Experiment 7

DIGITAL SIGNATURE ALGORITHM

7.1 Aim

To implement a program executing Digital Signature Algorithm.

8.2 Algorithm

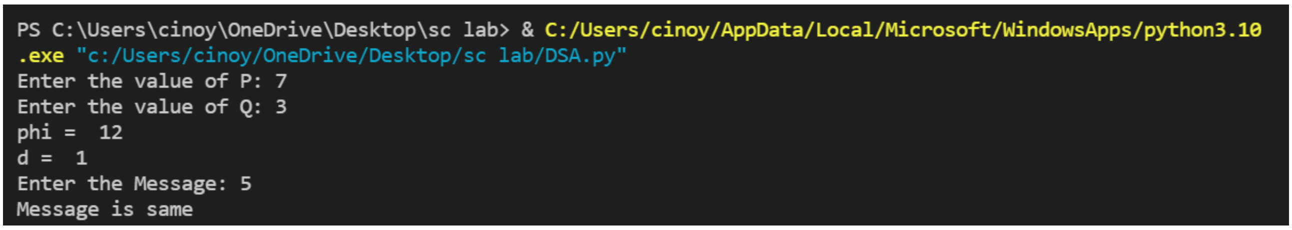
- **Key generation**
  1. Choose a prime number q, which is called the prime divisor.
  2. Choose another primer number p, such that p-1 mod q = 0. p is called the prime modulus in this.
  3. choose an integer g, such that 1 < g < p, g^q mod p = 1 and g = $h^{((p-1)/q)}$ mod p.
  4. Choose an integer, such that 0 < x < q for this
  5. Compute y as g^x mod p.
  6. K is user's secret key, pseudo random integer with 0 < k <q.
- **Signing**
  1. Compute r = (g^k mod p) mod q.
  2. S = [k^{-1} (H (M) + xr] mod q.
- **Sign verification**
  1. Compute w = (s^{-1}) mod q.
  2. Compute u1 = [H (m) w] mod q
  3. Compute u2 = (r w) mod q.
  4. Compute v = [(g^u1 g^u2) mod p] mod q
  5. TEST that if v = r

7.3 Program

```
import math

def gcd(a,h):
    while(1):
        temp = a % h
        if(temp==0):
            return h
        a,h = h,temp
```

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




def main():
    p = int(input(”Enter the value of P: ”))
    q = int(input(”Enter the value of Q: ”))

    n = p*q
    e = 13
    phi = (p-1)*(q-1)
    print(”phi = ”,phi)
    while(e < phi):
        if(gcd(e,phi)==1):
            break
        else:
            e+=1
    d = modInverse(e,phi)
    print(”d = ”,d)

    M = int(input(”Enter the Message: ”))

    S = pow(M,d)
    S = math.fmod(S,n)
    M1 = pow(S,e)
    M1 = math.fmod(M1,n)
    if(M==M1):
        print(”Message is same”)
    else:
        print(”Message is Not same”)

main()
```

7.4 Output



```
PS C:\Users\cinoy\OneDrive\Desktop\sc lab> & C:/Users/cinoy/AppData/Local/Microsoft/WindowsApps/python3.10
.exe "c:/Users/cinoy/OneDrive/Desktop/sc lab/DSA.py"
Enter the value of P: 7
Enter the value of Q: 3
phi =  12
d =  1
Enter the Message: 5
Message is same
```

Figure 1: Digital signature

7.5 Result

Implemented the program for Digital Signature Algorithm successfully.