In [1]:

*# Implementation of Diffie-Hellman key exchange*

In [5]:

*# P = 23*  
*# G = 9*  
*# a = 2*  
*# b = 3*  
p = int(input("Enter Value of P"))  
g = int(input("Enter Value of G"))  
  
a = int(input("Enter Secret key for User A"))  
b = int(input("Enter Secret key for User B"))  
  
pa = int(pow(g, a, p))  
pb = int(pow(g, b, p))  
  
print("Public Key A : ", pa)  
print("Public Key B : ", pb)  
  
print("Private Key A : ", a)  
print("Private Key B : ", b)  
  
Sb = int(pow(pa, b, p))  
Sa = int(pow(pb, a, p))  
  
print("Shared Key A : ", Sa)  
print("Shared Key B : ", Sb)

Public Key A : 12  
Public Key B : 16  
Private Key A : 2  
Private Key B : 3  
Shared Key A : 3  
Shared Key B : 3

In [ ]: