This project bases on python pyOpenssl, python socket, PyCryptodome, hashlib.
The main part of the lab is finished by myself based on the slide of IEMS5710-lab and the official document. Some functions are referenced with the codes of website.
In this lab, I meet some bugs. Some solutions are also from the websites.

The list of the websites is referred:
https://docs.python.org/zh-cn/3/library/socket.html
https://www.pyopenssl.org/en/latest/
Welcome to PyCryptodome's documentation — PyCryptodome 3.15.0 documentation
https://github.com/nuisttudou/Cryptographic-systems
https://cloud.tencent.com/developer/ask/sof/206525
https://stackoverflow.com/questions/43519363/create-csr-and-self-signed-certificate-with-pyopenssl
https://stackoverflow.com/questions/23103878/sign-csr-from-client-using-ca-root-certificate-in-python
https://stackoverflow.com/questions/46553338/how-to-verify-certificate-signature-in-pyopenssl
https://www.jianshu.com/p/5b38b4187b54
https://blog.csdn.net/lly1122334/article/details/104794160
https://github.com/kevin-w-du/BookCode/blob/master/Encryption/enc_gcm.py

zhao Yuyang