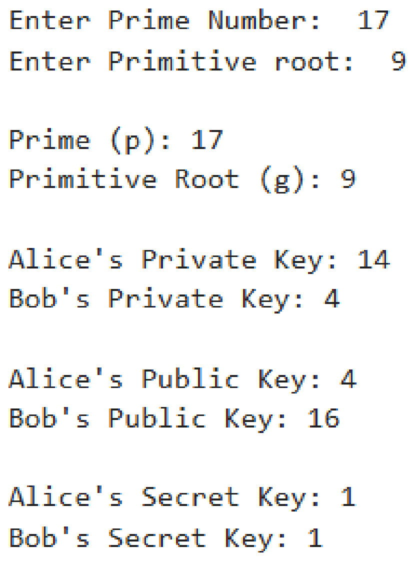
Name: Gaurang Vaghela
Rollno: TEAD-22561
Mini Project Lab
Practical 2
Problem Statement: Implementation of Diffie-Hellman key Exchange (DH)

Code:

```
import random
from sympy import isprime

p = int(input("Enter Prime Number: "))
g = int(input("Enter Primitive root: "))

# Step 2: Choose private keys
private_key_A = random.randint(2, p)  # Alice's private key
private_key_B = random.randint(2, p)  # Bob's private key

# Step 3: Compute public keys
public_key_A = pow(g, private_key_A, p)  # A = g^a mod p
public_key_B = pow(g, private_key_B, p)  # B = g^b mod p

# Step 4: Compute secret keys
secret_A = pow(public_key_B, private_key_A, p)  # S = B^a mod p
secret_B = pow(public_key_A, private_key_B, p)  # S = A^b mod p

# Output results
print(f"\nPrime (p): {p}")
print(f"Primitive Root (g): {g}\n")
print(f"Alice's Private Key: {private_key_A}")
print(f"Bob's Private Key: {private_key_B}\n")
print(f"Alice's Public Key: {public_key_A}")
print(f"Bob's Public Key: {public_key_B}\n")
print(f"Alice's Secret Key: {secret_A}")
print(f"Bob's Secret Key: {secret_B}")
```

Output:



```
Enter Prime Number:  17
Enter Primitive root:  9

Prime (p): 17
Primitive Root (g): 9

Alice's Private Key: 14
Bob's Private Key: 4

Alice's Public Key: 4
Bob's Public Key: 16

Alice's Secret Key: 1
Bob's Secret Key: 1
```