**Final Year B.Tech. (CSE) – II [ 2022-23 ]**

**Cryptograpy and Network Security Lab**

**PRN: 2019BTECS00015**

**Full name: Shraddha Sanjay Kharat**

**Batch: B1**

**Assignment No. 11**

**Title:**

Diffie-Hellman Key Exchange

**Aim:**

To Demonstrate Diffie-Hellman Key Exchange

**Theory:**

Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.

**Code:**

from random import randint

*# P = 941*

*# G = 627*

P = int(input("Enter a prime number P: "))

G = int(input("Enter a primitive root for P: "))

*# a = 347*

a = int(input("Enter a private key for A: "))

x = int(pow(G, a, P))

*# b = 781*

b = int(input("Enter a private key for B: "))

y = int(pow(G, b, P))

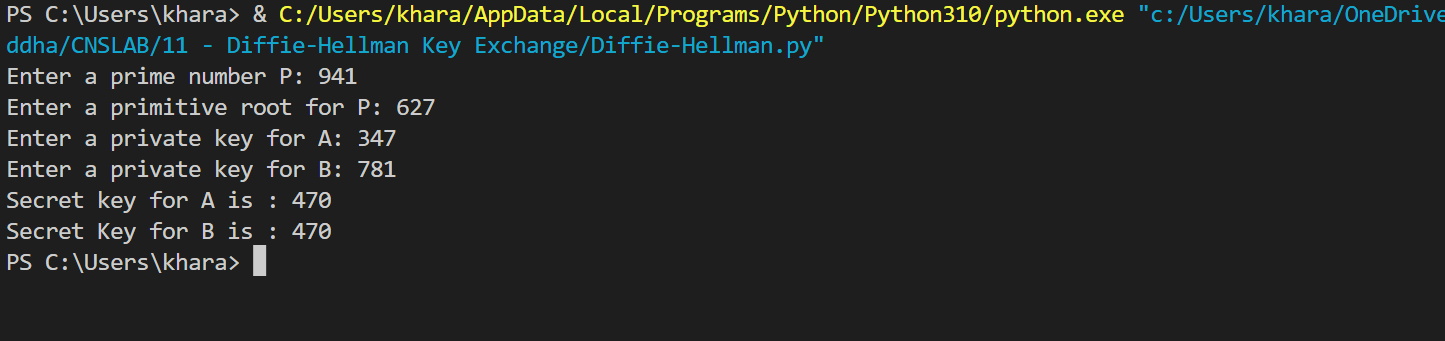
ka = int(pow(y, a, P))

kb = int(pow(x, b, P))

print('Secret key for A is : %d' % (ka))

print('Secret Key for B is : %d' % (kb))

**Output:**

****

**Conclusion:**

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.