Question 1. [20 points]

A painter comes up with a new business idea: She wants to offer custom paintings from photos. Both the photos and paintings will be transmitted in digital form via the Internet. One concern that she has is discretion towards her customers, since potentially embarrassing photos, e.g., nude photos, might be sent to her. Hence, the photo data should not be accessible for third parties during transmission. The painter needs multiple weeks for the creation of a painting, and hence he wants to assure that she cannot be fooled by someone who sends in a photo assuming a false name. She also wants to be assured that the painting will definitely be accepted by the customer and that she cannot deny the order. In order to do this, the painter needs to make use of some of the security services that we learnt about.

Answer which security service solves which problem for the painter:

1. The photos should arrive in an errorless fashion to the painter.
2. The client should not be able to deny that he/she ordered the painting.
3. The photos should come from the real client. (not from another impostor)
4. Her online service should be live 24/7 for her customers
5. No unauthorized person should enter into possession of the photos.

Consider the following security services to answer the questions above:

Confidentiality, Integrity, Authentication, Non-repudiation, Availability, Anonymity, Physical Security.

Question 2. [40 points]

Generate an RSA private and public key pair with the following properties:

1. The length of the private exponent should 1500 in bits
2. Use 257 as the public exponent (e, i.e. the exponent used as part of the public key) --- Remember that this value is small to allow for faster encryption. Also, note that 257 is a value of the $2^n + 1$ which allows for faster completion of exponentiation using Square & Multiply algorithm.

In order to do the task above, ensure that you have access to a Linux machine. Even a command-line access should be fine. **ONLY use** the openssl command line tool to accomplish this task (http://manpages.ubuntu.com/manpages/trusty/man1/openssl.1ssl.html)
In particular, you need to use the following openssl commands to accomplish this task.

1. openssl genpkey (http://manpages.ubuntu.com/manpages/trusty/en/man1/genpkey.1ssl.html)
2. openssl rsa (http://manpages.ubuntu.com/manpages/cosmic/en/man1/rsa.1ssl.html)

After generating them include the following in your answer:

1. RSA Public key (in PEM format)
2. The commands used for generating the RSA private key and RSA public key

Don't include your private key in the answer! Get into the habit of keeping your private keys safe.

Note:

1. This Stackoverflow answer might solve some confusion you might have regarding how the RSA keys work when using the openssl tool: https://stackoverflow.com/a/44350448/1224076
2. The -text option in "openssl rsa" command is also very useful for verification.

Question 3. [40 points]

Using your **private key from above to** sign a file that contains a message in the following format:

"I deserve 40 points for Question 3! - <FULL NAME>, <DATE>"

For example, "I deserve 40 points for Question 3! - Phani Vadrevu, 18th April, 2023". **ONLY use** "openssl rsautl" command for this. Please don't hash the file before signing. The rsautl command doesn't do the hashing either.

After getting the signature, include the signature file in your submission separately. Mention the name of the signature file in your main submission PDF file. In your solution, include all the commands that you've used for solving this problem.

Note:

1. You can use the same "openssl rsautl" command to verify that your signature is correct. Please do that before making the submission.