**CSS EXPERIMENT 3**

def diffie\_hellman\_key\_exchange(g, p, x, y):

    # Calculate R1 = g^x (mod p)

    R1 = pow(g, x, p)

    # Calculate R2 = g^y (mod p)

    R2 = pow(g, y, p)

    # Alice sends R1 to Bob

    # Bob sends R2 to Alice

    # Calculate K = (R2)^x (mod p) for Alice

    K\_Alice = pow(R2, x, p)

    # Calculate K = (R1)^y (mod p) for Bob

    K\_Bob = pow(R1, y, p)

    return R1, R2, K\_Alice, K\_Bob

# Get user input

g = int(input("Enter the generator 'g': "))

p = int(input("Enter the prime number 'p': "))

x = int(input("Enter the private key 'x' for Alice: "))

y = int(input("Enter the private key 'y' for Bob: "))

# Perform Diffie-Hellman key exchange

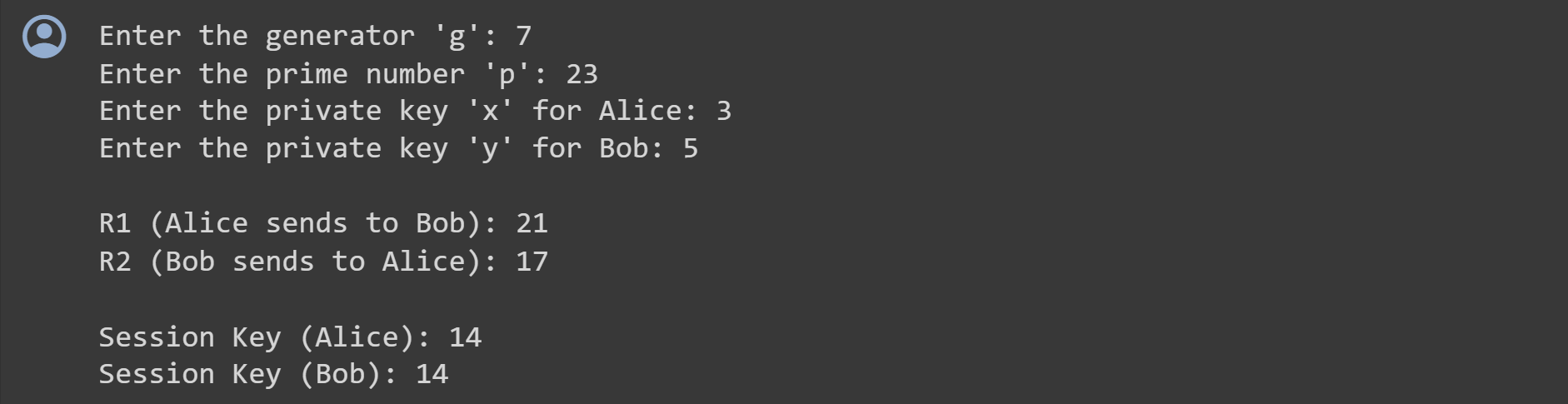
R1, R2, session\_key\_Alice, session\_key\_Bob = diffie\_hellman\_key\_exchange(g, p, x, y)

print("\nR1 (Alice sends to Bob):", R1)

print("R2 (Bob sends to Alice):", R2)

print("\nSession Key (Alice):", session\_key\_Alice)

print("Session Key (Bob):", session\_key\_Bob)

****