

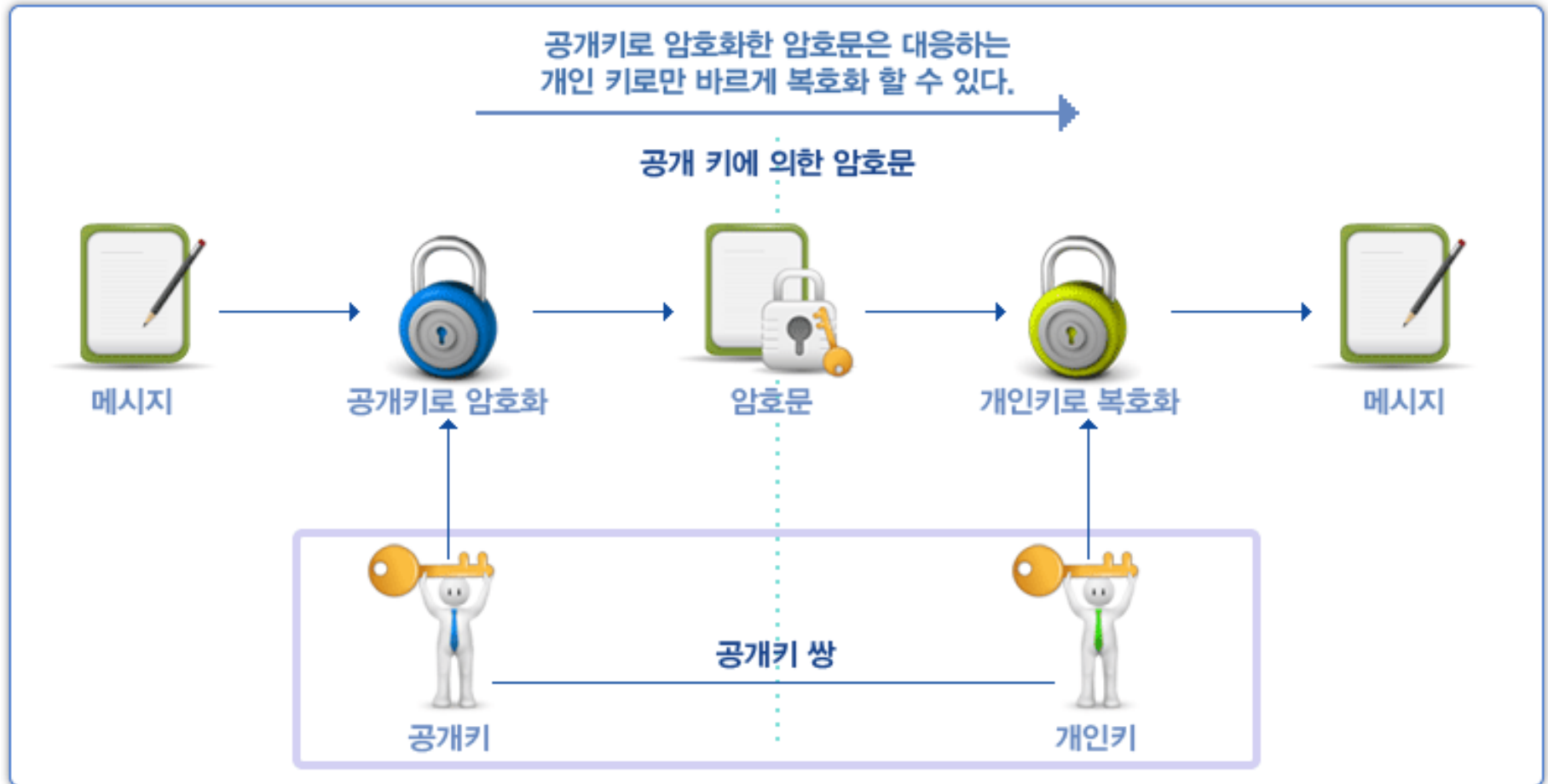
# 정보보호론 실습

공개 키 암호화

# 실습 내용

- Kleopatra를 이용하여 공개 키 암호화를 이해

## ▶ 공개 키에 의한 암호화 (공개 키 암호)



# [첫 번째] 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**.

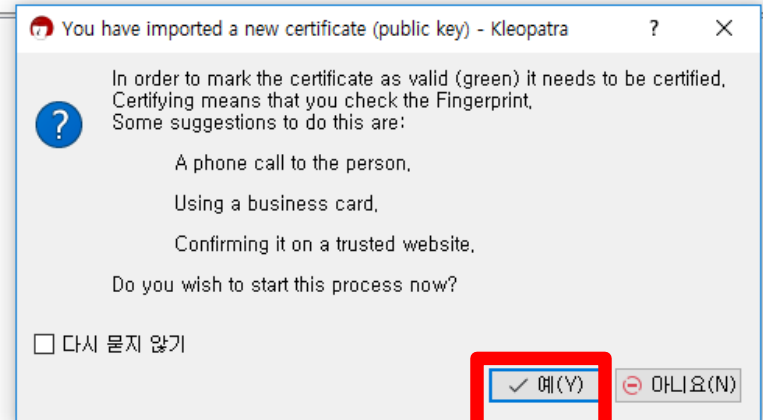
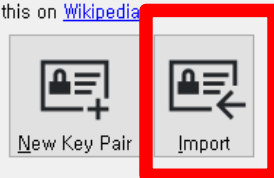
## Welcome to Kleopatra 3.1.8-gpg4win-3.1.10

Kleopatra is a front-end for the crypto software [GnuPG](#).

For most actions you need either a public key (certificate) or your own private key

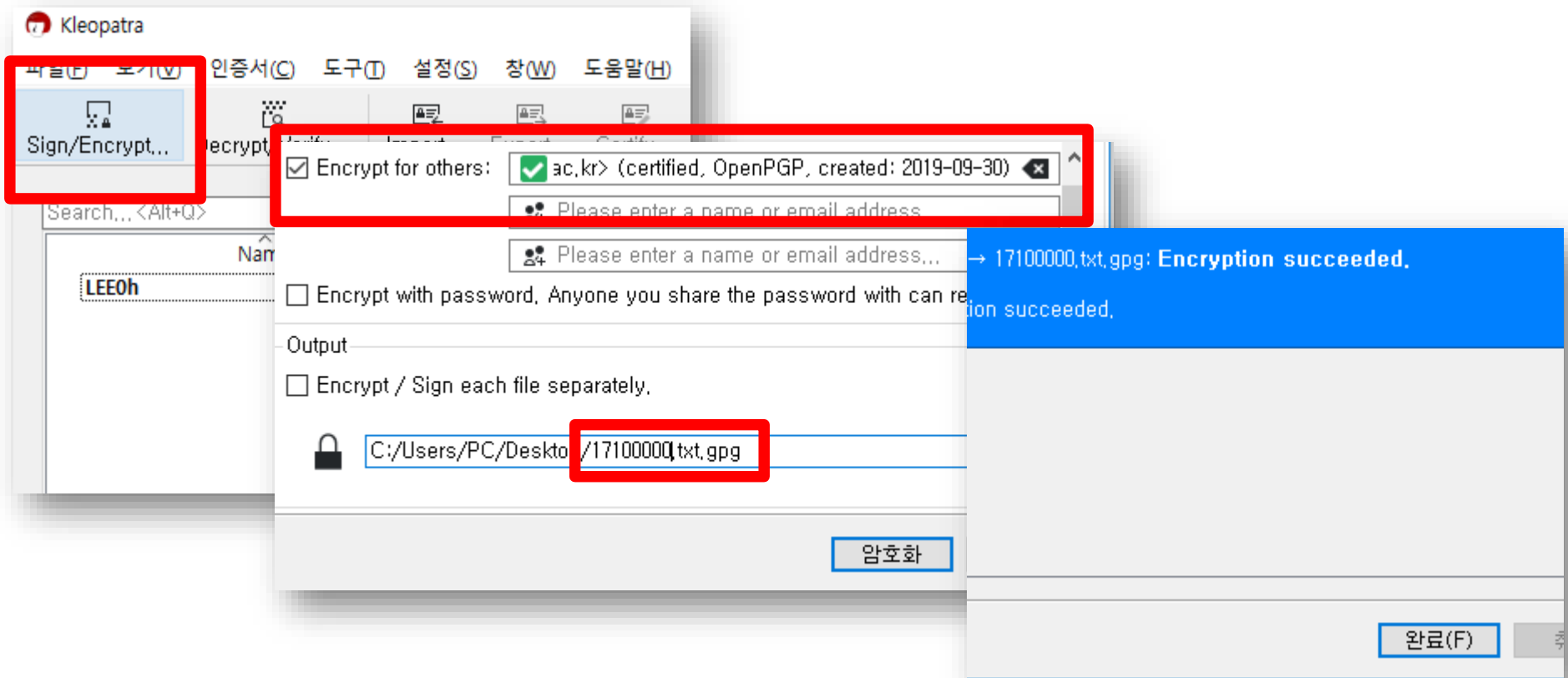
- The private key is needed to decrypt or sign,
- The public key can be used by others to verify your identity or encrypt to you

You can learn more about this on [Wikipedia](#)



E-Class에 올라와 있는 공개키를 PC에 저장, Import

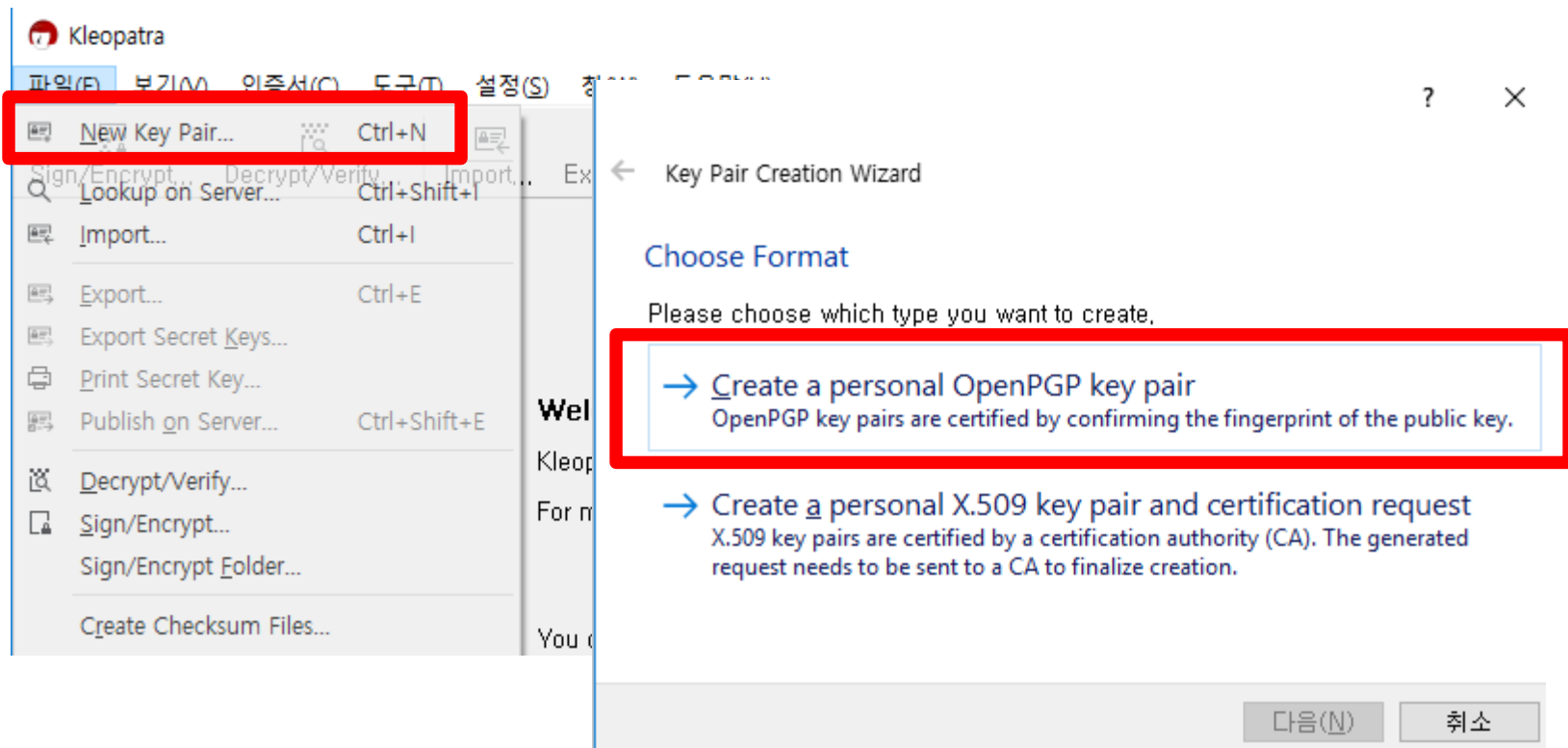
# [첫 번째] 주어진 공개 키로 암호화



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

1

← Key Pair Creation Wizard

## Enter Details

Please enter your personal details below. If you want more control over the parameters, click on the Advanced Settings button.

Name:  (선택 사항)

E-Mail:  (선택 사항)

LEE0h <movestok@seoultech.ac.kr>

pinentry-qt

Advanced Settings...

문(N)

취소

2

Please enter the passphrase to protect your new key

Passphrase:

Repeat:

Quality:

OK

Cancel

## Key Pair Successfully Created 3

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

### Result

Key pair created successfully.

### Next Steps

Make a Backup Of Your Key Pair...

Send Public Key By EMail...

Upload Public Key To Directory Service...

완료(E)

취소

Import...

Export...

Certify...

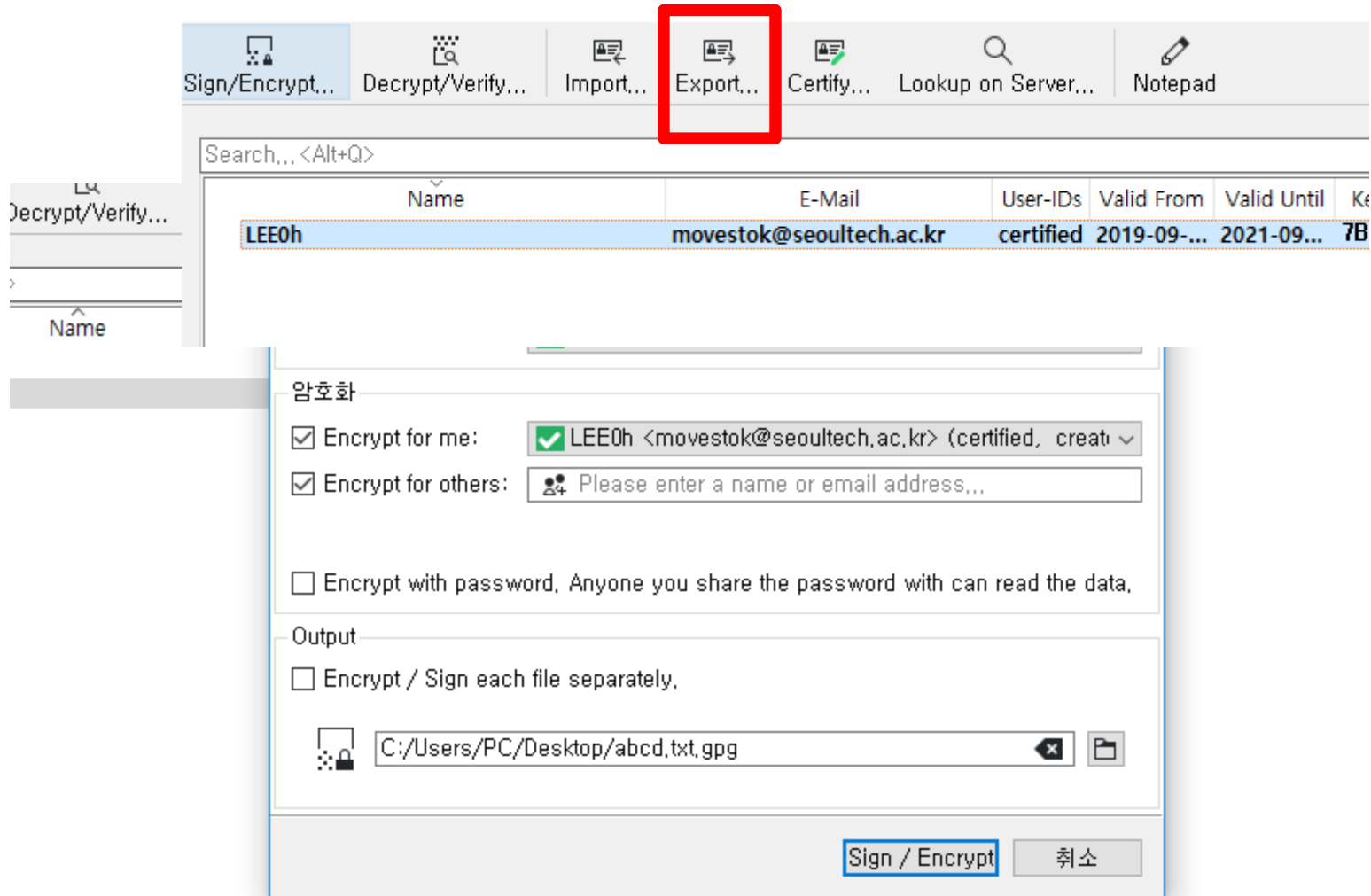
Lookup on Server...

Notepad

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
LEE0h	movestok@seoultech.ac.kr	certified	2019-09-...	2021-09-...	CB8...

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