Experiment Number: 2

Aim:

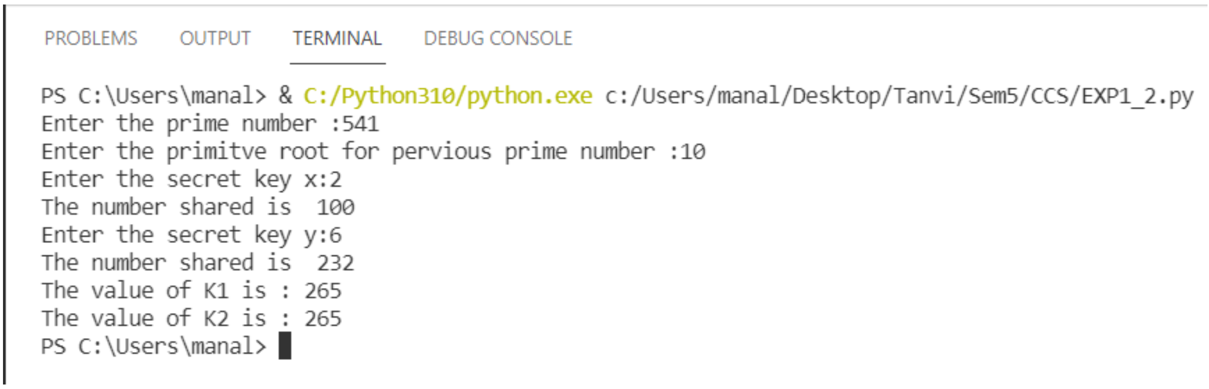
2) Implement Diffie Hellman key exchange algorithm in Scilab/C/Python/R.

For this experiment I have implemented the Diffie Hellman key exchange algorithm in Python

Program:

```
#implementation of Diffie Hellman key exchange algorithm
#function to calculate
def cal(a,b,P):
    if (b == 1):
        return a
    else:
        return ((pow(a, b)) % P)
P = int(input("Enter the prime number :"))
G = int(input("Enter the primitve root for pervious prime number :"))
e=0
if(G>=P):
    print("G can't be greater than P")
    e=1
if(e==0):
    x = int(input("Enter the secret key x:"))
    a = cal(G, x, P)
    print("The number shared is ",a)
    y = int(input("Enter the secret key y:"))
    b = cal(G, y, P)
    print("The number shared is ",b)
    #a and b are exchanged and the following values are calculated
    k1 = cal(b, x, P)
    k2 = cal(a, y, P)
    print("The value of K1 is :", k1)
    print("The value of K2 is :", k2)
```

Output:



```
PS C:\Users\manal> & C:/Python310/python.exe c:/Users/manal/Desktop/Tanvi/Sem5/CCS/EXP1_2.py
Enter the prime number :541
Enter the primitve root for pervious prime number :10
Enter the secret key x:2
The number shared is  100
Enter the secret key y:6
The number shared is  232
The value of K1 is : 265
The value of K2 is : 265
PS C:\Users\manal> █
```

Conclusion:

In this experiment I have implemented the Diffie Hellman key exchange algorithm. By using this algorithm 2 sides can decide on a secret symmetric key over a public channel. In this method even if the communication is overheard the symmetric keys aren't revealed. This is beneficial even in case of active man in the middle attack. This is the most effective way to define encryption keys security wise. If the key is known to everyone then the encrypted text can be decrypted by the eavesdropper, hence if we make use of such algorithm we can define a symmetric key without actually sharing it. But if we don't select the prime numbers properly then we are increasing the risk of revealing the key.

Github link: https://github.com/tanvipen/DiffieHellman.git