Projects 2 (OpenSSL):

In this project you will learn how to use OpenSSL in the command line for basic functions.

I. Please watch YouTube video, the link is given below and write detail report what you have learned from the tutorial
https://www.youtube.com/watch?v=-nEh7X4dtuw

II. Do the following easy tasks and write the detail report how you get your results. The results should be screenshots with the detail explanation uploaded in pdf format.

Tasks

1. Getting started: Start your PC (Windows or Linux) with an OpenSSL installation
   a. Start the OpenSSL command line
   $ openssl
   b. List commands by type
   > list-standard-commands
   > list-cipher-commands
   > list-message-digest-commands
   c. Use the help to find out more about OpenSSL
   > help

2. Performance of OpenSSL
   a. Make a speed test on your PC-platform with the speed command
   > speed
   b. Compare the results for symmetric encryption (e.g., AES-CBC) and RSA signature. Example:
   >openssl speed rsa1024

3. Using OpenSSL from the command line interface

   a. Create a text file with some input and encrypt it using
   i. AES-128 CBC
   ii. AES-256 CTR
   iii. DES

   b. Create a 2048 bit RSA public and private key

4. Exchange of encrypted data.
   a. Encrypt a file (e.g., a text file) with an algorithm and a key length of your choice.
   b. Exchange the file and the necessary credentials for decryption (i.e., algorithm, key) with your neighbor.
   c. Decrypt the secret of your neighbor.