Shri Vile Parle Kelavani Mandal's

DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING

(Autonomous College Affiliated to the University of Mumbai)

NAAC Accredited with "A" Grade (CGPA : 3.18)

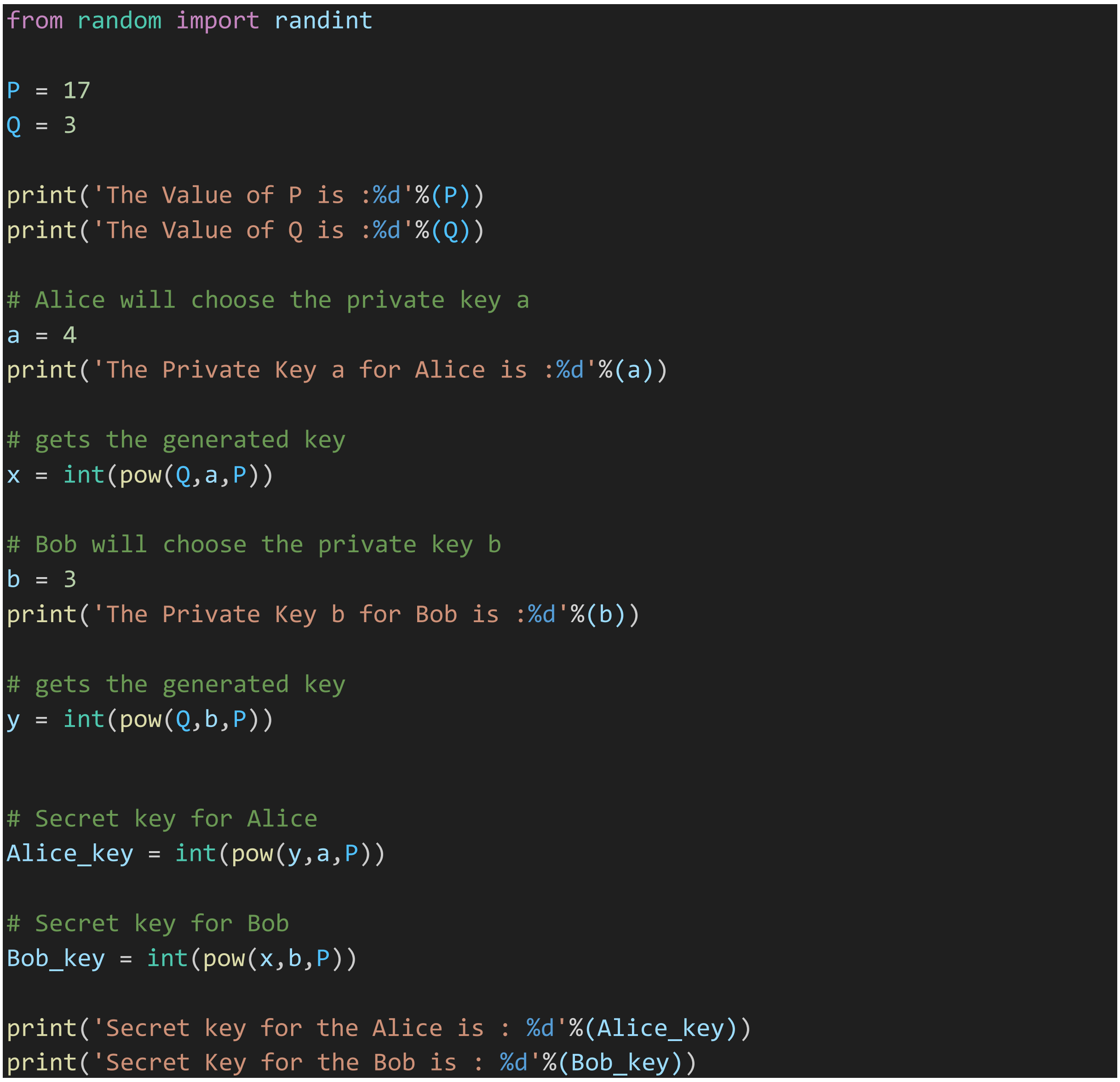
Academic Year: 2022-2023

EXPERIMENT 6

Shashwat Shah
TYBtech Comps B
C22
60004220126

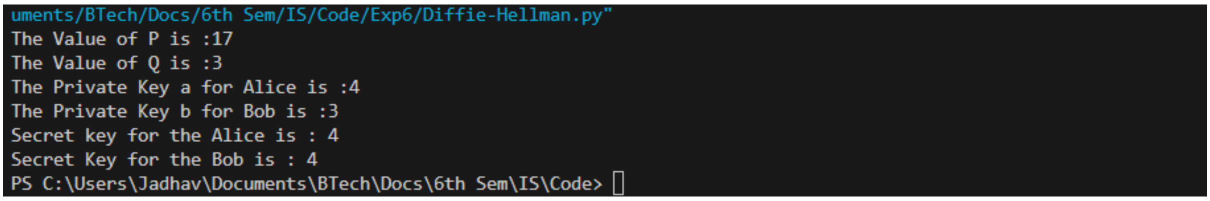
AIM: Study and Implement Diffie Hellman Key Exchange Algorithm.

CODE:



```python
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:



```
uments/BTech/Docs/6th Sem/IS/Code/Exp6/Diffie-Hellman.py"
The Value of P is :17
The Value of Q is :3
The Private Key a for Alice is :4
The Private Key b for Bob is :3
Secret key for the Alice is : 4
Secret Key for the Bob is : 4
PS C:\Users\Jadhav\Documents\BTech\Docs\6th Sem\IS\Code> 
```