|  |  |
| --- | --- |
| Name: | Prerna Sunil Jadhav |
| Sap Id: | 60004220127 |
| Class: | T. Y. B. Tech (Computer Engineering) |
| Course: | Information Security Laboratory |
| Course Code: | DJ19CEL603 |
| Experiment No.: | 06 |

**AIM:** Study and Implement Diffie Hellman Key Exchange Algorithm.

**CODE:**

from random import randint

P = 17

Q = 3

print('The Value of P is :%d'%(P))

print('The Value of Q is :%d'%(Q))

# 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(Q,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(Q,b,P))

# Secret key for Alice

Alice\_key = int(pow(y,a,P))

# Secret key for Bob

Bob\_key = int(pow(x,b,P))

print('Secret key for the Alice is : %d'%(Alice\_key))

print('Secret Key for the Bob is : %d'%(Bob\_key))

**OUTPUT:**

