Question 1:

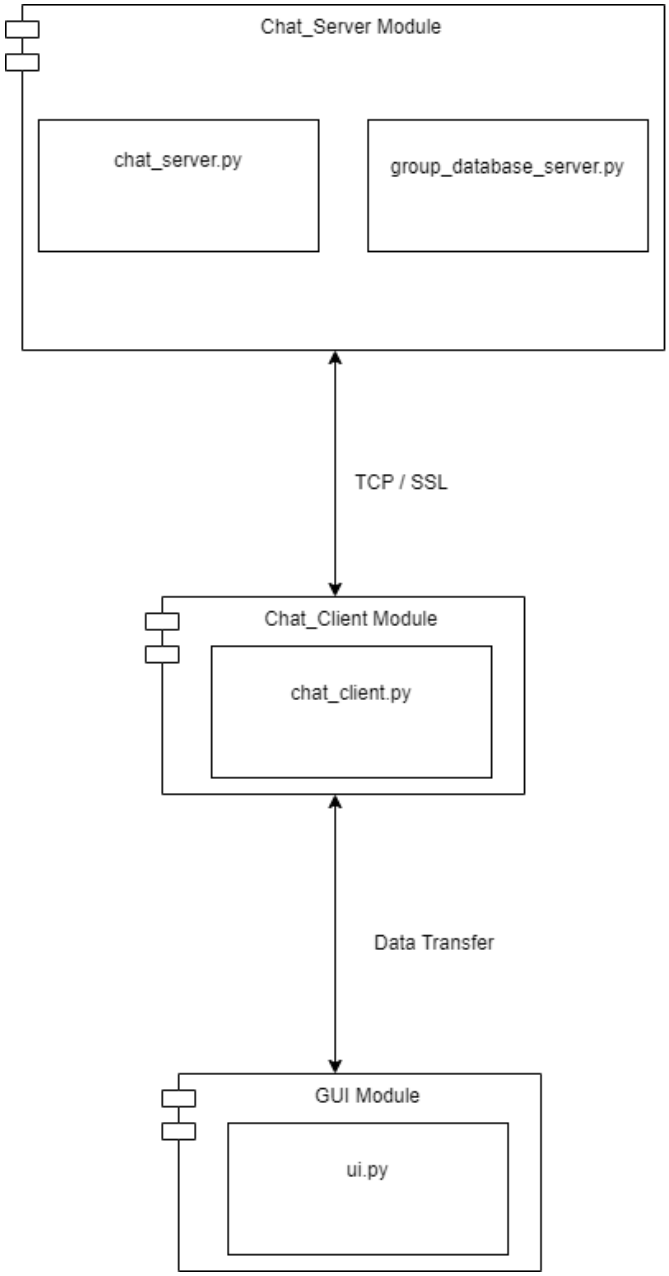

Figure 1, System Diagram

As shown in Figure 1, there are three modules present in the system: Chat_Server module, Chat_Client module and GUI module.

The Chat_Server module has the responsibility of managing the server-side logic. There are two python files relating to this module: chat_server.py and group_database_server.py. The chat_server.py is mainly responsible for establishing TCP connections with the clients, processing client messages and sending messages to clients. The group_database_server.py main contains the implementation on constructing the database for group chats.

The Chat_Client module has the responsibility of managing the client-side logic. Chat_cleint.py is the only python file in the implementation that supports the service. This module helps clients establish connections with the server and receive and send messages to the server.

The GUI module has the responsibility of providing the clients with the graphic user interface. The graphic user interface is implemented in ui.py.

The communication between the Chat_Server module and the Chat_Client module is done using a socket connection wrapped by SSL protocol. Whereas the communication between the Chat_Client module and the GUI Module is done using data transfer.

In the system, when one client talks to another client or one client talks to many clients in a room, the message is first sent to the server, the server then forwards the message to the recipients.

Question 2:

The encryption technology that is used in the system is using SSL protocol. This is done by wrapping the socket connections with the SSL protocol. The idea behind SSL protocol is that both the clients and server have their private keys. Apart from that, they also get the other's public key from a certificate authority. When a client establishes a connection with the server, the client and server agree on the encryption algorithms they will be used for later data communication encryption. When the client or server wants to send a message, the message is first encrypted by the client or server's private key. When the message arrives, the receiver uses the sender's public key to decrypt to get the message. The encryption technique is also known as asymmetric encryption. Because the messages are encrypted, the content is maintained confidential to other people unless they have the keys to decrypt the messages. Also, since the clients use their private keys to send the message and the receivers use the sender's public key to decrypt the message, the message sender's identity is ensured.