TAKE HOME:

NOTE‼️: Please complete the introductory document thoroughly before proceeding with this lab. You will be required to answer quiz questions based on the information provided in the document. Assume that all algorithms mentioned are the same unless specified otherwise in the questions. You'll find all the files related to each task organized within folders labeled with their corresponding task numbers.

IMPORTANT NOTE: Use the same commands given in intro doc with the same order of flags.

📁 If there is a file named file.txt then Please note the following extensions

file.enc - encrypted version of that file
file.dec - decrypted version of that file
file.pri - private key associated with that file
file.pub - public key associated with that file
file.csr - certificate signing request
file.cer - certificate associated with that the file
file.sig - signature associated with that the file

Hello! Today you will be communicating with JACK 🙂. JACK wants to send you an important message. So he writes that message in a file named 'confidential_message.txt' and sends it to you.

TASK-1 💡:
But unfortunately, JILL (enemy of JACK) wants to take revenge 😡. So she tampers the message in between the communication. Now, you are a network expert and you want to help JACK. So you introduce him to checksum verification. Along with the message he also sends you the SHA-256 checksum to verify it. You have a bunch of files, some are from JACK, but JILL tampered them (MITM attack). You are being provided with the checksum of the correct file that JACK sent. You need to identify which is the correct file? 🤔

TASK-2 💡:
Oh no! JILL strikes again!!!! 🤬 Being determined to disrupt JACK's communication, JILL tampers the message and sends the checksum associated with it. Now, to help JACK you introduce him to symmetric encryption. Now JACK encrypts the message using a key and sends that key and message to you. Now you decrypt that message. What's the original message that JACK had sent? 🤔

TASK-3 💡:
JILL, gets to know this and again tries to tamper the message as you know the key is publicly available. JILL just won't quit, huh?😈 But neither will JACK (ofcourse, with the expert’s (your) help)! Now, you help JACK and you introduce him to asymmetric encryption. JACK now encrypts the file using asymmetric encryption and sends that file to you and now you guys can happily communicate. What is the original message from JACK? 🤔

TASK-4 💡:
To further secure the communication, you suggest JACK to use hybrid encryption i.e; first symmetric encryption and then asymmetric encryption. JACK first encrypts the file using a key (symmetric encryption) and then further encrypts the key using a public key shared by you (asymmetric encryption) and sends the encrypted file and encrypted key to you. What is the original message again? 🤔

TASK-5 💡:
Uh-oh, JILL is back for more trouble! JILL finds a way to impersonate JACK 😈 and communicate with you. Upon discovering this, you leverage your networking knowledge to inform JACK about digital signatures. Now he sends the message digitally signed and encrypted. Now you have a bunch of encrypted messages and the signature of the correct encrypted file. Find out the message that JACK actually sent. What is the correct message? 🤔

TASK-6 💡:
JILL again finds a way to sign the document on behalf of JACK and send it to you. However, to further enhance the security of your communication, you introduce JACK to the concept of Digital Certificates. JACK generates a self-signed certificate and sends it to you along with the digitally signed and encrypted message. You are given a bunch of files and the signature and certificate sent by JACK. You need to find out the correct file. What's the message again? 🤔

TASK-7 💡:
Now to secure this communication, you tell JACK the concept of Certificate Authorities (CAs). JACK obtains a digital certificate from a reputable CA (can you guess who), which contains his public key and identifying information, and sends it to you along with the digitally signed and encrypted message. You are given root CA from

which you need to issue the certificate and then answer the quiz questions.

TASK-8 💡:

To conclude the lab on a high note, there's an exciting surprise hidden within the secret.png file. Decrypt it to unveil the surprise! Use the symmetric encryption technique.