Name: Tooba Khan
Entry Number: 2021JCS2245
Report for Assignment 3 of SIL765
Readme for Problem 2.

Problem 2:

Figure 1 Server Side (my_server.py)

Figure 2 Client side(my_client.py)

Figure 3 TTP side(my_ttp.py)

To run the code, following steps have to be followed:

1. Run python3 my_ttp.py
2. Run python3 my_server.py
3. Run python3 my_client.py

Security and efficiency of the protocol:

1. TLS provides message authentication which is provided by the use of certificates and a trusted third party in my implementation.
2. It is safe against replay attacks because nonces are generated by both the client and server and they are used in the generation of session keys.
3. TLS provides encryption by using symmetric key to encrypt the data being exchanged. This key is generated by sharing a premaster key encrypted using public keys of client and server.
4. TLS works with most of the web browsers.
5. TLS is invisible to the client because it is implemented below the application layer.
6. It can also work with servers running on Windows 2003.
7. TLS also provides a wide range of encryption methods making it flexible enough for different use cases.