NAME: SAKSHI VEER

ROLL NO: 4101066

BATCH: BA2

**Problem Statement:** **To implement a Diffie-Hellman Key Exchange algorithm.**

**CODE:**

#Diffie Hellman Key Exchange Alogorithm

# Begin

sharedPrime = int(input("Enter shared Prime(n):"))

sharedBase = int(input("Enter shared Base(g):"))

aliceSecret = int(input("Enter Alice Secret Key(x):"))

bobSecret = int(input("Enter Bob Secret Key(y):"))

print( "Publicly Shared Variables:")

print( " Publicly Shared Prime: " , sharedPrime )

print( " Publicly Shared Base: " , sharedBase )

# Alice Sends Bob A = g^x mod n

A = (sharedBase\*\*aliceSecret) % sharedPrime

print( "\n Alice Sends(A) Over Public Chanel: " , A )

# Bob Sends Alice B = g^y mod n

B = (sharedBase \*\* bobSecret) % sharedPrime

print("Bob Sends(B) Over Public Chanel: ", B )

print( "\n------------\n" )

print( "Privately Calculated Shared Secret:" )

# Alice Computes Shared Secret: K1 = B^x mod n

aliceSharedSecret = (B \*\* aliceSecret) % sharedPrime

print( " Alice Shared Secret: ", aliceSharedSecret )

# Bob Computes Shared Secret: K2 = A^y mod n

bobSharedSecret = (A\*\*bobSecret) % sharedPrime

print( " Bob Shared Secret: ", bobSharedSecret )

**OUTPUT:**

C:\Users\saksh\OneDrive\Desktop\college\LP3\ICS\3>python dh.py

Enter shared Prime(n):23

Enter shared Base(g):9

Enter Alice Secret Key(x):4

Enter Bob Secret Key(y):3

Publicly Shared Variables:

Publicly Shared Prime: 23

Publicly Shared Base: 9

Alice Sends(A) Over Public Chanel: 6

Bob Sends(B) Over Public Chanel: 16

------------

Privately Calculated Shared Secret:

Alice Shared Secret: 9

Bob Shared Secret: 9

C:\Users\saksh\OneDrive\Desktop\college\LP3\ICS\3>