HW 4 Austin Strobel

1.

a)

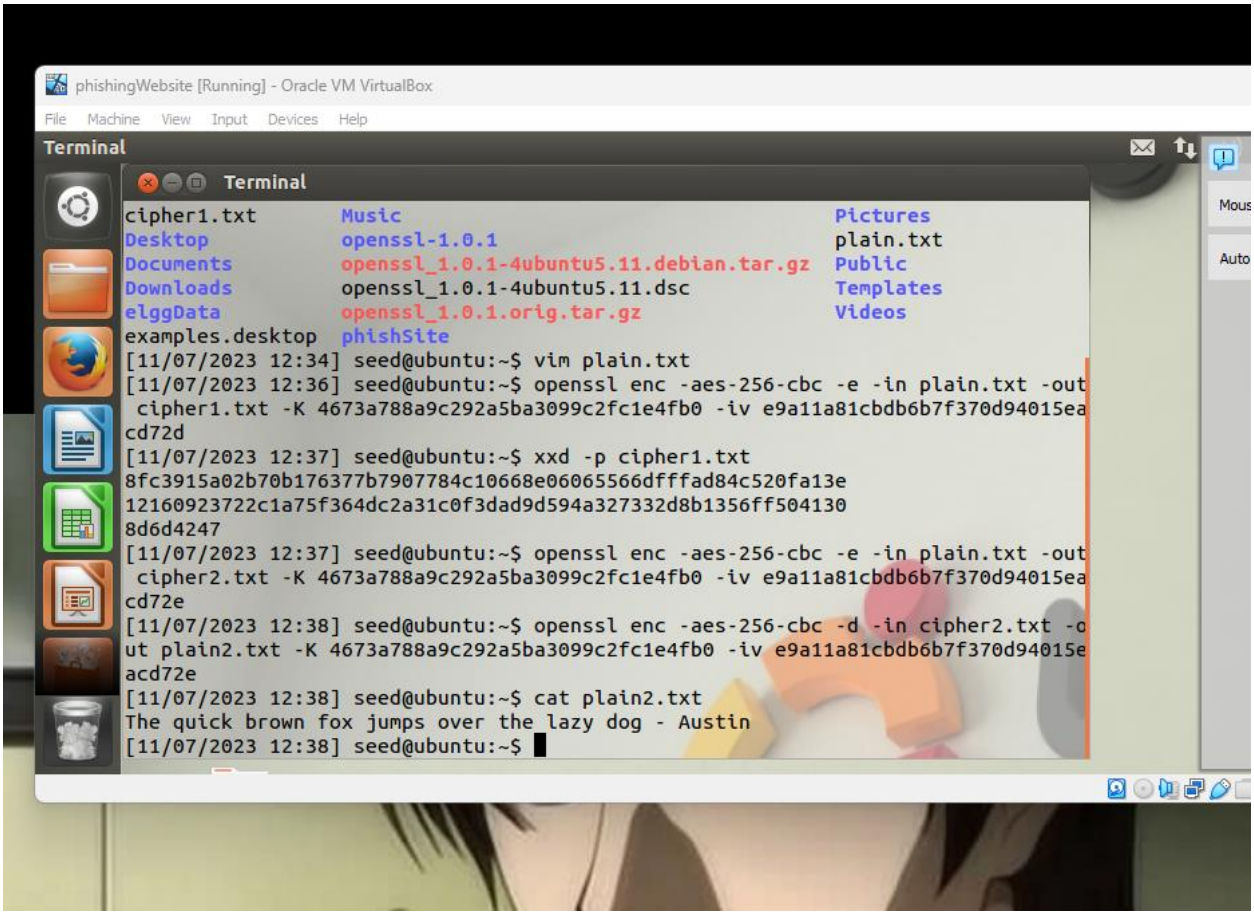
Alice needs to use her private key to encrypt the symmetric key. Alice can start by generating a random symmetric key to be used for transmission. She can use this key to encrypt the data file. She can use Bob's public key to encrypt the symmetric key using asymmetric cryptography. She would then proceed to combine the encrypted symmetric key with the encrypted data file into a message to transmit.

b)

Bob can start by decrypting the encrypted symmetric key with use of his private key to give him the original symmetric key, and Bob needs to use Alice's public key to decrypt the symmetric key. He can then get the original data file using the symmetric key to decrypt the encrypted data file.

2.

a)



b)

3.

Bob can use public key cryptography to confirm that Alice is Alice. First, Bob can make a message for Alice to respond to. Bob would then encrypt the message using Alice's public key and send the encrypted message to Alice. Alice would then decrypt the message using her private key. Alice would send the

decrypted message back to Bob, who would compare her decrypted message with his original message. If they're the same, Alice is indeed Alice.