NAME : PAREENITA A.SHIRSATH PRN : 221101062 ROLL.NO : 57 T.E.A.I.&.D.S.

**CSS EXPERIMENT NO : 3**

**CODE:**

# Diffie-Hellman Code

# Power function to return value of a^b mod P

def power(a, b, p):

if b == 1:

return a

else:

return pow(a, b) % p

# Main function

def main():

# Both persons agree upon the public keys G and P

# A prime number P is taken

P = 23

print("The value of P:", P)

# A primitive root for P, G is taken

G = 9

print("The value of G:", G)

# Alice chooses the private key a

# a is the chosen private key

a = 4

print("The private key a for Alice:", a)

# Gets the generated key

x = power(G, a, P)

# Bob chooses the private key b

# b is the chosen private key

b = 3

print("The private key b for Bob:", b)

# Gets the generated key

y = power(G, b, P)

# Generating the secret key after the exchange of keys

ka = power(y, a, P) # Secret key for Alice

kb = power(x, b, P) # Secret key for Bob

print("Secret key for Alice is:", ka)

print("Secret key for Bob is:", kb)

if \_\_name\_\_ == "\_\_main\_\_":

main()

**OUTPUT :**

