**ASSIGNMENT NO: 8**

**NAME: Viraj Patil**

**PRN : 21510097**

**Q - Implement the Diffie-Hellman Key Exchange algorithm for a given problem.**

def power(a, b, P):

if b == 1:

return a

else:

return pow(a, b, P)

def main():

P = int(input("Enter the prime number P: ")) # 23

print(f"The value of Prime Value : {P}")

G = int(input("Enter the primitive root G: ")) # 9

print(f"The value of Primitive Root : {G}")

a = int(input("Enter the private key a for Alice: ")) # 4

print(f"The private key a for Alice : {a}")

x = power(G, a, P)

b = int(input("Enter the private key b for Bob: ")) # 3

print(f"The private key b for Bob : {b}")

y = power(G, b, P)

ka = power(y, a, P)

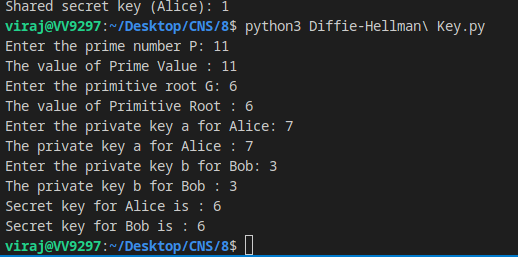
kb = power(x, b, P)

print(f"Secret key for Alice is : {ka}")

print(f"Secret key for Bob is : {kb}")

main()

**OUTPUT :**

****