**LAB 7**

**OBJECTIVE**

To implement Diffie-Hellman key exchange algorithm

**THEORY**

Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography.

Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

**CODE**

# Python program to implement Diffie-Hellman key exchange

import random

def is\_prime(n):

count = 0

for i in range(1, int(n/2)+1):

if (n % i == 0):

count += 1

if (count == 1):

return True

else:

return False

while(True):

p = int(input("Enter a prime number : "))

if (is\_prime(p)):

break

g = int(input("Enter the primitive root of prime number : "))

Pr\_A = random.randint(1,p)

print("\nPrivate key of A : {}".format(Pr\_A))

Pr\_B = random.randint(1,p)

print("Private key of B : {}".format(Pr\_B))

Pu\_A = (g\*\*Pr\_A) % p

print("\nPublic key of A : {}".format(Pu\_A))

Pu\_B = (g\*\*Pr\_B) % p

print("Public key of B : {}".format(Pu\_B))

Se\_A = (Pu\_B\*\*Pr\_A) % p

Se\_B = (Pu\_A\*\*Pr\_B) % p

if(Se\_A==Se\_B):

print("\nThe shared secret is : {}".format(Se\_A))

**OUTPUT**

Enter a prime number : 353

Enter the primitive root of prime number : 3

Private key of A : 331

Private key of B : 300

Public key of A : 108

Public key of B : 83

The shared secret is : 44

**CONCLUSION**

In this lab, we got familiar with Diffie-Hellman key exchange algorithm and implemented it using python programming language. Also, we tested our program for different prime and primitive root pairs.