**EXPERIMENT-8**

Write a program to implement Diffie Hellman Key Exchange algorithm.

**Program:**

print("Specify the Value of MOD Prime - Q : ")

q = int(input())

print("Specify the Value of Primitive Root - A : ")

a = int(input())

print("Specify the Private Key of Sender - RS : ")

rs = int(input())

print("Specify the Private Key of Receiver - RR : ")

rr = int(input())

us = (a \*\* rs) % q

ur = (a \*\* rr) % q

print("Public Key of Sender - US : ", us)

print("Public Key of Receiver - UR : ", ur)

print("Sharing of Public Keys among Sender and Receiver !")

ks = (ur \*\* rs) % q

kr = (us \*\* rr) % q

print("Secret Key computed by Sender - KS : ", ks)

print("Secret Key computed by Receiver - KR : ", kr)

ktest = (a \*\* (rs \* rr)) % q

print("Checking the Value of Computed Secret Key by both Sender and Receiver - KTEST : ", ktest)

**Output:**

Specify the Value of MOD Prime - Q : 17

Specify the Value of Primitive Root - A : 3

Specify the Private Key of Sender - RS : 7

Specify the Private Key of Receiver - RR : 15

Public Key of Sender - US : 11

Public Key of Receiver - UR : 6

Sharing of Public Keys among Sender and Receiver !

Secret Key computed by Sender - KS : 14

Secret Key computed by Receiver - KR : 14

Checking the Value of Computed Secret Key by both Sender and Receiver - KTEST : 14