IEMS 5710 Cryption Lab
Li Kaixu
1155180259

Contribution:

1. build a simple CUHK-Blackboard-Student crypted communication system
2. complete the X509 certificate and csr based on pyOpenSSL
3. use the RSA and AES GCM for message encryption and transmit it through socket

Signatue: 李凯旭

Reference:

[1] https://cloud.tencent.com/developer/article/1882149
[2] https://docs.python.org/zh-cn/3/library/socket.html
[3]https://mohomedarfath.medium.com/signing-a-certificate-using-created-ca-cert-by-using-python-script-8f20117737d7
[4] https://detailed.wordpress.com/2017/01/25/create-self-signed-root-ca-certificate-with-the-help-of-python-using-openssl/
[5] https://pyopenssl.sourceforge.net/pyOpenSSL.html/openssl-x509.html
[6] https://www.pyopenssl.org/en/stable/api/crypto.html
[7]https://stackoverflow.com/questions/17958347/how-can-i-convert-a-python-urandom-to-a-string
[8] https://cryptobook.nakov.com/mac-and-key-derivation
[9] https://pycryptodome.readthedocs.io/en/latest/src/cipher/modern.html#gcm-mode
[10] https://cryptobook.nakov.com/asymmetric-key-ciphers/rsa-encrypt-decrypt-examples