Ex.No: 6 **DIFFIE-HELLMAN KEY EXCHANGE**

Date: **ALGORITHM**

Aim:

To implement Diffie-Hellman Key Exchange Algorithm.

Algorithm:

1) Start the program
2) Get the q and alpha values from the users
3) Prompt the user to enter the Alice's Secret Key and Bob's Secret Key
4) Compute the YA and YB values using functions
5) After computing the private keys, find the common sessions

Program:

```
def bob(YA,XB,q):
    return YA**XB%q
def alice(YB,XA,q):
    return YB**XA%q
def main():
    q= int(input("Enter the prime number(q): "))
    alpha = int(input("Enter the primitive root (alpha): "))
    XA = int(input("Enter Alice Secret Key(XA): "))
    XB= int(input("Enter Bob secret Key:(XB) "))
    YA = alpha**XA%q
    YB= alpha**XB%q
    print("Bob Public Key :(KAB)", bob(YA,XB,q))
```

```
        print("Alice Public Key (KAB): ", alice(YB,XA,q))
main()
```

Output:

```
==================== RESTART: C:\Users\New\Desktop\diffie.py ==================
Enter the prime number(q): 353
Enter the primitive root (alpha): 3
Enter Alice Secret Key(XA): 97
Enter Bob secret Key:(XB) 233
Bob Public Key :(KAB) 160
Alice Public Key (KAB):  160
>>>
```

Result:

Thus, Diffie-Hellman algorithm has been implemented and verified successfully.