lab**
Class : TE-CO	**Batch : Computer Engineering**
Roll no : 18CO63	**Name : SHAIKH TAUSEEF MUSHTAQUE ALI**

Experiment : 03
Aim : Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA.

Code :

```
import hashlib
import random
import math
print("..........RSA Encyption Technique.........")
pt=input("Enter the text to be encrypted:")
code = hashlib.sha1(pt.encode())
code = code.hexdigest()
plain = pt.replace(" ","")
if plain.isalpha():
    pta=pt.lower()
    ptn=[ord(i)%97 for i in pta]
elif pt.isdigit():
    ptn=int(pt)

#n=int(input("Enter a composite prime number(n)"))
primes = []
for x in range(1,1001):
            for y in range(2,x):
                        if x%y==0:
                                    break
            else:
                        primes.append(x)

p, q = random.choice(primes), random.choice(primes)
phi=(p-1)*(q-1)
n = p * q
e= 0
for i in range(2,26):
    if math.gcd(i,phi)==1:
        e=i
        break
def modInverse(a,m):
    for x in range(1, m):
        if (((a%m) * (x%m)) % m == 1):
            return x
    return -1
d = modInverse(e,phi)
print(d)
if d!= -1:
    if plain.isalpha():
        ct= [(i**e)%n for i in ptn]
        print("Encrypted value::",*ct)
        dt= [(i**d)%n for i in ct]
    else:
        ct = (ptn**e) % n
        dt = (ct**d) % n
else:
    print("Encryption is not Possible!!!!!!!!")

if plain.isalpha() and pt.islower():
    dt = "".join([chr(int(i)+97) for i in dt]).replace("\x81"," ")
elif plain.isalpha() and pt.isupper():
    dt = "".join([chr(65+int(i)) for i in dt]).replace("a"," ")
else:
    dt= str(dt)

hashvalue = hashlib.sha1(dt.encode())
hashvalue = hashvalue.hexdigest()
if code==hashvalue:
    print("Message Integrity is maintained!!!")
    print("Decrypted value::",dt)
else:
    print("Corrupted message!!")
```

Output:



```
mastmac@MASTMACs-Mac-mini code % python3 en.py
..........RSA Encyption Technique.........
Enter the text to be encrypted:TAUSEEF
251597
Encrypted value:: 372884 0 255499 206996 1024 1024 3125
Message Integrity is maintained!!!
Decrypted value:: TAUSEEF
mastmac@MASTMACs-Mac-mini code %
```

Conclusion:

Implemented and analyzed RSA cryptosystem and Digital signature scheme using RSA.