Write a program that uses public key-private key encryption to encrypt and decrypt a text file.

There are two clients and a server in the application. The two clients communicate with each other via the server. When one client sends a message to the server, the server stores the message as a text file in the server, where the filename is clientid_timestamp.txt. The server then encrypts and sends the file to the other client that decrypts the file and displays its content on its terminal.

1. The server, as a command-line argument, accepts the binding port number, and the public key of each of the two clients. (2 marks)
2. The two clients accept the server's IP address and port number as command-line arguments. (1 mark)
3. After connecting to the server, each of the clients keeps on reading a line from the standard input. (2 marks)
4. The first client sends the line read from the standard input to the server. (2 marks)
5. The server writes a new line it receives from the client in a new text file (Filename: <clientid>_<timestamp>.txt). It then encrypts the file and sends the encrypted text file to the second client. (6 marks)
6. The server displays "MESSAGE SENT TO <IP ADDRESS>:<PORT NO>" on its terminal. Replace <IP ADDRESS> and <PORT NUMBER> with actual values. (4 marks)
7. The second client, on receiving the encrypted file, decrypts the file using the private key that you can put directly in the program, reads the content of the file, and displays the content on the terminal. (6 marks)
8. Both clients exit when either client sends "EXIT" from the terminal. (1 mark)

What to submit:

1. The C program for the server and client (1 mark)
2. The public key of each client in 2 separate text files (name the file as publicKey_client1.txt, and publicKey_client2.txt) (1 Mark)
3. The private key of each client in 2 separate text files (name the file as privateKey_client1.txt, and privateKey_client2.txt) (1 mark)
4. A readme file on how to compile and execute the program (1 mark)

You may use the OpenSSL library for encryption and decryption. You cannot use any existing commands, such as GnuPG, for encryption and decryption. Tutorials for OpenSSL are available at http://www.cs.toronto.edu/~arnold/427/19s/427_19S/tool/ssl/notes.pdf https://www.oreilly.com/library/view/network-security-with/059600270X/ch01.html