**SYSTEM SECURITY**

**LAB 9**

**Diffie-Hellman Key Exchange algorithm**

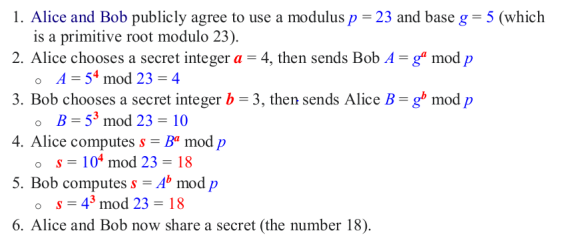
**P.R.N:** 20190802058

**Name:** Krushal Milan Shah

**Aim:**

Write a program to implement the Diffie-Hellman Key Exchange algorithm.

**Steps:**



**Code:**

#Taking prime number

p = int(input("Prime number 1 (P): "))

g = int(input("Prime number 2 (G): "))

#Private key of Pratik and Krushal

Krushal\_Private\_key = int(input("\nKrushal Private key: "))

Pratik\_Private\_key = int(input("Pratik Private key: "))

#Generating Pubic Values

Krushal\_Public\_key = p\*\*Krushal\_Private\_key % g

Pratik\_Public\_key = p\*\*Pratik\_Private\_key % g

#print("\nKrushal Public key: " , Krushal\_Public\_key , "\nPratik Public key: " , Pratik\_Public\_key)

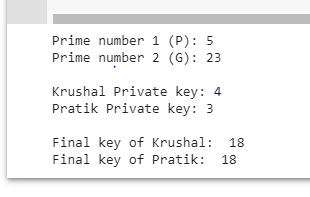
#generating final key3

Krushal = Pratik\_Public\_key\*\*Krushal\_Private\_key % g

Pratik = Krushal\_Public\_key\*\*Pratik\_Private\_key % g

print("\nFinal key of Krushal: " , Krushal,"\nFinal key of Pratik: ",Pratik)

**Results:**

****

**Conclusion:**

Successfully implemented Diffie-Hellman Key Exchange algorithm.