

Exp No: 5

Roll.No: 210701314

Date:

Diffie Hellman Key Exchange

Aim:

To implement Diffie Hellman Key Exchange technique for the user input key.

Algorithm:

Step 1: Get the prime number from the user and verify whether it is a prime number.

Step 2: Get the primitive root for the prime number and verify it with primitive_checker() function.

Step 3: Get the Private key of User 1 and User 2 from the user

Step 4: Generate the public key for the User 1 and User 2 using the user given inputs

Step 5: Generate the Secret Key for User 1 and User 2 using Public and Private keys of both users

Step 6: Exchange the keys if both users Secret keys are same and print Successful.

Program:

```
def prime_checker(p):
    if p < 1:
        return -1
    elif p > 1:
        if p == 2:
            return 1
        for i in range(2, p):
            if p % i == 0:
                return -1
        return 1

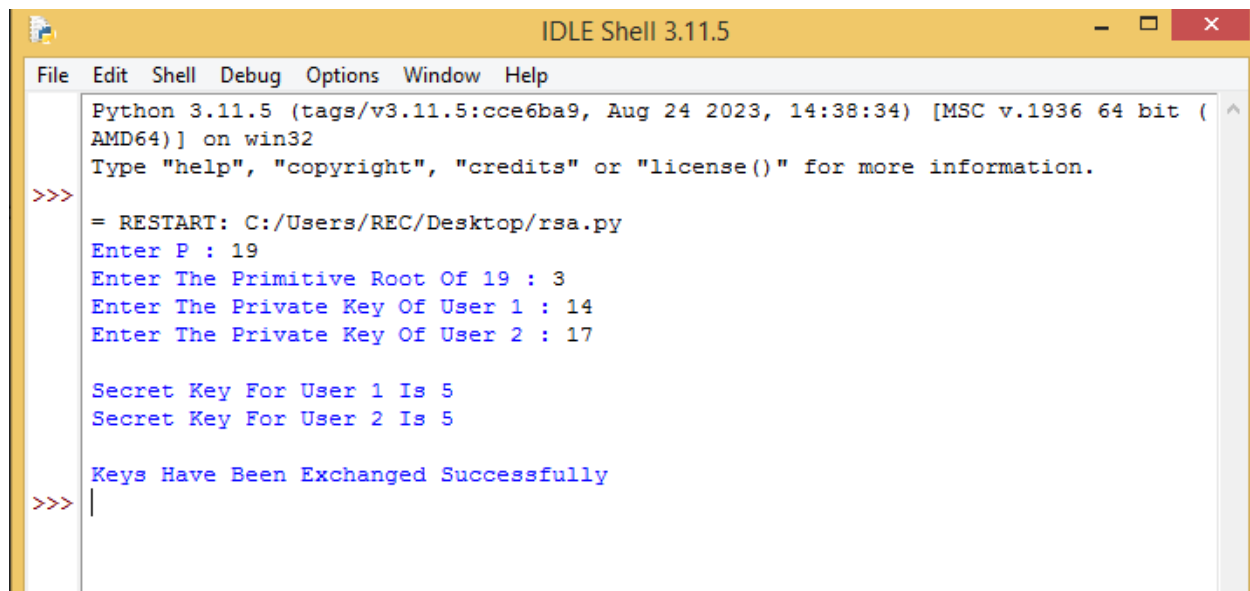
def primitive_check(g, p, L):
    for i in range(1, p):
        L.append(pow(g, i) % p)
```

```
for i in range(1, p):
    if L.count(i) > 1:
        L.clear()
        return -1
return 1
```

```
l = []
while 1:
    P = int(input("Enter P : "))
    if prime_checker(P) == -1:
        print("Number Is Not Prime, Please Enter Again!")
        continue
    break
```

```
while 1:
    G = int(input(f"Enter The Primitive Root Of {P} : "))
    if primitive_check(G, P, l) == -1:
        print(f"Number Is Not A Primitive Root Of {P}, Please Try Again!")
        continue
    break
x1, x2 = int(input("Enter The Private Key Of User 1 : ")), int(
input("Enter The Private Key Of User 2 : "))
while 1:
    if x1 >= P or x2 >= P:
        print(f"Private Key Of Both The Users Should Be Less Than {P}!")
        continue
    break
y1, y2 = pow(G, x1) % P, pow(G, x2) % P
k1, k2 = pow(y2, x1) % P, pow(y1, x2) % P
print(f"\nSecret Key For User 1 Is {k1} \nSecret Key For User 2 Is {k2} \n")
if k1 == k2:
    print("Keys Have Been Exchanged Successfully")
else:
    print("Keys Have Not Been Exchanged Successfully")
```

Output:



```
Python 3.11.5 (tags/v3.11.5:cce6ba9, Aug 24 2023, 14:38:34) [MSC v.1936 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:/Users/REC/Desktop/rsa.py
Enter P : 19
Enter The Primitive Root Of 19 : 3
Enter The Private Key Of User 1 : 14
Enter The Private Key Of User 2 : 17

Secret Key For User 1 Is 5
Secret Key For User 2 Is 5

Keys Have Been Exchanged Successfully
>>> |
```

Result:

Thus the Diffie Hellman Key Exchange technique implemented successfully.