EX NO: 5 **REGISTER NO:210701509**

DATE:

DIFFIE HELLMAN KEY EXCHANGE

AIM:

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

ALGORITHM:

- Get the prime number from the user and verify whether it is a prime number.
- Get the primitive root for the prime number and verify it with primitive_checker() function.
- Get the Private key of User 1 and User 2 from the user
- Generate the public key for the User 1 and User 2 using the user given inputs
- Generate the Secret Key for User 1 and User 2 using Public and Private keys of both users
- Exchange the keys if both users Secret keys are same and print Successful.

PROGRAM CODE:

```
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:

```
Enter P : 23
Enter The Primitive Root Of 23 : 5
Enter The Private Key Of User 1 : 12
Enter The Private Key Of User 2 : 19

Secret Key For User 1 Is 16
Secret Key For User 2 Is 16

Keys Have Been Exchanged Successfully
```

RESULT: