정보보호론 실습

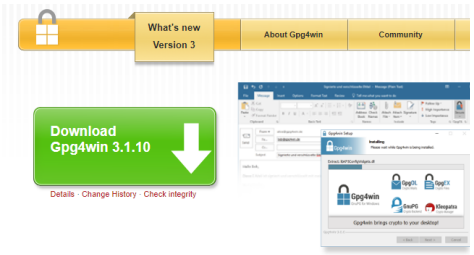
공개 키 암호화

실습 내용

- Kleopatra를 이용하여 공개 키 암호화를 이해

[첫번째] 주어진 공개 키로 암호화

- http://www.gpg4win.org/index.html
  - Download Gpg4win
  - Certificate Creating



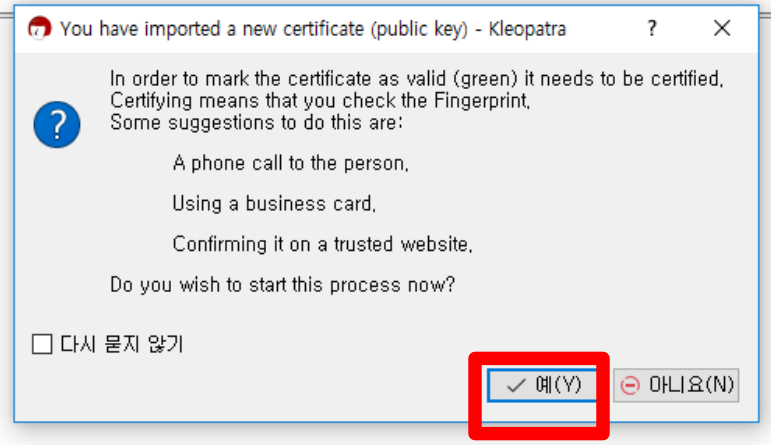
Gpg4win - a secure solution...

... for file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

High algorithmic strength of GnuPG

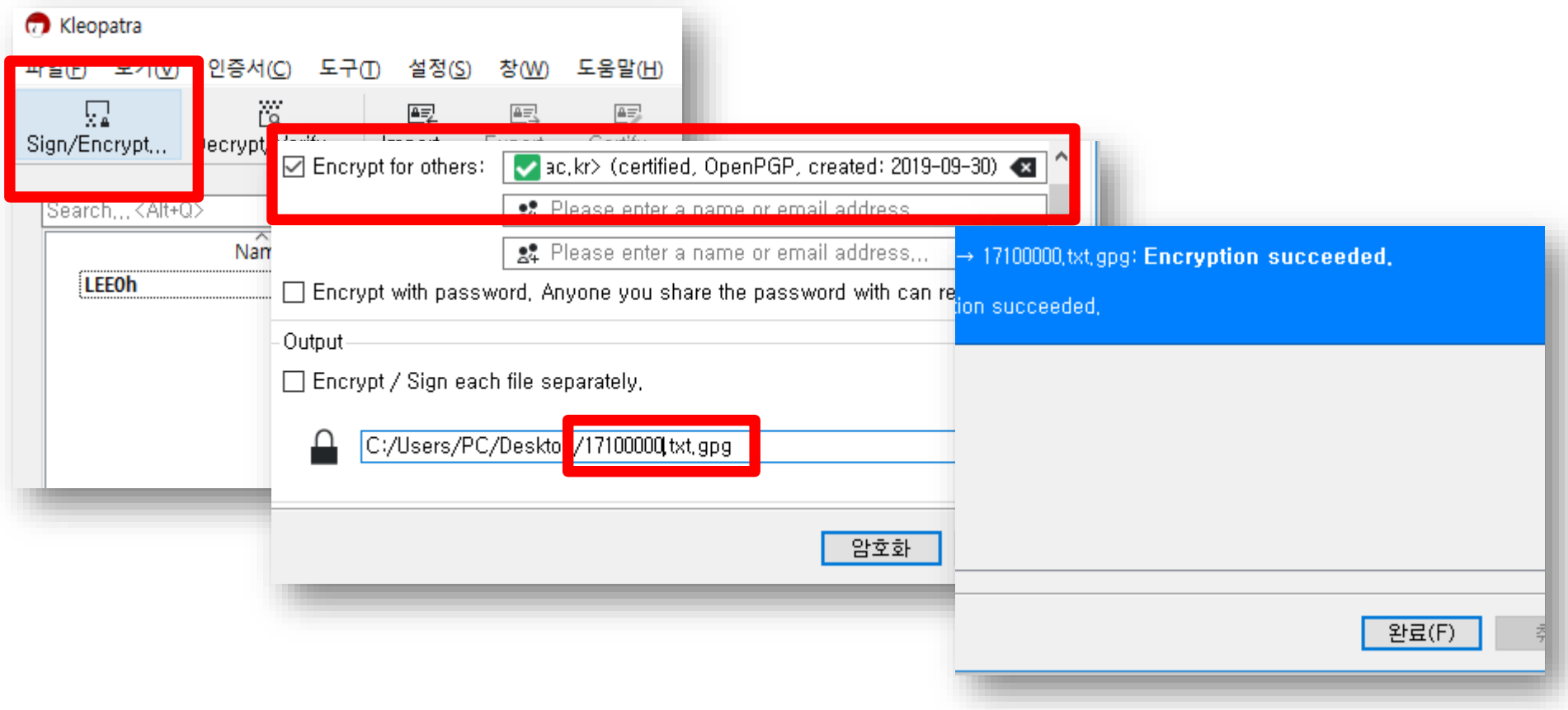
Gpg4win is the official GnuPG distribution for Windows and provides the high cryptographic standards of the GNU Privacy Guard. GnuPG follows the recommendations regarding algorithms and key length of the German Federal Office for Information Security (BSI).

To create OpenPGP and X.509 certificates Gpg4win uses a key length of 2048bit by default. The default algorithm for signing and encrypting is RSA.



E-Class에 올라와 있는 공개키를 PC에 저장, Import

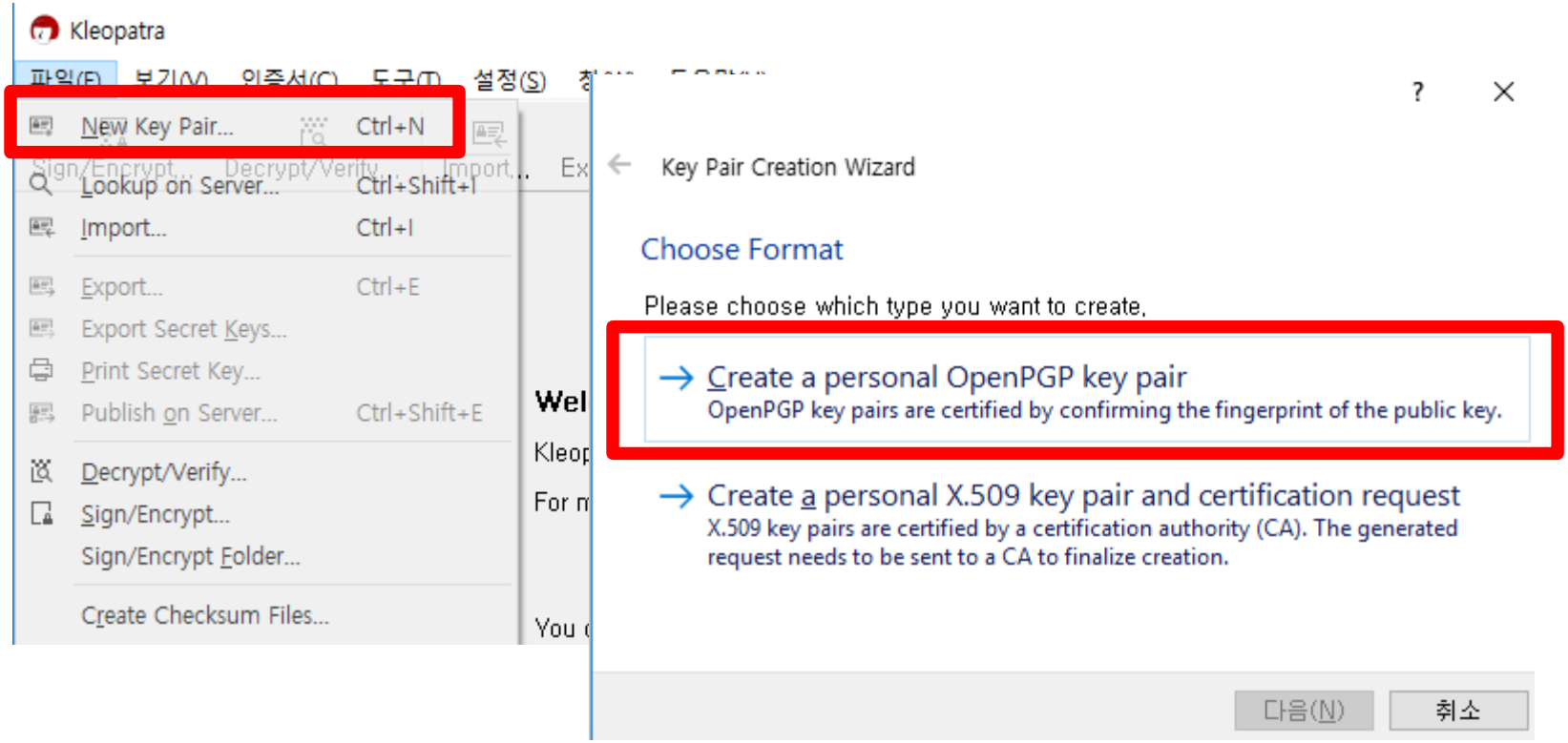
[첫번째] 주어진 공개 키로 암호화



자신 학번으로 텍스트 파일 생성, 주어진 공개키로 암호화

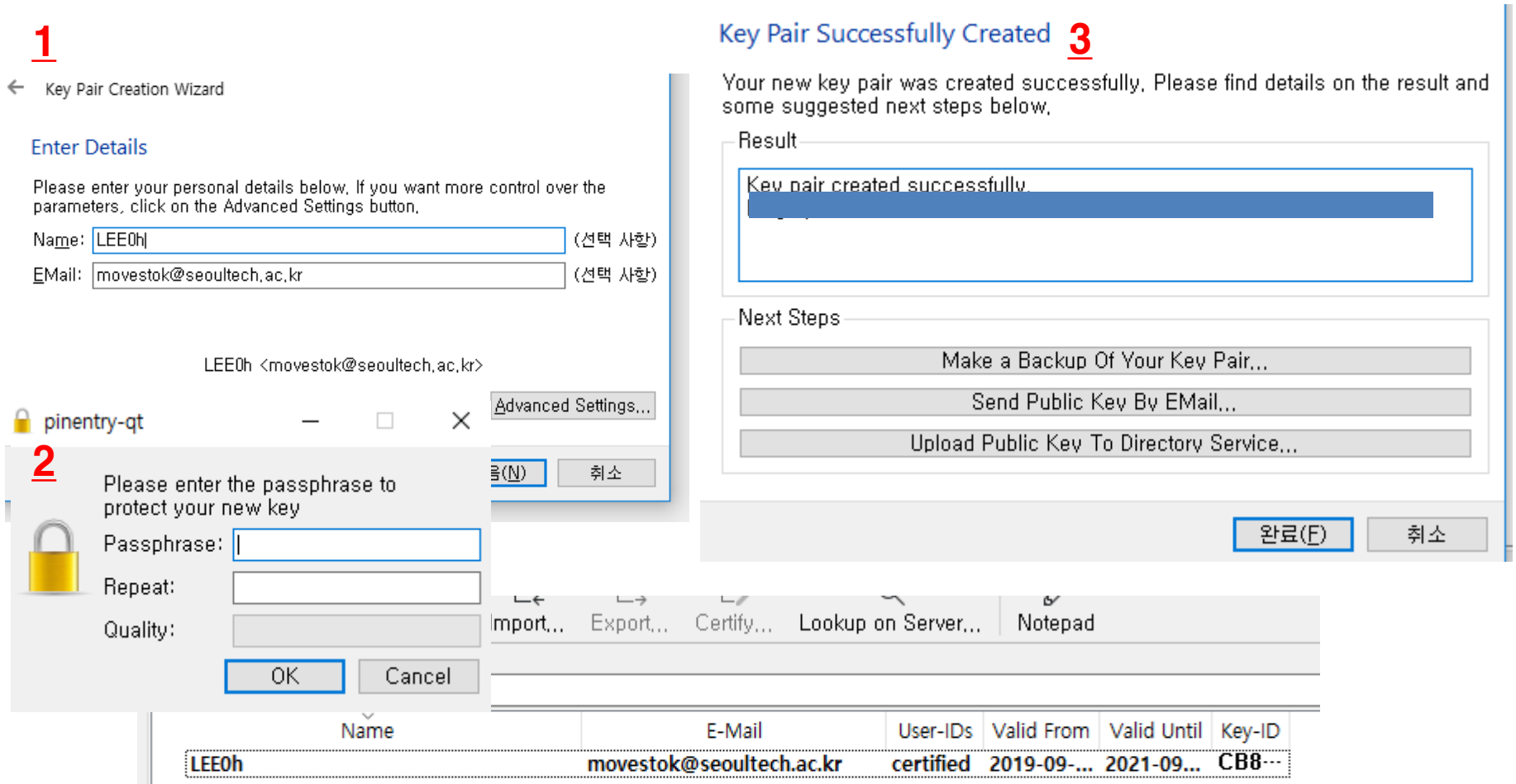
생성된 E-class 과제 게시판에 올리기

[두번째] 공개 키 생성 & 암호화



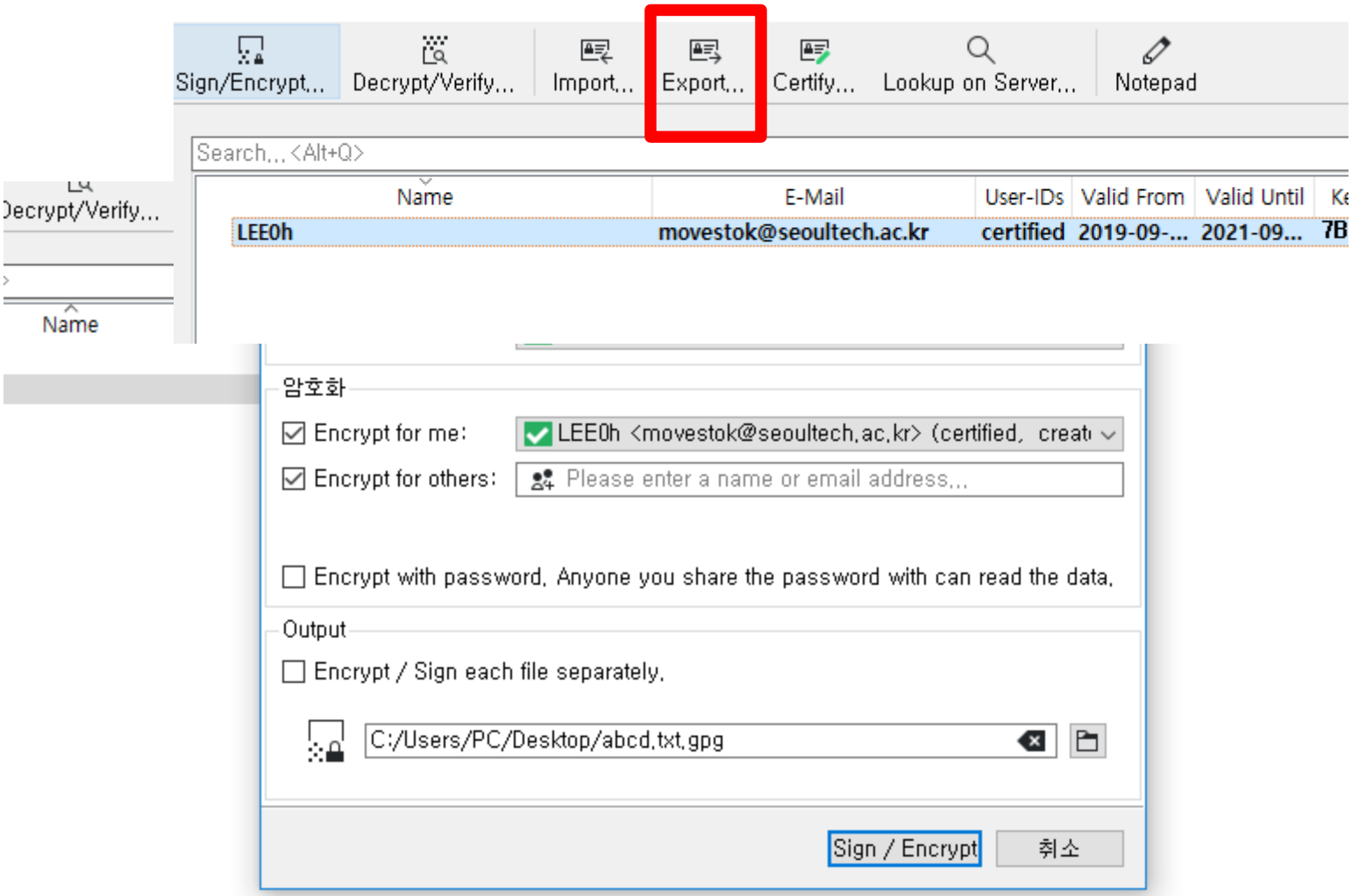
자신의 공개키 개인키(key pair) 생성

[두번째] 공개 키 생성 & 암호화



정보 입력하여 생성 가능

[두번째] 공개 키 생성 & 암호화



생성된 공개키를 추출 및 공유 할 수 있음

실습문제 정리

실습 1번 : **자신 학번으로** 텍스트 파일 생성, 주어진 공개키로 암호화, 생성된 E-class 과제 게시판에 암호화된 파일 올리기

- **제출 제목 양식 : 이름_학번_5주차**

참고문헌

- 정보 보안 개론[개정3판], 양대일 저, 한빛미디어, 2018, 1.
- 컴퓨터보안, William Stalling 저, 한티미디어, 2016. 8
- 정보보안과 사이버 해킹의 기초, 김경신 저, 2016. 8

Q & A