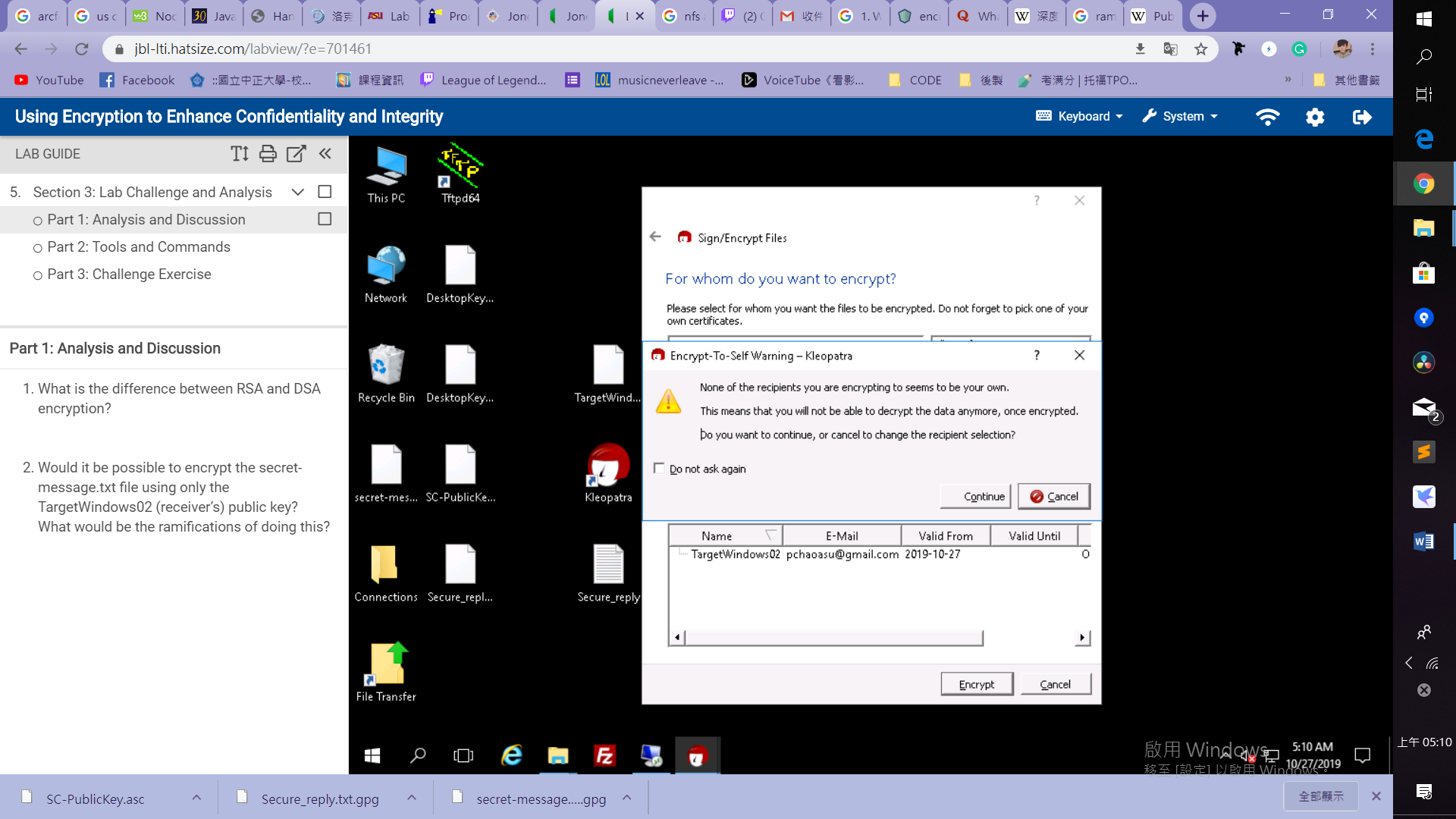
Part 1

1. What is the difference between RSA and DSA encryption?

An RSA crypto-algorithm is based on large-number factorization -- i.e., P \* Q = N, and in the other side, A DSA crypto-algorithm is based on discrete logarithms -- i.e., B to the K power = G. DSA is a bit faster than RSA when creating a signature but slower for validation, slower when encrypting but faster when decrypting. RSA is opposite.

1. The data can not be decrypt anymore, once the encrypt happened.



Part 2

Generate Keys on the PGP Command Line

pgp --gen-key "Sean <[sean@example.com](mailto:sean@example.com)>" --key-type rsa --encryption-bits 2048 --signing-bits 2048 --passphrase 1Tsecurity! --expiration-date 2019-12-22

Encrypt & Sign a file:

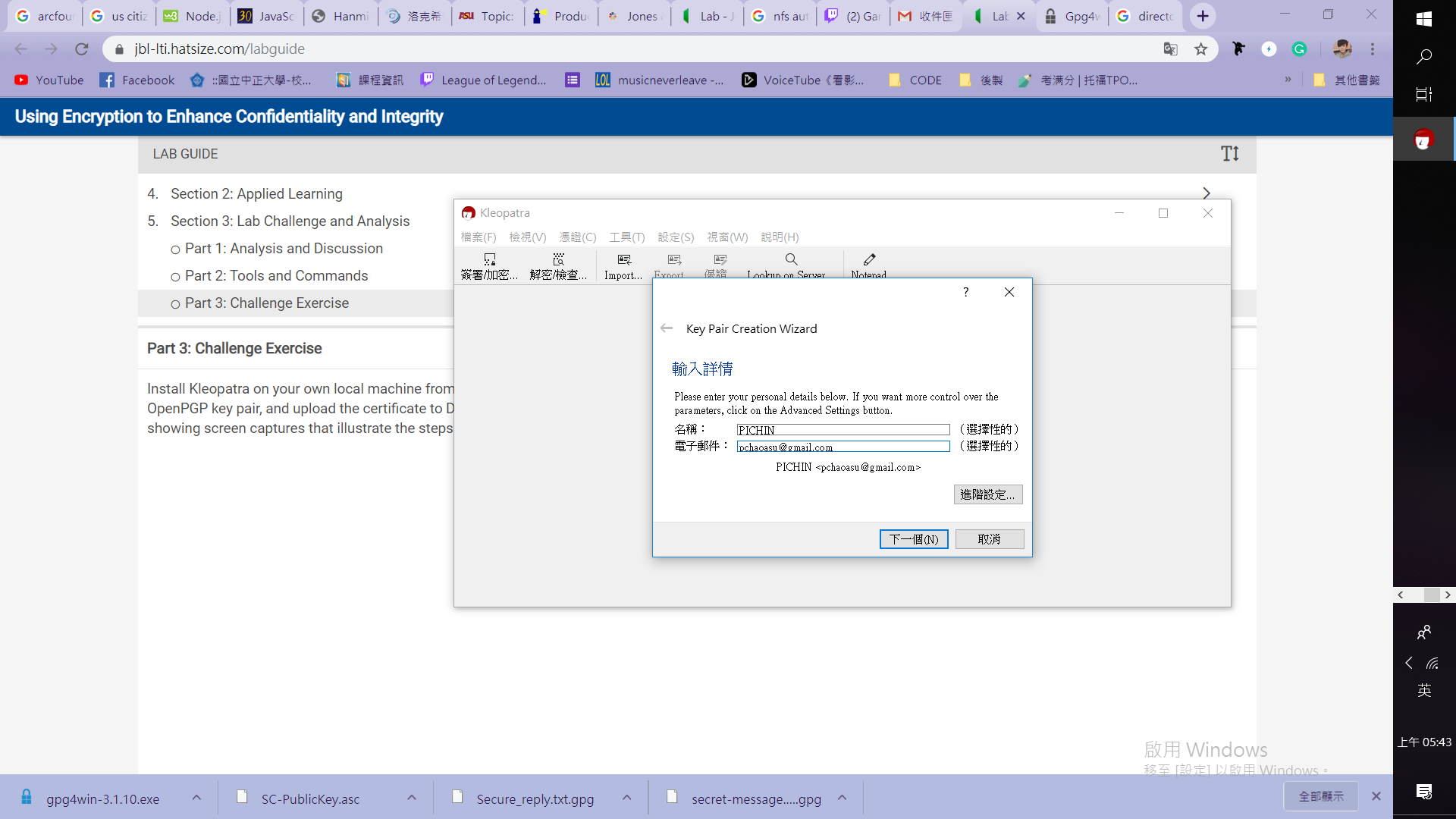
pgp --encrypt my-message.txt -recepient public key –sig secret-message.txt --signer "Sean" --passphrase <1Tsecurity!>

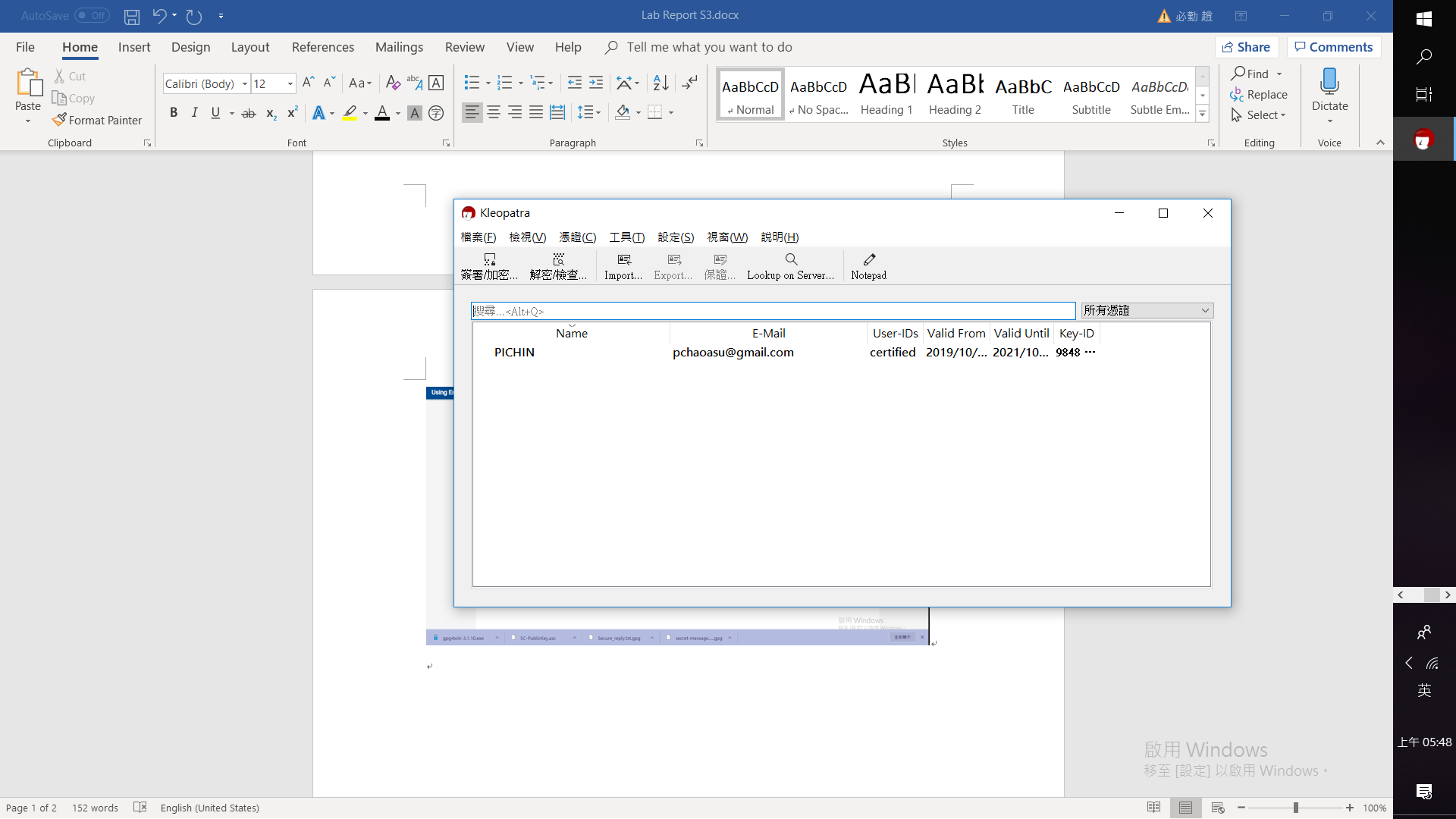
Generate revocation certificate

gpg --output revoke.asc --gen-revoke mykey

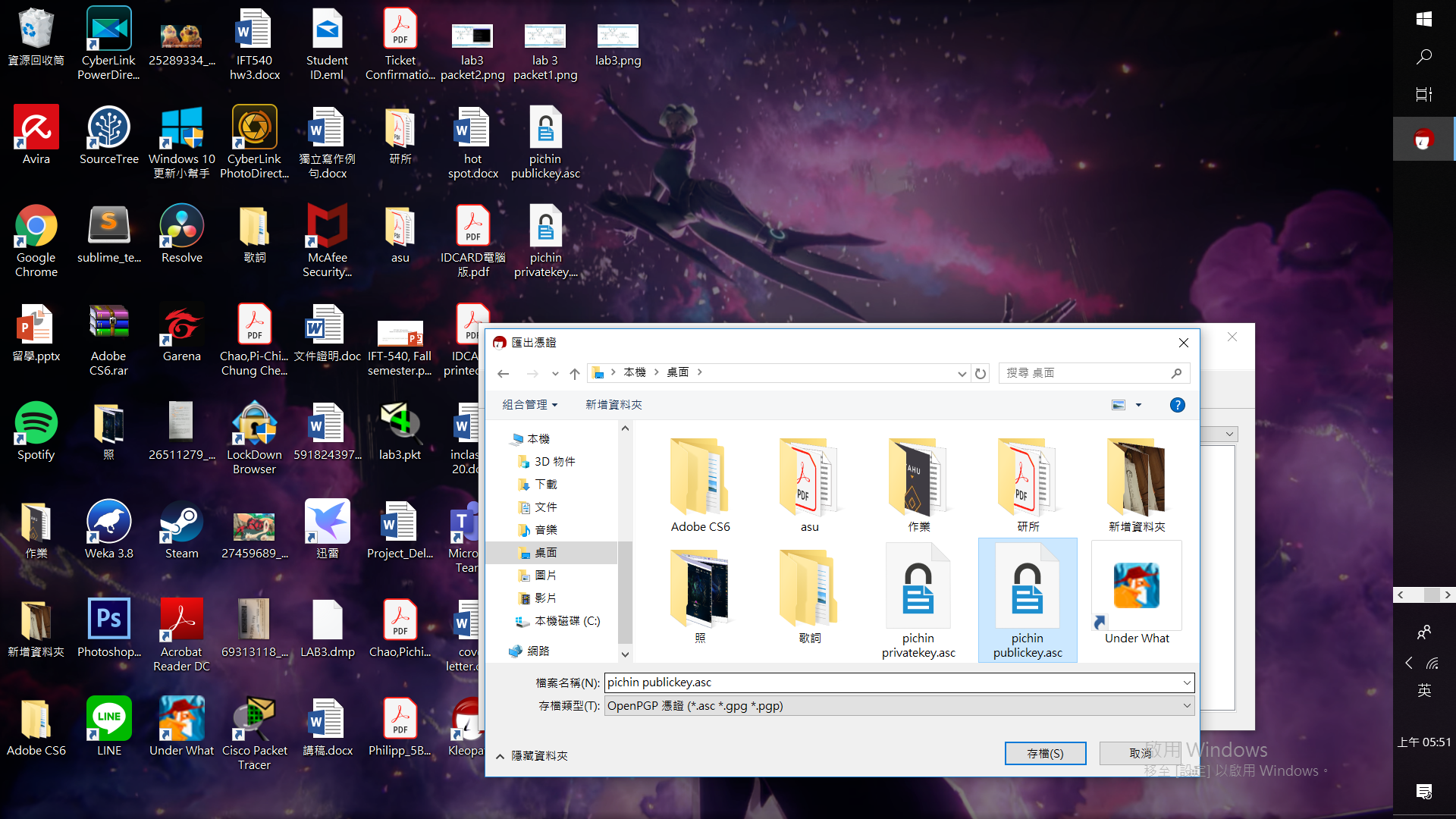
Part 3

Create own personal OpenPGP key

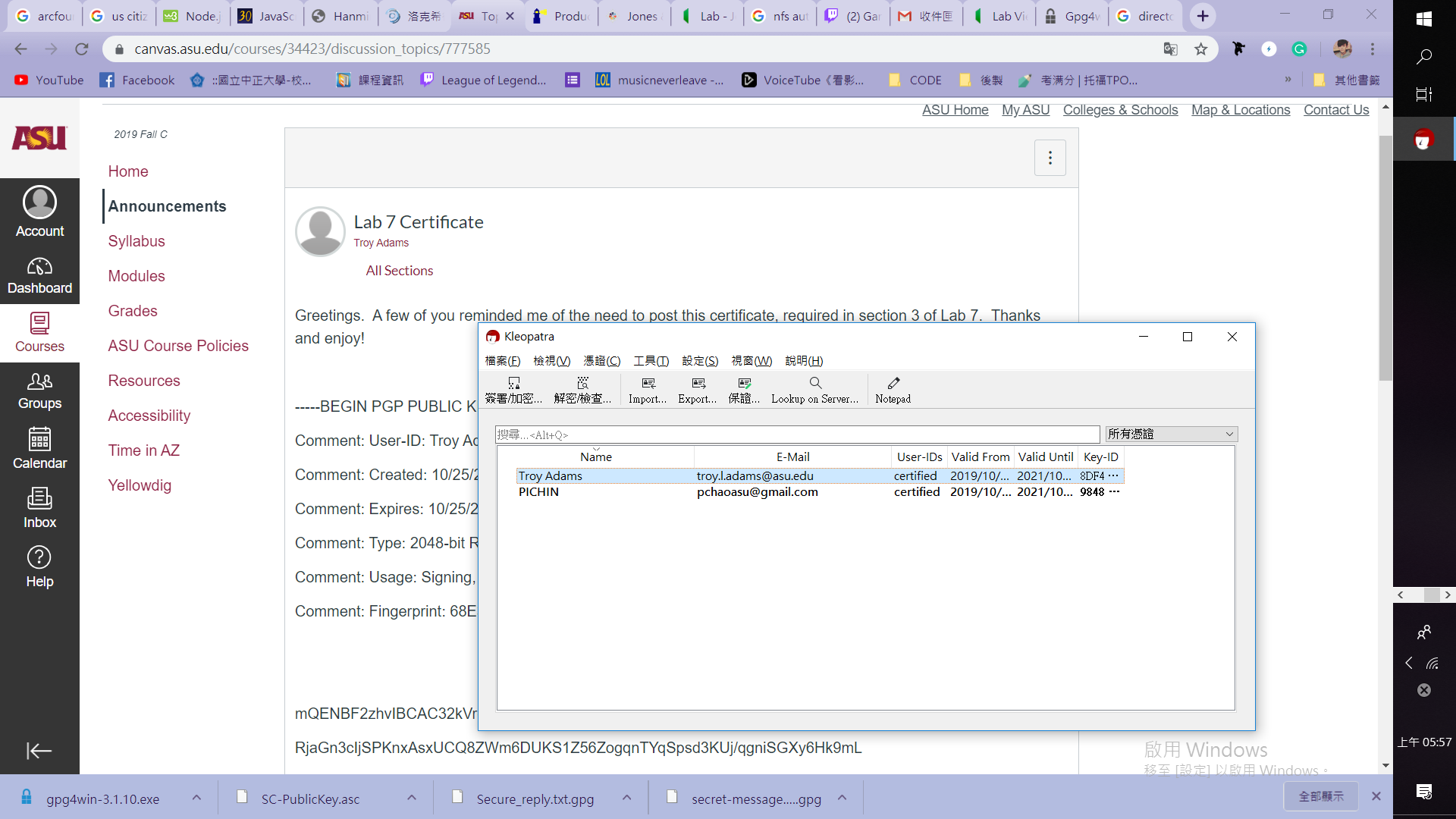




Export Private key and Public key



Import the certification provided by Professor



Encrypt a copy of Lab Report S1

