**EXPERIMENT NO -15**

**OBJECTIVE-**Write a program to implement Diffie-Hellman key exchange Algorithm to exchange the symmetric key and show the encryption & decryption.

**SOURCE CODE-**

|  |
| --- |
| **from random import randint**    **if \_\_name\_\_ == '\_\_main\_\_':**    **# Both the persons will be agreed upon the**  **# public keys G and P**  **# A prime number P is taken**  **P = 23**    **# A primitve root for P, G is taken**  **G = 9**      **print('The Value of P is :%d'%(P))**  **print('The Value of G is :%d'%(G))**    **# Alice will choose the private key a**  **a = 4**  **print('The Private Key a for Alice is :%d'%(a))**    **# gets the generated key**  **x = int(pow(G,a,P))**    **# Bob will choose the private key b**  **b = 3**  **print('The Private Key b for Bob is :%d'%(b))**    **# gets the generated key**  **y = int(pow(G,b,P))**      **# Secret key for Alice**  **ka = int(pow(y,a,P))**    **# Secret key for Bob**  **kb = int(pow(x,b,P))**    **print('Secret key for the Alice is : %d'%(ka))**  **print('Secret Key for the Bob is : %d'%(kb))** |

**Output:**

The value of P : 23

The value of G : 9

The private key a for Alice : 4

The private key b for Bob : 3

Secret key for the Alice is : 9

Secret Key for the Bob is : 9

**Developed by:** Abhishek Pandey