Name:-Amrit Ranjan

Reg No:-21BCE1847

Cryptography And Network Security

Assignment 7

Faculty Name:-Dr Tapabarta Roy

Man In the Middle Attack



Ques: Perform a man in the middle attack for diffie helmann key exchange, selecting suitable parameters for the two communicating parties and the eavesdropper.

Writing the Code in Python Language

Code:-

Runn in the dedicated terminal

// order

Eve->alice->bob

Eve Code:-

import socket

s = socket.socket()

port = 12345

s.bind(('', port))

s.listen(5)

print("Server is listening, waiting for Alice and Bob")

c1, addr1 = s.accept()  #Alice

print("ALice is connected")

c2, addr2 = s.accept() #Bob

print("Bob is connected")

p = 29 #prime number

a = 2  #primitive root

                                            #2.Selecting false key for Bob and sending

ya = int(c1.recv(1024).decode())

#Xd1 is the private key of the hacker

xd1 = int(input("Enter false key for Bob:"))

yd1 = pow(a, xd1, p)  #public key to be sent to Bob

print(f"Public key for Bob: {yd1}")

c2.send(str(yd1).encode())

print("Sent public key Bob")

#receive the public key of Bob .... done after all the work at Bob's end

yb = int(c2.recv(1024).decode())

                                            #5. Selecting the public key to be sent to the Alice

#Xd2 is used to calculate the public key for Alice

xd2 = int(input("Enter false key for Alice:"))

yd2 = pow(a, xd2, p)

print(f"Public key for Alice: {yd2}")

                                            #6. Calculate the secret key of Bob and Alice

#Secret key of Bob

kbob = pow(yb,xd1,29) # same as k1 calculated at Bob's end

print(f"Key of Bob calculated by Hacker(Darth):{kbob}")

#Secret key of ALice

kalice = pow(ya,xd2,29) #same as k2 calculated at Alice's end

print(f"Key of Alice calculated by Hacker(Darth):{kalice}")

c1.send(str(yd2).encode()) #Sent to the Alice

print("Sent public key for Alice to client 2")

c1.close()

c2.close()

s.close()

Alice Code:-

import socket

port = 12345

client\_socket = socket.socket()

client\_socket.connect(('localhost', port))

                                            # 1. Calculating the public key of Alice and send

#As per the algorithm it would be the first step  getting Alices public key and sending to Bob which would be intruded by Darth

xa = int(input("Enter the private key for ALice:"))

ya = pow(2,xa,29) #Public key of Alice

client\_socket.send(str(ya).encode())

yd2 = int(client\_socket.recv(1024).decode()) #received the public key decided by Darth

print("Received public key for Alice:", yd2)

                                            #7. Calculate the secret key sent by Bob which does not match with Bob

k2 = pow(yd2, xa, 29)

print(f"Secret key decrypted by ALice: {k2}")

client\_socket.close()

Bob Code:-

import socket

port = 12345

client\_socket = socket.socket()

client\_socket.connect(('localhost', port))

                                            #<3 Generating public key of Bob and sending it to Alice (which would be intruded)>

yd1 = int(client\_socket.recv(1024).decode())

print("Received public key for Bob:", yd1)

xb = int(input("Enter private key of Bob:"))

yb = pow(2,xb,29) #Public Key of BOB

print(f"Public key of Bob is: {yb}")

                                            #4. Calculating the secret key

k1 = pow(yd1,xb,29)

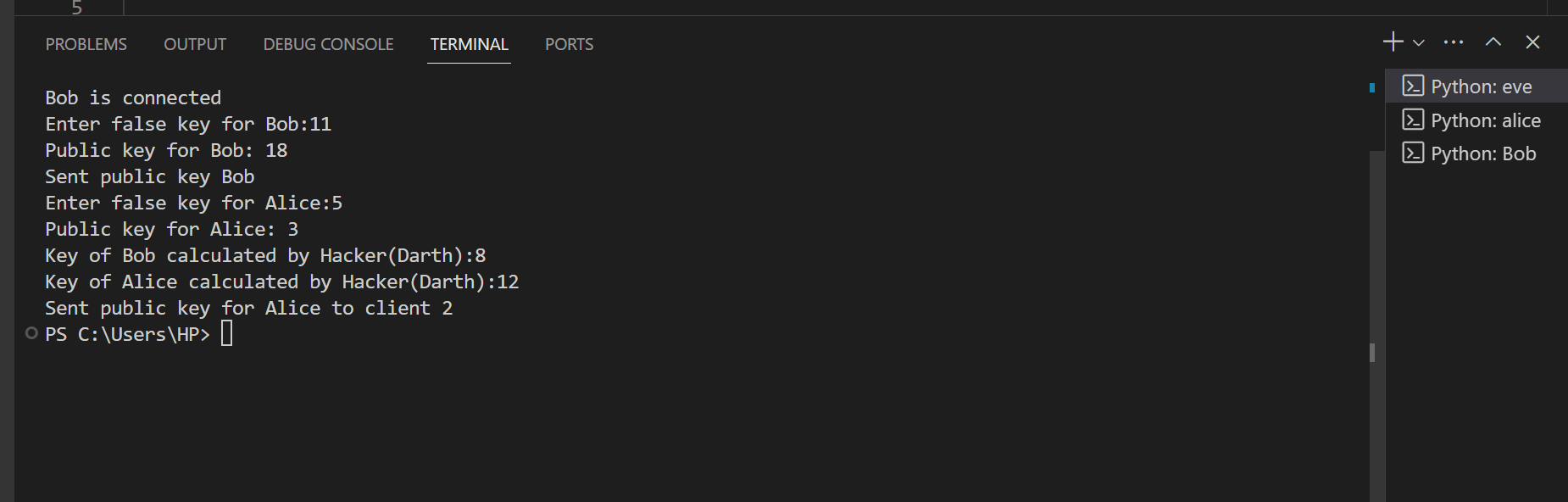
print(f"Secret key decrypted by Bob: {k1}")

client\_socket.send(str(yb).encode())

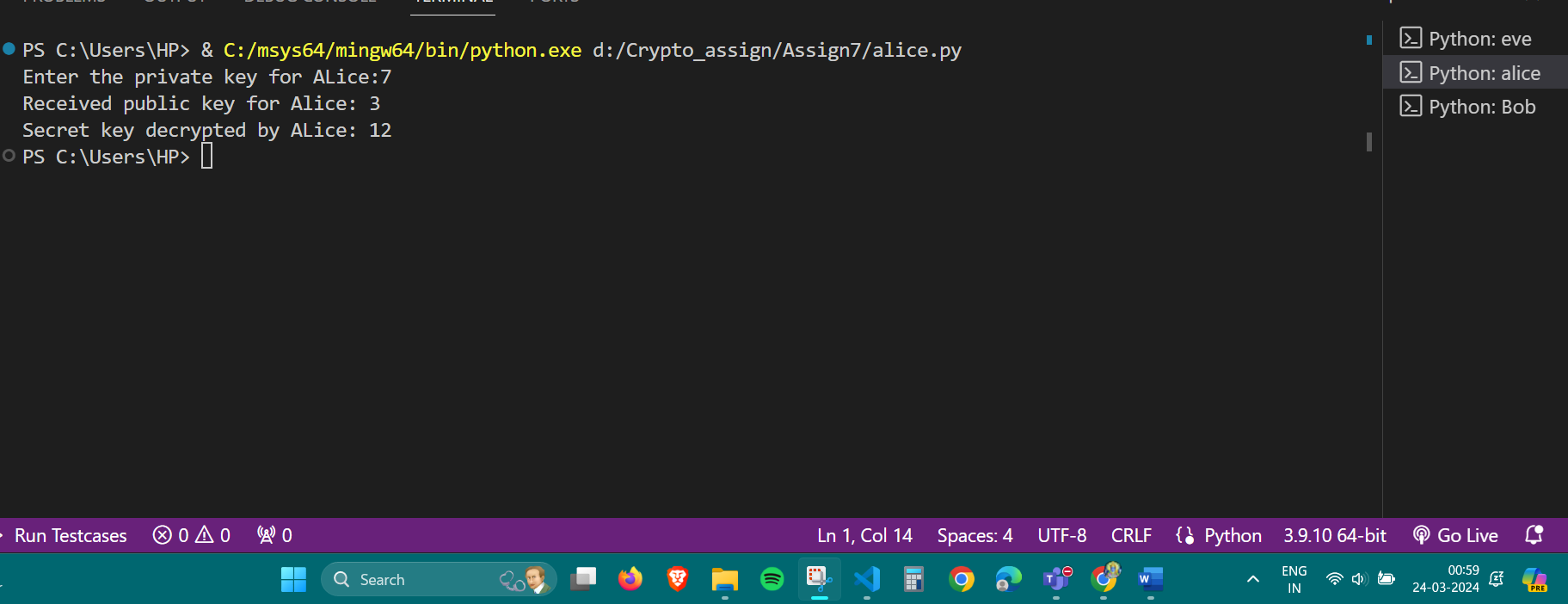
client\_socket.close()

Output:-

Eve:-



Output Alice



Output Bob

