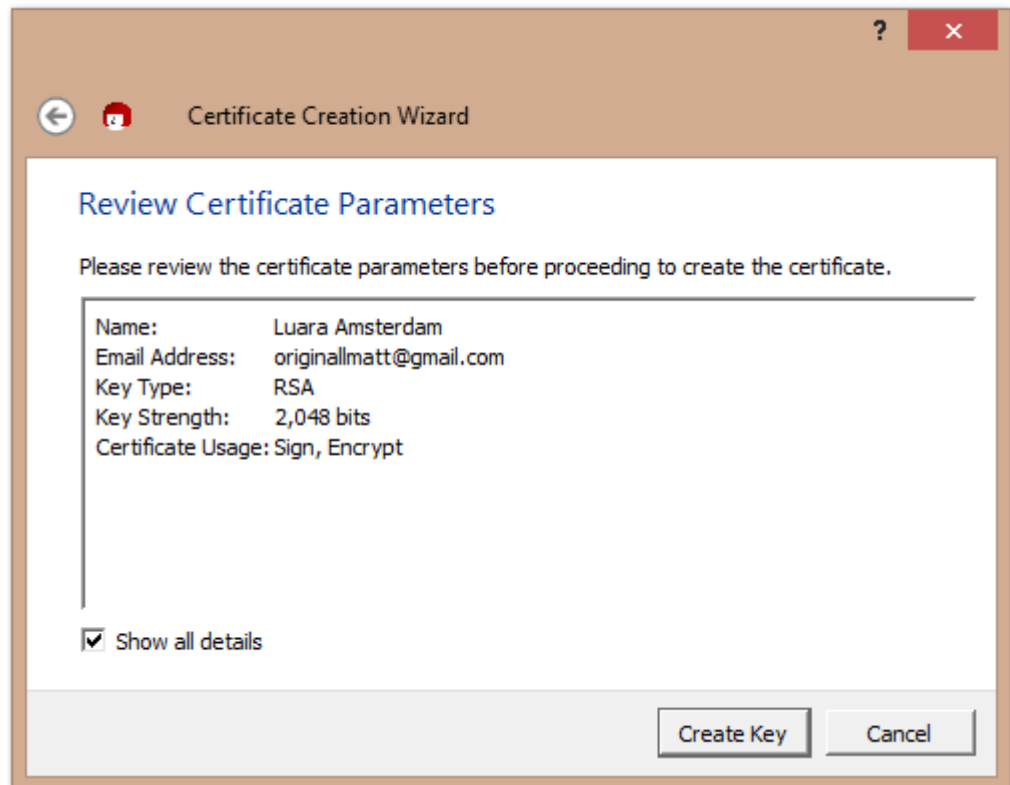


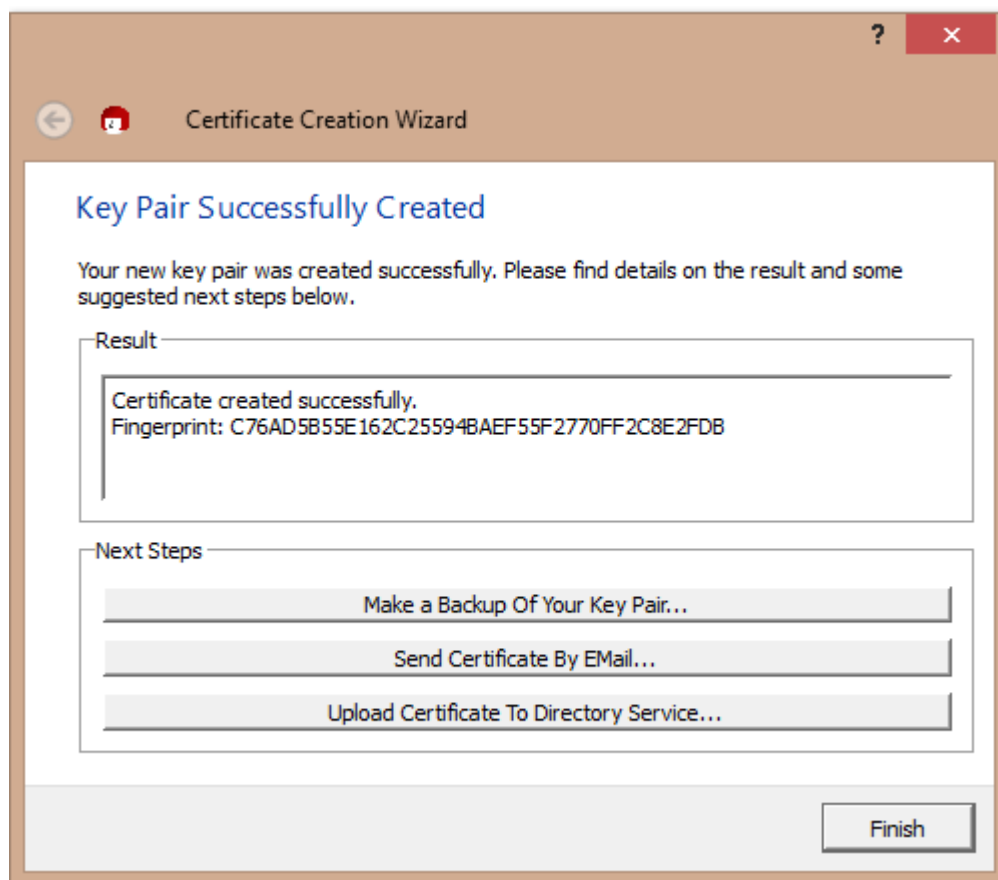
Отчет по лабораторной работе №3  
Программа для шифрования и подписи  
GPG, пакет Gpg4win

Греченко Лаура

25 мая 2015 г.

1. Изучить документацию, запустить графическую оболочку Kleopatra  
Была изучена документация перечисленная в разделе материалы.
2. Создать ключевую пару OpenPGP (File => New Certificate) Создали  
новый сертификат.





3. Экспортировать сертификат (File => Export Certificate) Экспортировали сертификат.
4. Поставить ЭЦП на файл (File => Sign/Encrypt Files)  
Выбираем пункт подписать и зашифровать.

← Sign/Encrypt Files

### What do you want to do?

Please select here whether you want to sign or encrypt files.

Selected file:

- E:\Study\ZI\Result\3\sign\_file.txt

☐ Archive files with: TAR (PGP®-compatible)

Archive name (OpenPGP): E:\Study\ZI\Result\3\sign\_file.txt.tar

Archive name (S/MIME): E:\Study\ZI\Result\3\sign\_file.txt.tar.gz

☒ Sign and Encrypt (OpenPGP only)

☐ Encrypt

☐ Sign

☐ Text output (ASCII armor)

☐ Remove unencrypted original file when done

Next Cancel

Выбираем сертификат.

Sign/Encrypt Files

For whom do you want to encrypt?

Please select for whom you want the files to be encrypted. Do not forget to pick one of your own certificates.

Search...

All Certificates

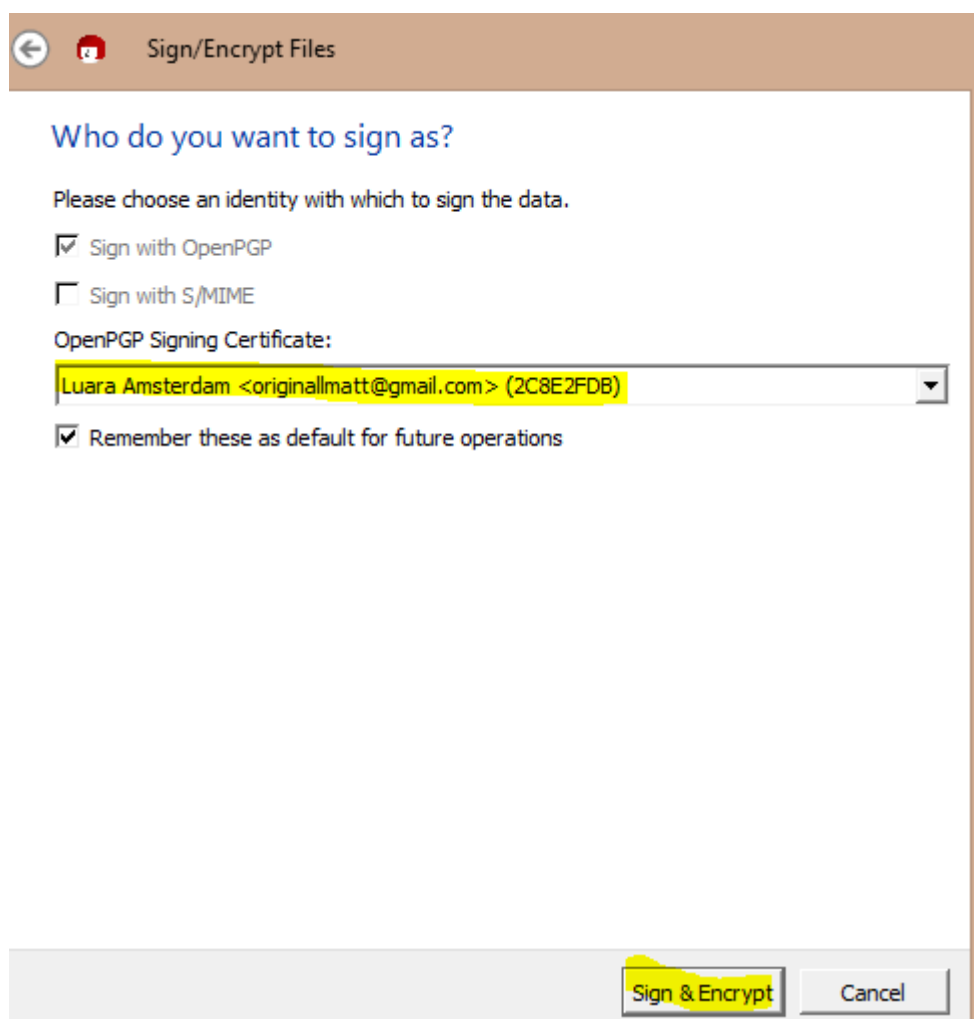
Name	E-Mail	Valid From	Valid Until
<input type="checkbox"/> Luara Amsterdam	originalmatt@gmail.com	2015-05-25	
<input type="checkbox"/> Karina Vilegzhana	k.vilegzhana@gmail.com	2015-02-08	

AddRemove

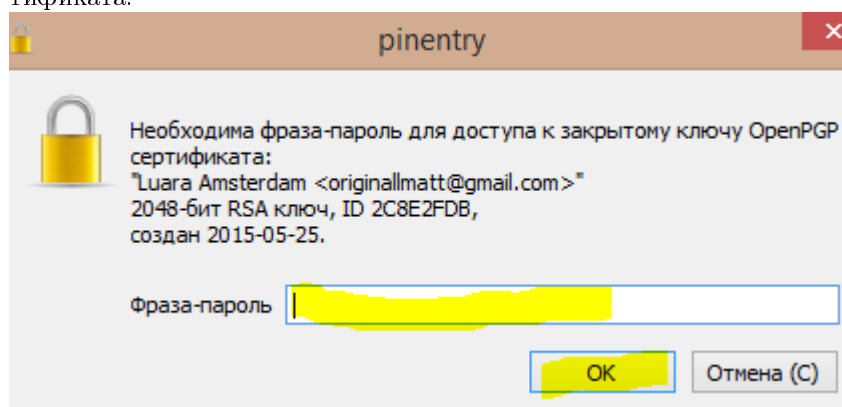
Name	E-Mail	Valid From	Valid Until
<input checked="" type="checkbox"/> Luara Amsterdam	originalmatt@gmail.com	2015-05-25	

NextCancel

Выбираем сертификат OpenPGP.



Необходимо ввести фразу-пароль, введенную при формировании сертификата.



В результате успешно зашифровали и подписали данные.

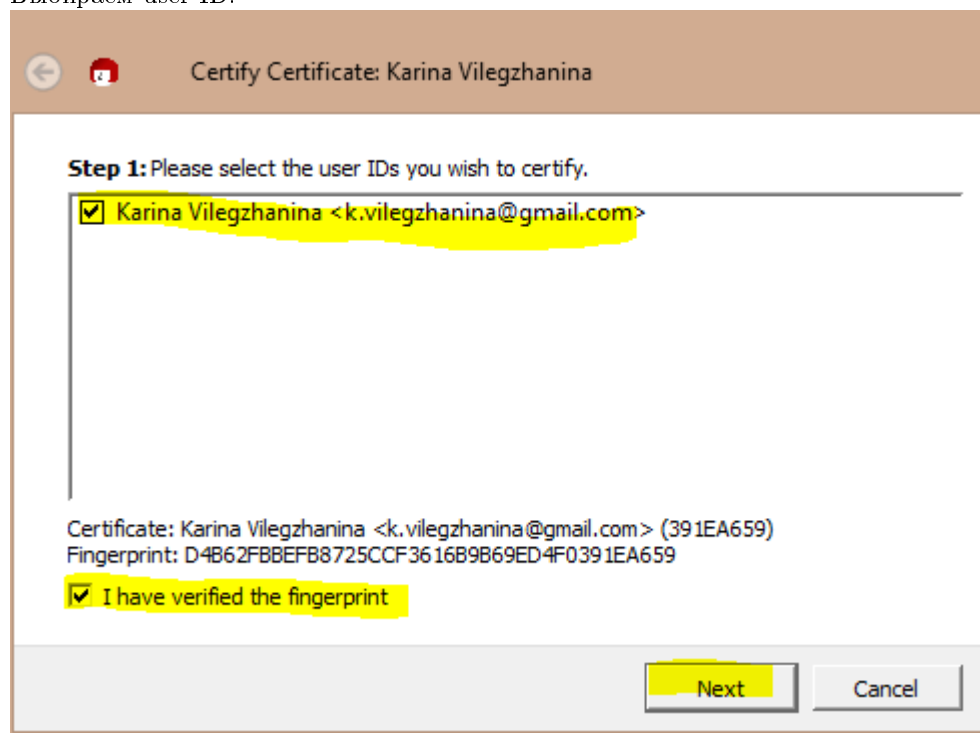
## Results

Status and progress of the crypto operations is shown here.

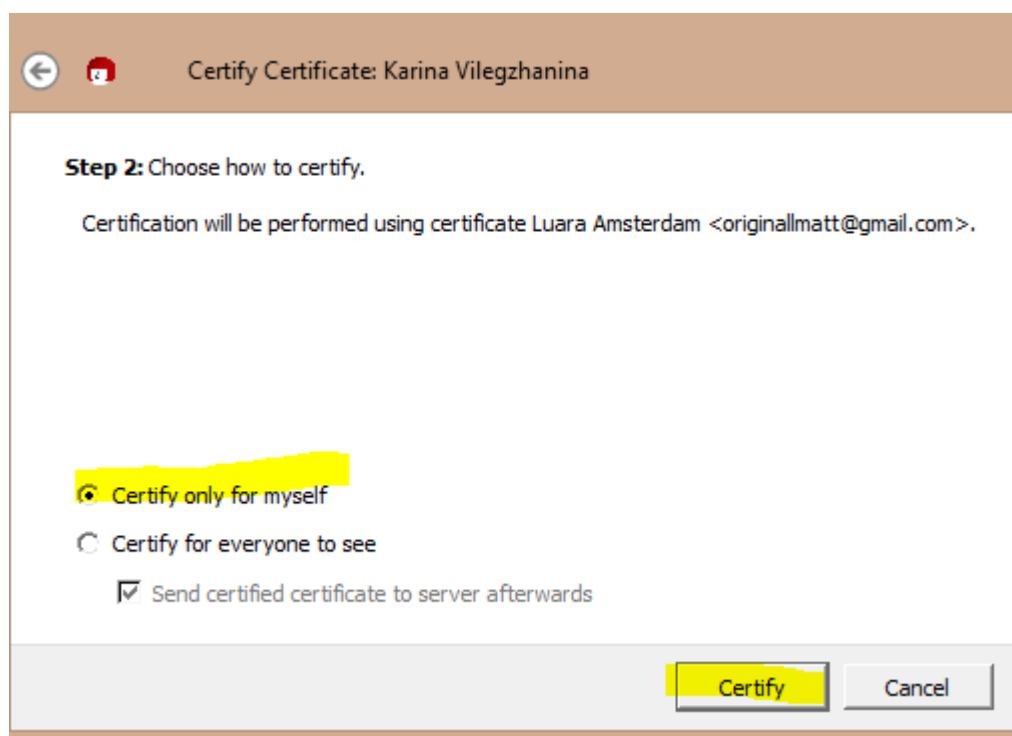
OpenPGP: All operations completed.

sign\_file.txt → sign\_file.txt.gpg: **Signing and encryption succeeded.**

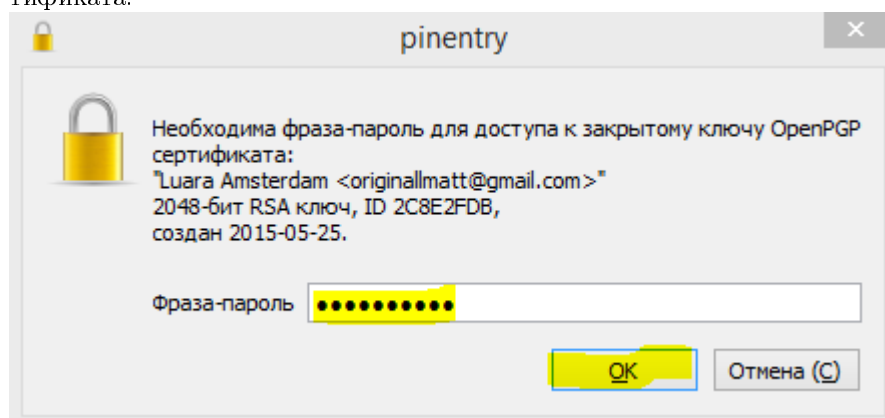
5. Получить чужой сертификат из репозитория  
Скачали сертификат с <https://github.com/vilegzhanina/InfoSecCourse201>,  
файл с данными и файл с сигнатурой (подписью).
6. Импортировать сертификат, подписать его  
Выбираем user ID.



Сертифицируем только для себя.

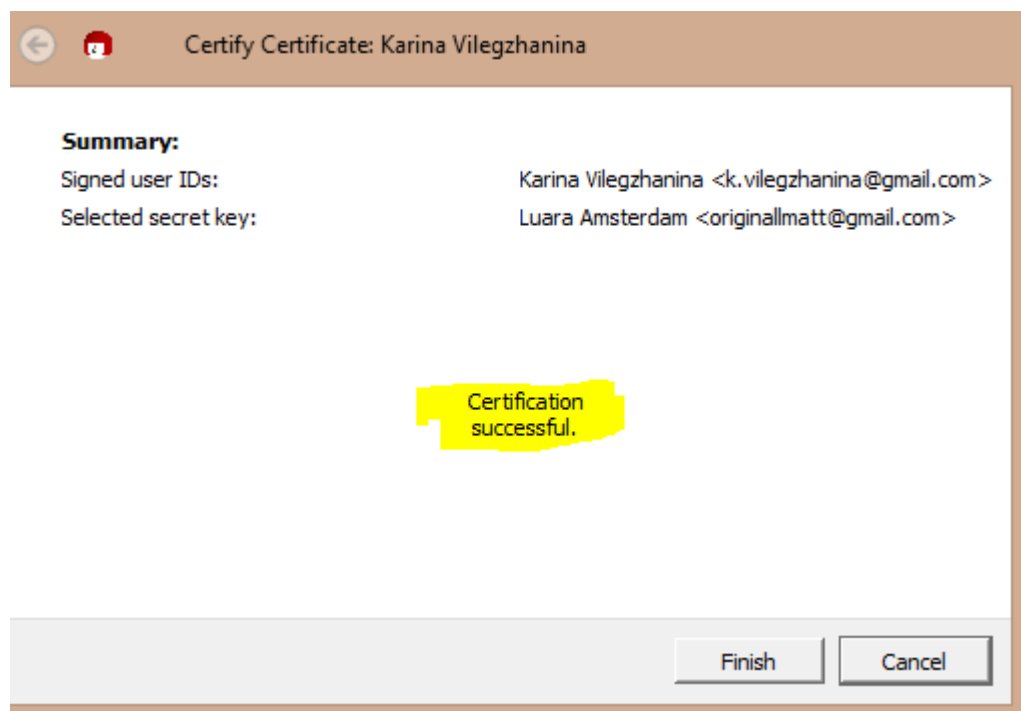


Необходимо ввести фразу-пароль, введенную при формировании сертификата.

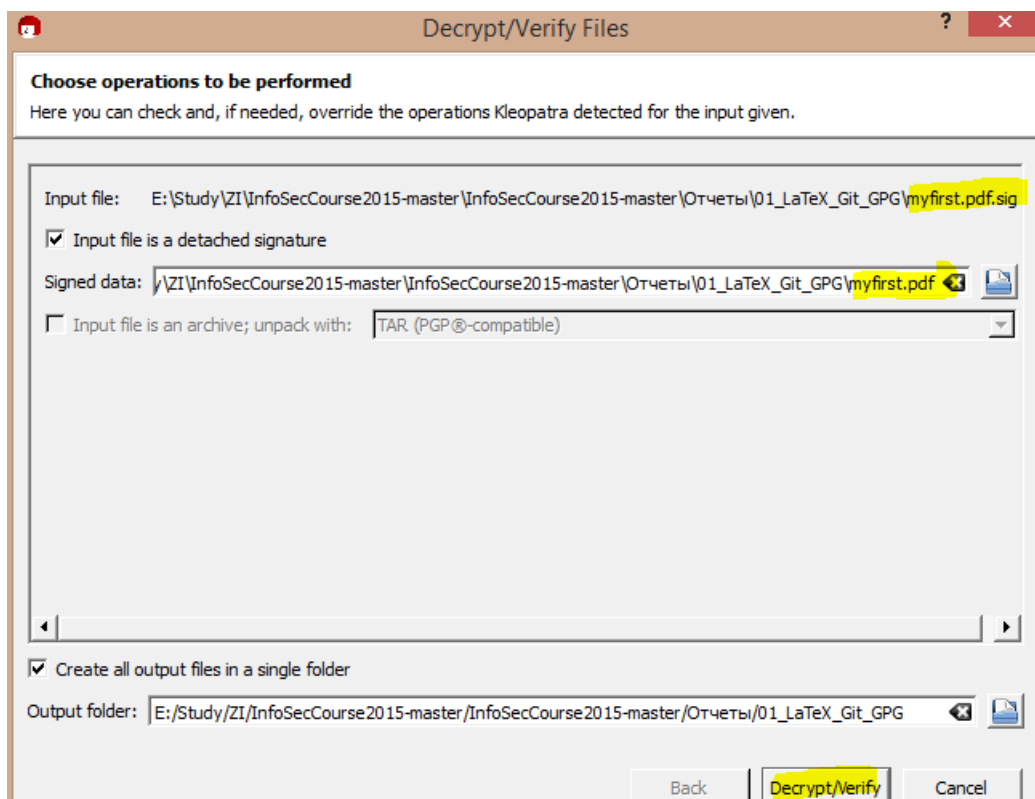


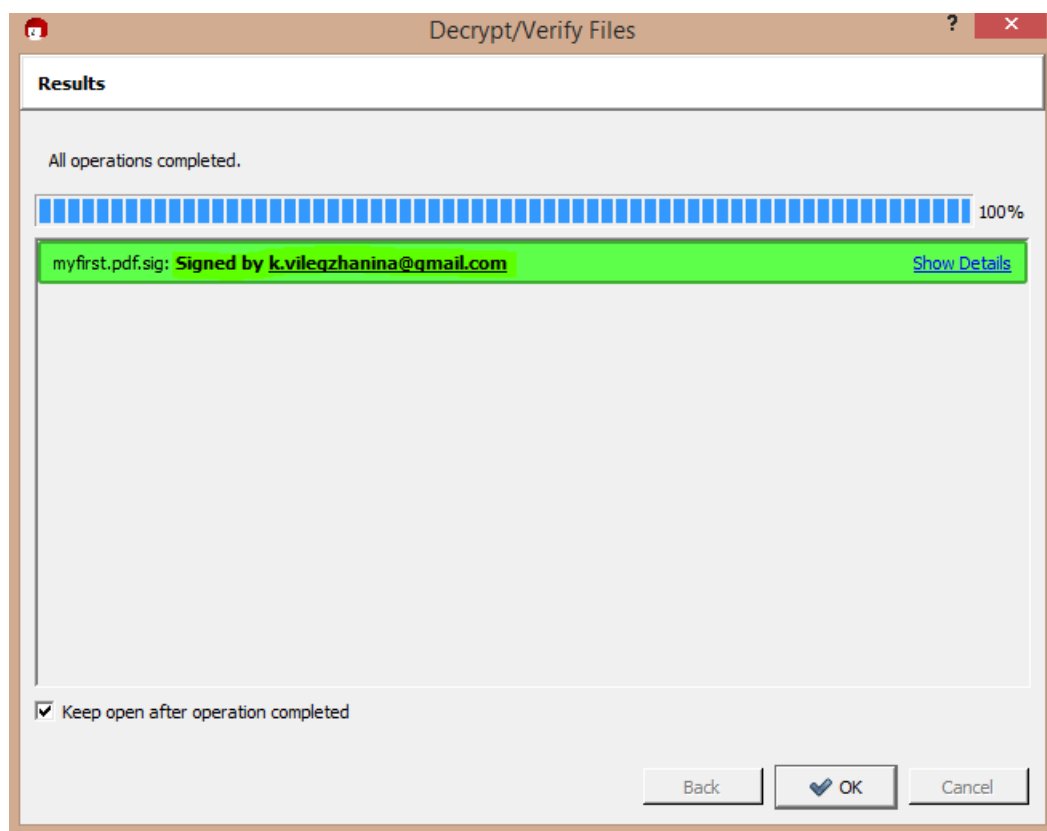
В результате успешно выполнили сертификацию.





7. Проверить подпись  
Верифицируем скаченный файл с данными и файл с подписью.





8. Взять сертификат кого-либо из коллег, зашифровать и подписать для него какой-либо текст, предоставить свой сертификат, убедиться, что ему удалось получить открытый текст, проверить подпись Подписали и зашифровали данные для коллеги (Певцов И.).

Sign/Encrypt Files

### For whom do you want to encrypt?

Please select for whom you want the files to be encrypted. Do not forget to pick one of your own certificates.

All Certificates

Name	E-Mail
Windows Remote Shaman (www.remoteshaman.com)	remoteshaman.com@gr
Pevtsov	huxley92@mail.ru
<b>Luara Amsterdam (test)</b>	<b>originallmatt@gmail.co</b>
<b>Luara Amsterdam</b>	<b>originallmatt@gmail.co</b>
Karina Vilegzhanina	k.vilegzhanina@gmail.co

▼ Add

▲ Remove

Name	E-Mail	Valid From	Valid Until /	Details
Pevtsov	huxley92@mail.ru	2015-05-25		OpenPGP 24

Next

Cancel

### Results

Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

sign\_file.txt → sign\_file.txt.gpg: **Signing and encryption succeeded.**

☒ Keep open after operation completed

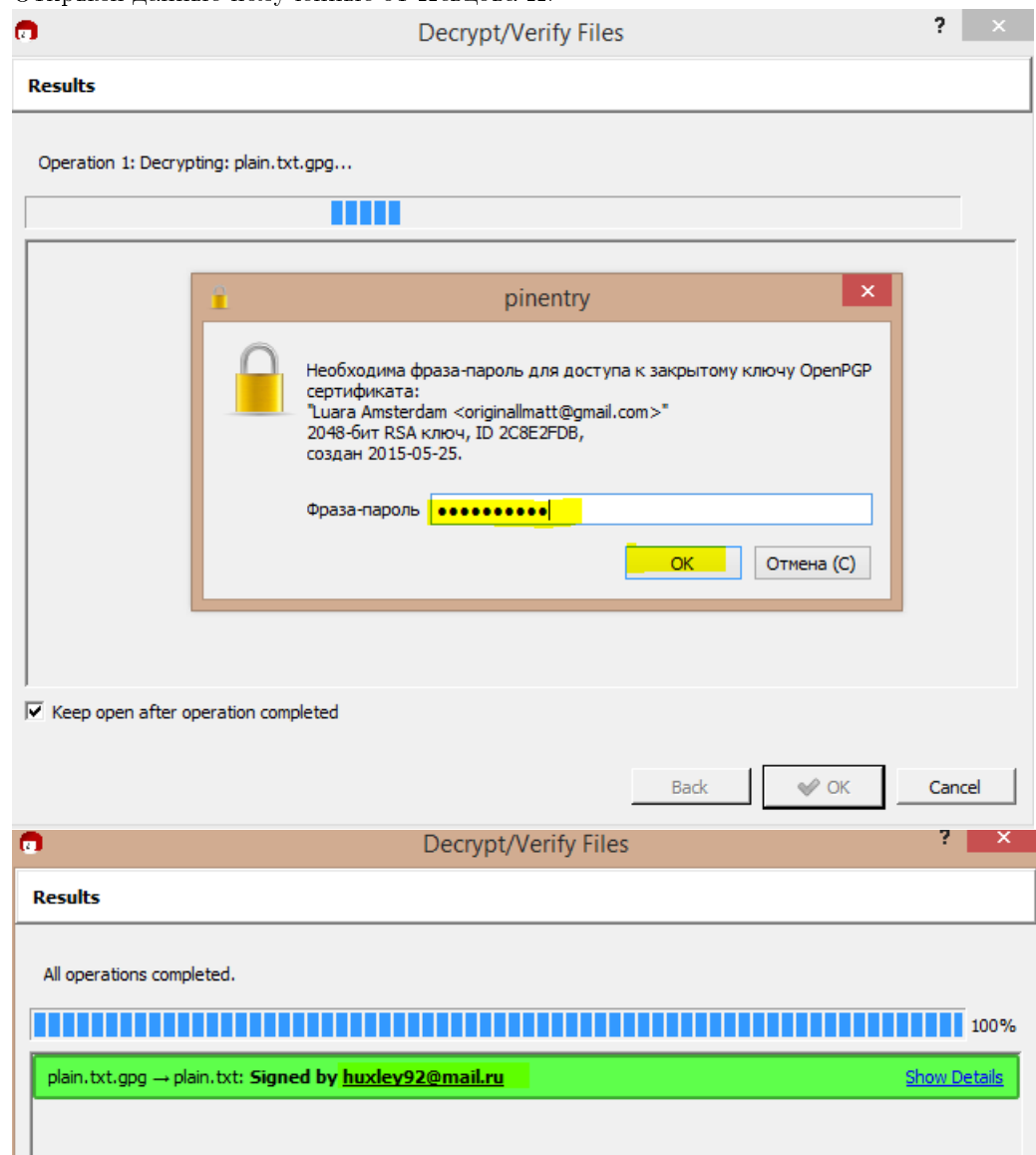
Finish

Cancel

Певцов И. подтвердил успешное открытие данных.

9. Предыдущий пункт наоборот.

Открыли данные полученные от Певцова И.



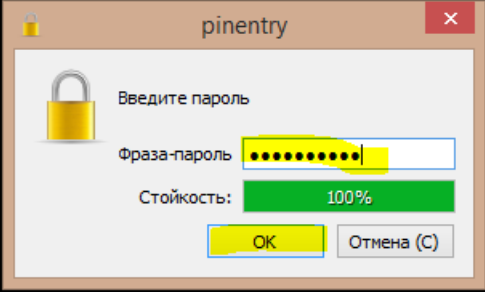
10. Используя GNU Privacy handbook (ссылка в материалах) потренироваться в использовании gpg через интерфейс командной строки, без использования графических оболочек.

Создание пары PGP ключей

```
E:\Study\ZI\Result\3\cmd>gpg --gen-key
gpg (GnuPG) 2.0.27; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Выберите тип ключа:
(1) RSA и RSA (по умолчанию)
(2) DSA и Elgamal
(3) DSA (только для подписи)
(4) RSA (только для подписи)
Ваш выбор? 1
Ключи RSA могут иметь длину от 1024 до 4096 бит.
Какой размер ключа Вам необходим? (2048)
Запрошенный размер ключа - 2048 бит
Выберите срок действия ключа.
  0 = без ограничения срока действия
  <n> = срок действия - n дней
  <n>w = срок действия - n недель
  <n>m = срок действия - n месяцев
  <n>y = срок действия - n лет
Срок действия ключа? (0) 6m
Ключ действителен до: 11/21/15 17:02:06 Russia TZ 2 Standard Time
Все верно? (y/N) y

GnuPG необходимо составить ID пользователя в качестве идентификатора ключа.
Ваше настоящее имя: Luara Amsterdam
Адрес электронной почты: originallmatt@gmail.com
Комментарий: test
Вы выбрали следующий ID пользователя:
  "Luara Amsterdam (test) (originallmatt@gmail.com)"
Сменить (N)Имя, (C)Комментарий, (E)Адрес или (O)Принять/(Q)Выход? O
Для защиты закрытого ключа необходима фраза-пароль.
```



Получение публичного PGP ключа

Шифровка и обмен файлами с использованием публичных ключей

```

E:\Study\ZI\Result\3\cmd>gpg --keyserver keys.gnupg.net --recv-keys 346B72D7
gpg: запрашиваю ключ 346B72D7 с hkp сервера keys.gnupg.net
gpg: DBG: armor-keys-failed <KEY 0x346B72D7 BEGIN
> ->0
gpg: DBG: armor-keys-failed <KEY 0x346B72D7 END
> ->0
gpg: ключ 346B72D7: импортирован открытый ключ "Windows Remote Shaman <www.remoteshaman.com> <GPG key for remoteshaman.com@gmail.com email> <remoteshaman.com@gmail.com>"
gpg: Всего обработано: 1
gpg: импортировано: 1 (RSA: 1)

E:\Study\ZI\Result\3\cmd>gpg -e -r 346B72D7 sign_file.txt
gpg: 6D2314B5: Нет свидетельств того, что данный ключ принадлежит названному пользователю

pub 4096R/6D2314B5 2014-01-19 Windows Remote Shaman <www.remoteshaman.com> <GPG key for remoteshaman.com@gmail.com email> <remoteshaman.com@gmail.com>
Отпечаток главного ключа: 8CC0 592D 17F5 0B9D A625 3324 1590 B040 346B 72D7
Отпечаток подключа: F711 E6D7 034B 4D58 B324 DFB2 6B94 B164 6D23 14B5

Нет уверенности в том, что ключ принадлежит человеку, указанному в ID пользователя ключа. Если Вы ТОЧНО знаете, что делаете, можете ответить на следующий вопрос утвердительно.

Все равно использовать данный ключ? (y/N) y

```

Вывод списка ключей.

```

E:\Study\ZI\Result\3\cmd>gpg --list-keys
C:/Users/Laura/AppData/Roaming/gnupg/pubring.gpg
-----
pub 2048R/2C8E2FDB 2015-05-25
uid [абсолютное] Luara Amsterdam <originallmatt@gmail.com>

pub 2048R/391EA659 2015-02-08
uid [ полное ] Karina Vilegzhanina <k.vilegzhanina@gmail.com>

pub 2048R/9CEC5726 2015-05-25 [срок действия истекает: 2015-11-21]
uid [абсолютное] Luara Amsterdam (test) <originallmatt@gmail.com>
sub 2048R/3EDF1F75 2015-05-25 [срок действия истекает: 2015-11-21]

pub 4096R/346B72D7 2014-01-19
uid [неизвестно] Windows Remote Shaman <www.remoteshaman.com> <GPG key for remoteshaman.com@gmail.com email> <remoteshaman.com@gmail.com>
sub 4096R/6D2314B5 2014-01-19

```

Для расшифрования полученных данных необходимо знать приватный ключ.

```

E:\Study\ZI\Result\3\cmd>gpg -d sign_file.txt.gpg > new_file.txt
gpg: зашифровано 4096-битным ключом RSA, с ID 6D2314B5, созданным 2014-01-19
"Windows Remote Shaman <www.remoteshaman.com> <GPG key for remoteshaman.com@gmail.com email> <remoteshaman.com@gmail.com>"
gpg: свой расшифровки: No secret key

```

Экспорт/импорт PGP (GnuPG) ключей

Приведённая выше команда выполнит экспорт публичного PGP ключа (с ИД 346B72D7) в файл 346B72D7.public.gpg в двоичном (binary) формате, но это может быть неудобно при его пересылке например в теле сообщения по электронной почте. Мы можем выполнить экспорт ключа в ASCII формате добавив флаг `--armor` (или просто `-a`).

```

E:\Study\ZI\Result\3\cmd>gpg --export --armor --output 9CEC5726.public.gpg 9CEC5726
E:\Study\ZI\Result\3\cmd>gpg --export-secret-keys -a --output 9CEC5726.private.gpg 9CEC5726

```

Вывод:

В ходе данной лабораторной работы мы научились создавать сертификаты, шифровать файлы и ставить ЭЦП. Использовались инструменты графическая оболочка Kleopatra, утилита gpg.