**Name : Aarya Tiwari**

**Batch : B2:**

**Roll No. : 16010421119**

**Course: INS**

**Experiment No. : 6**

**Code:**

def calculate\_generator(p):

    for g in range(2, p):

        if pow(g, p - 1, p) == 1:

            return g

def diffie\_hellman\_key\_exchange(p, g, a, RB):

    RA = pow(g, a, p)

    KAB = pow(RB, a, p)

    return RA, KAB

def xor\_encrypt(message, key):

    encrypted\_message = ""

    for i in range(len(message)):

        encrypted\_char = chr(ord(message[i]) ^ key)

        encrypted\_message += encrypted\_char

    return encrypted\_message

def calculate\_modular\_exponentiation(q, a, p):

    a\_star = pow(q, a, p)

    return a\_star

def xor\_decrypt(encrypted\_message, key):

    decrypted\_message = ""

    for i in range(len(encrypted\_message)):

        decrypted\_char = chr(ord(encrypted\_message[i]) ^ key)

        decrypted\_message += decrypted\_char

    return decrypted\_message

def diffie\_hellman():

    prime = 7237

    generator = calculate\_generator(prime)

*#Alice and Bob's private keys are known only to them*

    alice\_private\_key = 5356

    bob\_private\_key = 1813

*#Alice and Bob's public keys are calculated using their private keys*

    alice\_public\_key = calculate\_modular\_exponentiation(generator, alice\_private\_key, prime)

    print("Alice's public key:", alice\_public\_key)

    bob\_public\_key = calculate\_modular\_exponentiation(generator, bob\_private\_key, prime)

    print("Bob's public key:", bob\_public\_key)

*# Calculate shared secrets*

    alice\_shared\_secret = calculate\_modular\_exponentiation(bob\_public\_key, alice\_private\_key, prime)

    bob\_shared\_secret = calculate\_modular\_exponentiation(alice\_public\_key, bob\_private\_key, prime)

    return alice\_shared\_secret, bob\_shared\_secret

alice\_shared\_secret, bob\_shared\_secret = diffie\_hellman()

print("Alice's shared secret:", alice\_shared\_secret)

print("Bob's shared secret:", bob\_shared\_secret)

*# Message to be sent from Alice to Bob*

message = "Hey bro my name is Aarya"

*# Encrypt the message using XOR encryption and Alice's shared secret*

encrypted\_message = xor\_encrypt(message, alice\_shared\_secret)

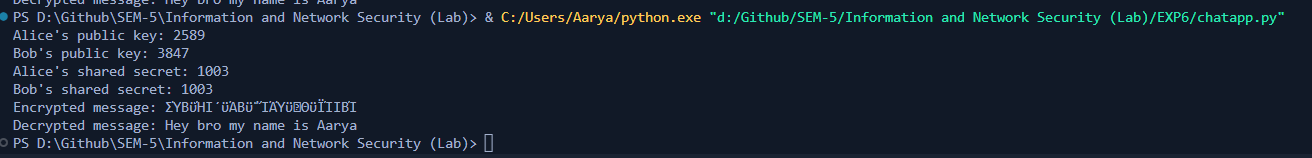
print("Encrypted message:", encrypted\_message)

*# Decrypt the message using XOR decryption and Bob's shared secret*

decrypted\_message = xor\_decrypt(encrypted\_message, bob\_shared\_secret)

print("Decrypted message:", decrypted\_message)

**Output:**

****

**Outcomes:**

**Conclusion:**