Practical 1

Blockchain Technology

2CSDE93

Dhruv Sonani

20BCE527

Date

August 30, 2022

NIRMA
UNIVERSITY
INSTITUTE OF TECHNOLOGY
NAAC ACCREDITED 'A' GRADE

Department of Computer Science and Engineering
Institute of Technology

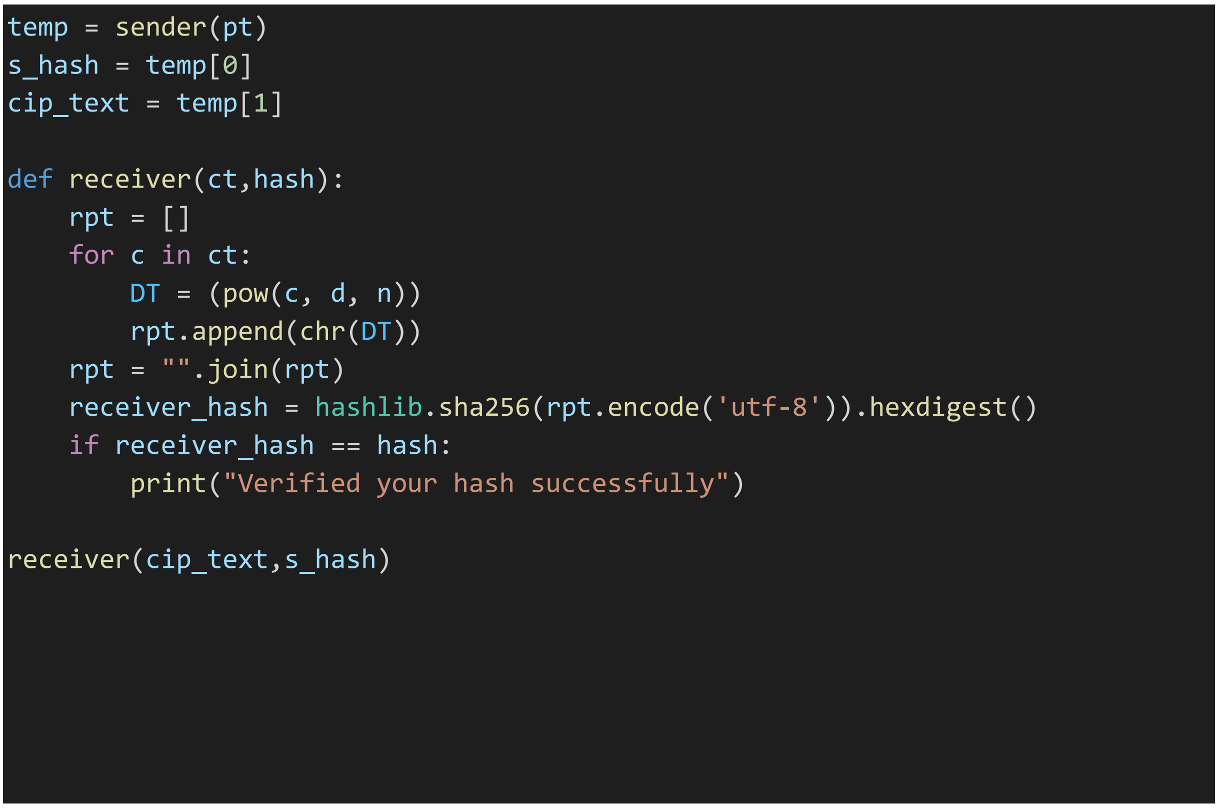
Nirma University

Ahmedabad

Aim: To implement digital signature to sign and verify authenticated user. Also, show a message when tampering is detected.

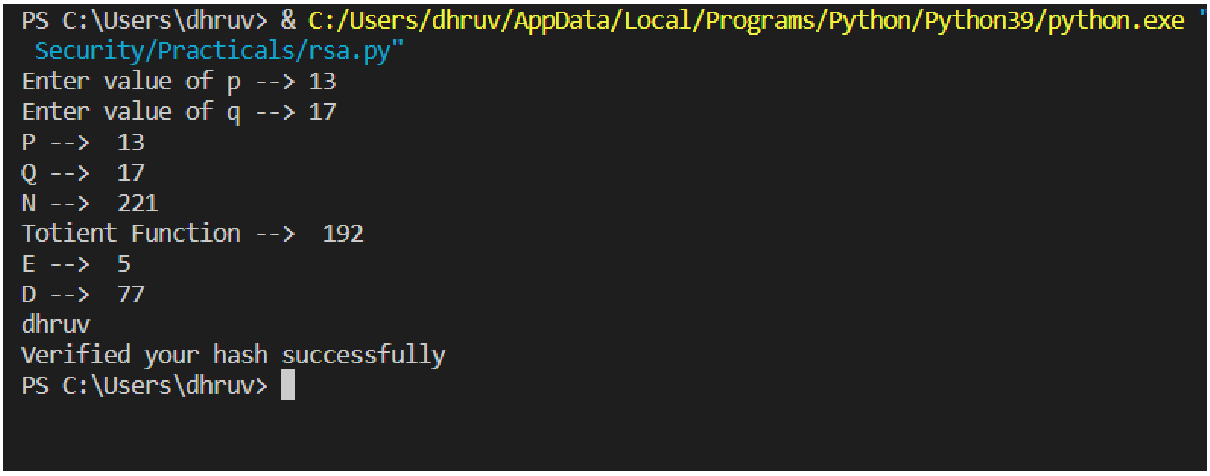
Code: (Python3)

```
import hashlib

def gcd(a,b):
    if(a==0):
        return b
    return gcd(b%a,a)
p =int(input("Enter value of p --> "))
q =int(input("Enter value of q --> "))
print("P --> ",p)
print("Q --> ",q)
n = p*q
print("N --> ",n)
TF = ((p-1)*(q-1))
print("Totient Function --> ",TF)
for i in range(2,TF):
    if(gcd(i,TF)==1):
        e=i
        break
print("E --> ",e)

for k in range(2,TF):
    if((k*e % TF)==(1 % TF )):
        d = k
print("D --> ",d)

pt = input()

ct = []

def sender(pt):
    plaintext = list(pt)
    sender_hash = hashlib.sha256(pt.encode('utf-8')).hexdigest()
    for i in range(len(plaintext)):
        asc = ord(plaintext[i])
        ct.append(pow(asc, e, n))
    return [sender_hash,ct]
```

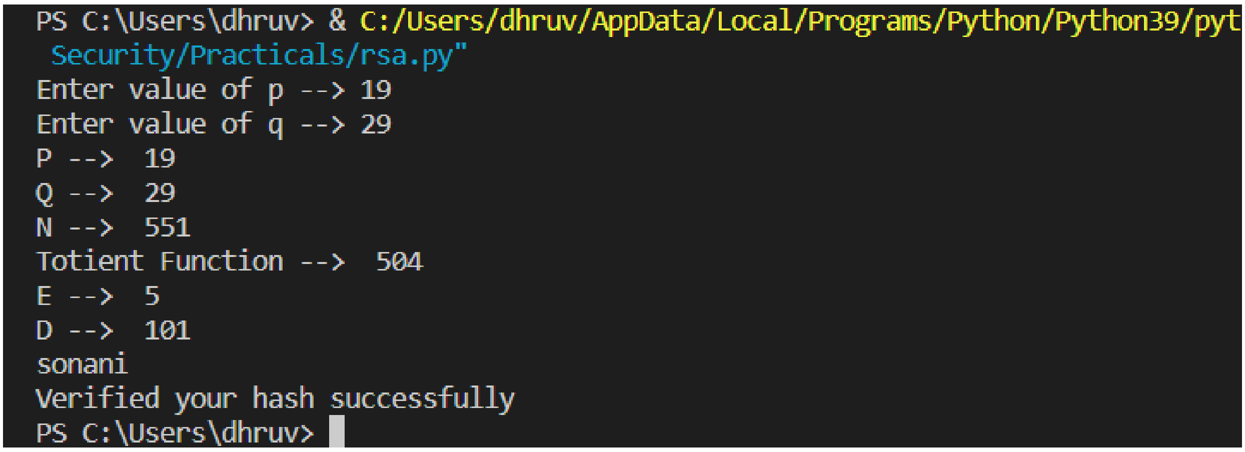


```
temp = sender(pt)
s_hash = temp[0]
cip_text = temp[1]

def receiver(ct,hash):
    rpt = []
    for c in ct:
        DT = (pow(c, d, n))
        rpt.append(chr(DT))
    rpt = "".join(rpt)
    receiver_hash = hashlib.sha256(rpt.encode('utf-8')).hexdigest()
    if receiver_hash == hash:
        print("Verified your hash successfully")

receiver(cip_text,s_hash)
```

Output:



```
PS C:\Users\dhruv> & C:/Users/dhruv/AppData/Local/Programs/Python/Python39/python.exe "
 Security/Practicals/rsa.py"
Enter value of p --> 13
Enter value of q --> 17
P -->  13
Q -->  17
N -->  221
Totient Function -->  192
E -->  5
D -->  77
dhruv
Verified your hash successfully
PS C:\Users\dhruv> 
```



```
PS C:\Users\dhruv> & C:/Users/dhruv/AppData/Local/Programs/Python/Python39/pyt
 Security/Practicals/rsa.py"
Enter value of p --> 19
Enter value of q --> 29
P -->  19
Q -->  29
N -->  551
Totient Function -->  504
E -->  5
D -->  101
sonani
Verified your hash successfully
PS C:\Users\dhruv> 
```