Consider a scenario where in a company two employee wants to authenticate them self as legitimate entity. Provide a solution for authentication of two parties through digital signature use DSS

CODE:

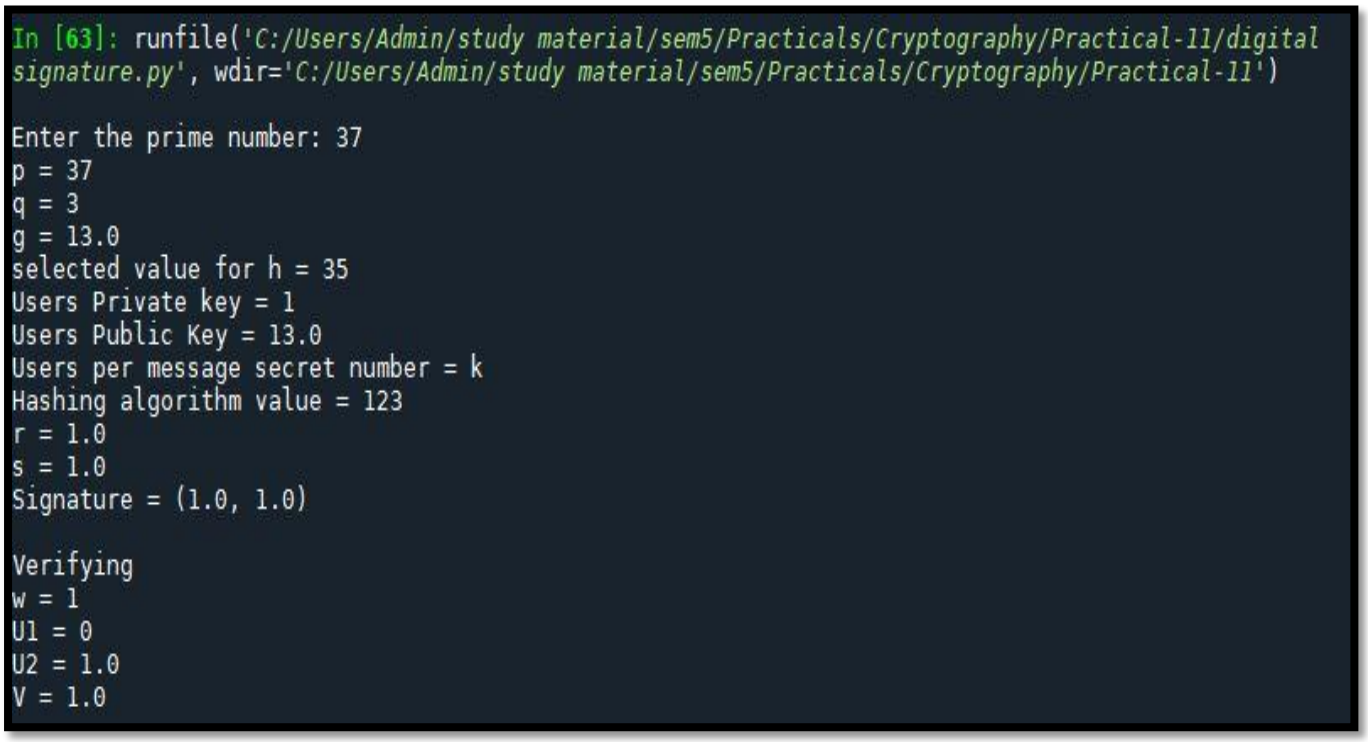
```
import random
def check_prime(num):
    if num > 1:
        for i in range(2, num):
            if (num % i) == 0:
                return 0
                break
        else:
            return 1
    else:
        return 0

def modInverse(a, m) :
    a = a % m;
    for x in range(1, m) :
        if ((a * x) % m == 1) :
            return x
    return 1

hash_value=123
p=int(input('Enter the prime number: '))
for i in range(1, p):
    if (p-1)%i==0:
```

```
        if check_prime(i)==1:
            q=i
            break
        else:
            continue

a=(p-1)//q
for i in range(2, p):
    if (i**a)%p >1:
        h=i
        g=(i*(p-1))/q
        g=g%p

x=random.randint(1, q-1)
y=g**x
y=y%p
k=random.randint(1, q-1)

r=((g**k)%p)%q
k_in=modInverse(k, q)
s=((k_in*hash_value)+(x*r))%q


w=modInverse(s, q)
u1=(hash_value*w)%q
u2=(r*w)%q
v=(((g**u1)*(y**u2))%p)%q
```

```
print(f'p = {p}\nq = {q}\ng = {g}\nselected value for h = {h}\nUsers Private key = {x}\nUsers Public Key = {y}')

print(f'Users per message secret number = k')

print(f'Hashing algorithm value = {hash_value}')

print(f'r = {r}\ns = {s}')

print(f'Signature = ({r}, {s})')

print(f'\nVerifying')

print(f'w = {w}\nU1 = {u1}\nU2 = {u2}\nV = {v}')
```

OUTPUT:

Hash value: 123



```
In [60]: runfile('C:/Users/Admin/study material/sem5/Practicals/Cryptography/Practical-11/digital
signature.py', wdir='C:/Users/Admin/study material/sem5/Practicals/Cryptography/Practical-11')

Enter the prime number: 11
p = 11
q = 5
g = 7.0
selected value for h = 9
Users Private key = 2
Users Public Key = 5.0
Users per message secret number = k
Hashing algorithm value = 123
r = 0.0
s = 4.0
Signature = (0.0, 4.0)

Verifying
w = 4
U1 = 2
U2 = 0.0
V = 0.0
```

Hash value: 1234

```
In [65]: runfile('C:/Users/Admin/study material/sem5/Practicals/Cryptography/Practical-11/digital
signature.py', wdir='C:/Users/Admin/study material/sem5/Practicals/Cryptography/Practical-11')

Enter the prime number: 13
p = 13
q = 3
g = 5.0
selected value for h = 11
Users Private key = 1
Users Public Key = 5.0
Users per message secret number = k
Hashing algorithm value = 1234
r = 2.0
s = 0.0
Signature = (2.0, 0.0)

Verifying
w = 1
U1 = 1
U2 = 2.0
V = 2.0
```

Tejas Tripathi

```
In [66]: runfile('C:/Users/Admin/study material/sem5/Practicals/Cryptography/Practical-11/digital
signature.py', wdir='C:/Users/Admin/study material/sem5/Practicals/Cryptography/Practical-11')

Enter the prime number: 19
p = 19
q = 3
g = 7.0
selected value for h = 17
Users Private key = 2
Users Public Key = 11.0
Users per message secret number = k
Hashing algorithm value = 1234
r = 2.0
s = 0.0
Signature = (2.0, 0.0)

Verifying
w = 1
U1 = 1
U2 = 2.0
V = 2.0

In [67]:
```