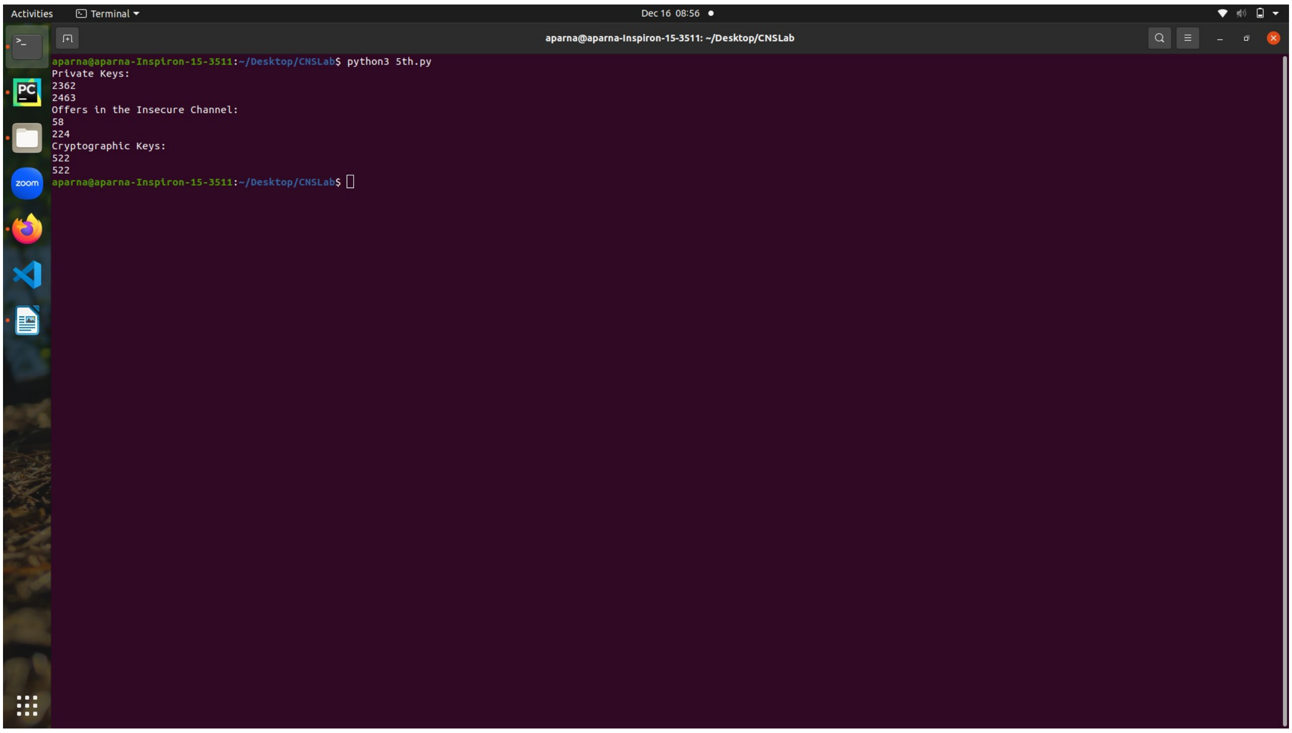
```
"""
Name : Aparna Shivhari Bhavwat
PRN : 1941004
Aim : Demonstrate how Diffie-Hellman key exchange works
with Man-In-The-Middle attack.
"""
import random
class Party:
    def __init__(self, name):
        self.name = name
        self.priv_key = random.randint(500, 4000)
    def computeOffer(pers, g, p):
        return (g ** pers.priv_key) % p
    def computeKey(pers, offer, p):
        K = (offer ** pers.priv_key) % p
        return K
if __name__ == "__main__":
    pub_g = random.randint(10, 100)
    pub_p = random.randint(500, 900)
    party_a = Party("Party A")
    party_b = Party("Party B")
    print("Private Keys: ")
    print(party_a.priv_key)
    print(party_b.priv_key)
    A = party_a.computeOffer(pub_g, pub_p)
    B = party_b.computeOffer(pub_g, pub_p)
    print("Offers in the Insecure Channel: ")
    print(A)
    print(B)
    print("Cryptographic Keys:")
    print(party_a.computeKey(B, pub_p))
    print(party_b.computeKey(A, pub_p))
```

Ouput:



```
aparna@aparna-Inspiron-15-3511:~/Desktop/CNSLab$ python3 5th.py
Private Keys:
2362
2463
Offers in the Insecure Channel:
58
224
Cryptographic Keys:
522
522
aparna@aparna-Inspiron-15-3511:~/Desktop/CNSLab$ 
```