

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Кафедра Компьютерных Систем и Программных Технологий

ОТЧЕТ

по лабораторной работе №3

Тема: «Программа для шифрования и подписи GPG, пакет Gpg4win»

Дисциплина: «Методы и средства защиты информации»

Выполнил: студент гр. 53501/2

Пономарев М.А.

Преподаватель

Вылегжанина К.Д.

Санкт-Петербург

2015

Содержание

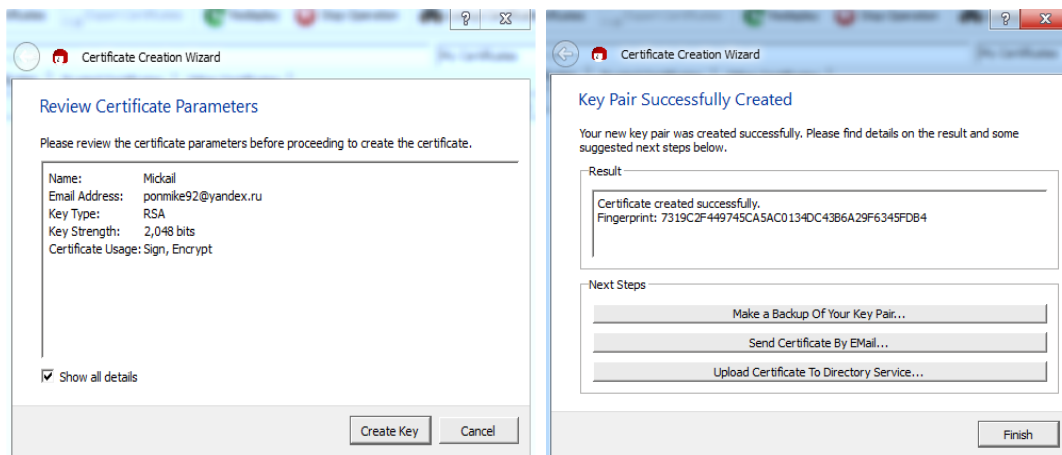
1	Задание	2
2	Выполнение	3
2.1	Создать ключевую пару OpenPGP (File → New Certificate)	3
2.2	Экспортировать сертификат (File → Export Certificate)	3
2.3	Поставить ЭЦП на файл (File → Sign/Encrypt Files)	4
2.4	Получить чужой сертификат из репозитория, файл с данными и файл с сигнатурой	4
2.5	Импортировать сертификат, подписать его	5
2.6	Проверить подпись	6
2.7	Взять сертификат кого-либо из коллег, зашифровать и подписать для него какой-либо текст, предоставить свой сертификат, убедить- ся, что ему удалось получить открытый текст, проверить подпись . .	6
2.8	Используя GNU Privacy handbook (ссылка в материалах) потрени- роваться в использовании gpg через интерфейс командной строки, без использования графических оболочек.	7
3	Выводы	10

1 Задание

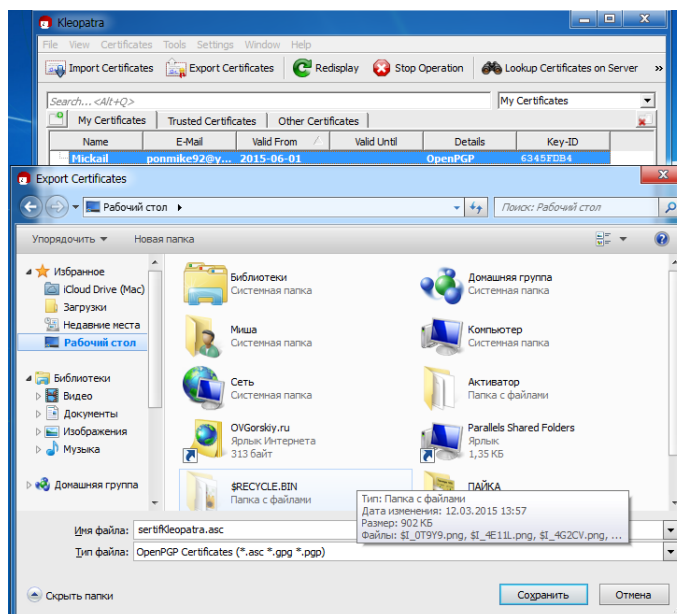
- а) Изучить документацию, запустить графическую оболочку Kleopatra
- б) Создать ключевую пару OpenPGP (File → New Certificate)
- в) Экспортировать сертификат (File → Export Certificate)
- г) Поставить ЭЦП на файл (File → Sign/Encrypt Files)
- д) Получить чужой сертификат из репозитория, файл с данными и файл с сиг-
натурой
 - е) Импортировать сертификат, подписать его
 - ж) Проверить подпись
 - з) Взять сертификат кого-либо из коллег, зашифровать и подписать для него
какой-либо текст, предоставить свой сертификат, убедиться, что ему удалось полу-
чить открытый текст, проверить подпись
 - и) Предыдущий пункт наоборот
 - к) Используя GNU Privacy handbook (ссылка в материалах) потренироваться в
использовании gpg через интерфейс командной строки, без использования графиче-
ских оболочек.

2 Выполнение

2.1 Создать ключевую пару OpenPGP (File → New Certificate)

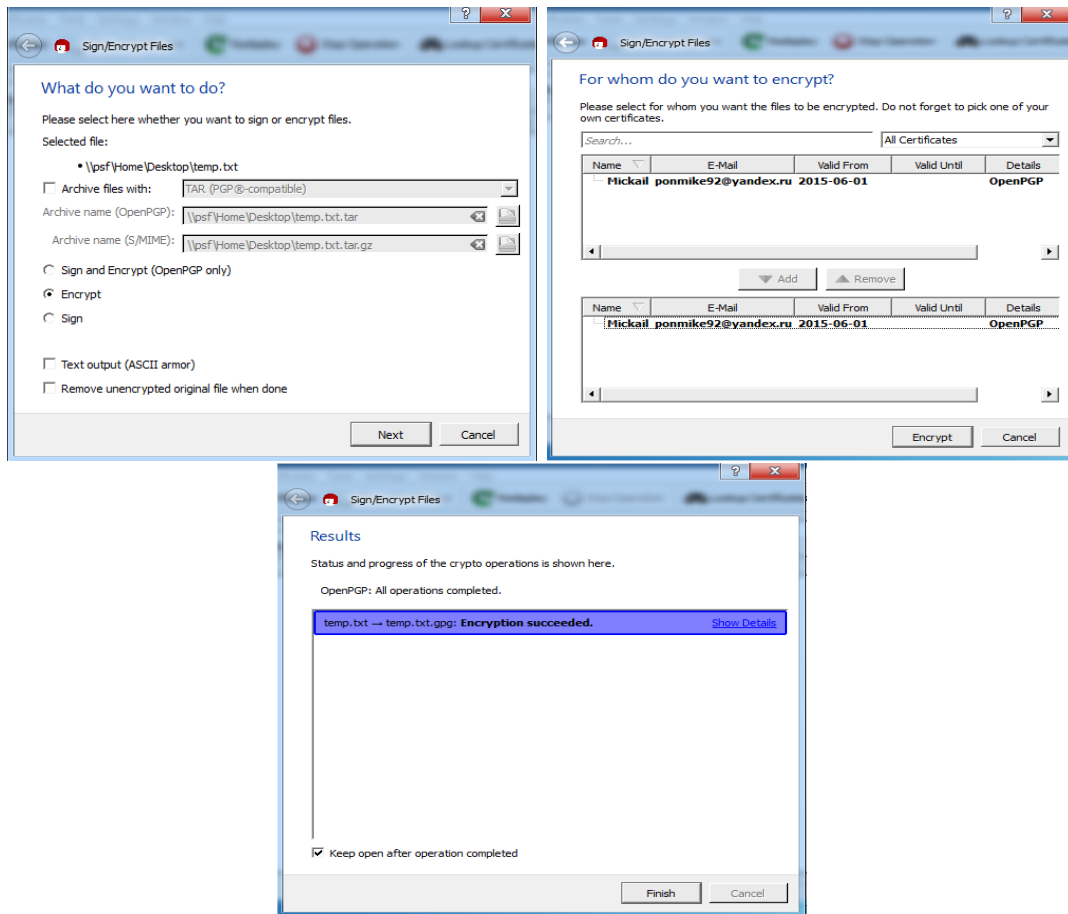


2.2 Экспортировать сертификат (File → Export Certificate)



2.3 Поставить ЭЦП на файл (File → Sign/Encrypt Files)

Создадим файл «temp.txt», чтобы впоследствии зашифровать его.



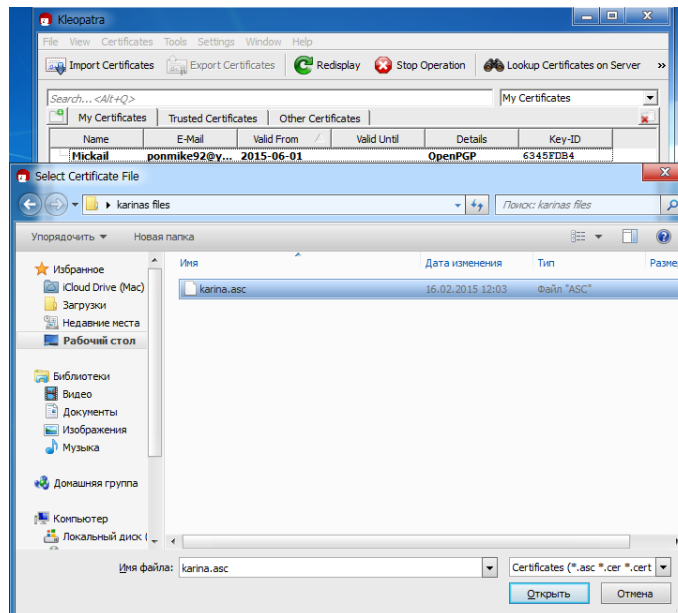
В ходе шифрования нас попросят ввести фразу-пароль.

2.4 Получить чужой сертификат из репозитория, файл с данными и файл с сигнатурой

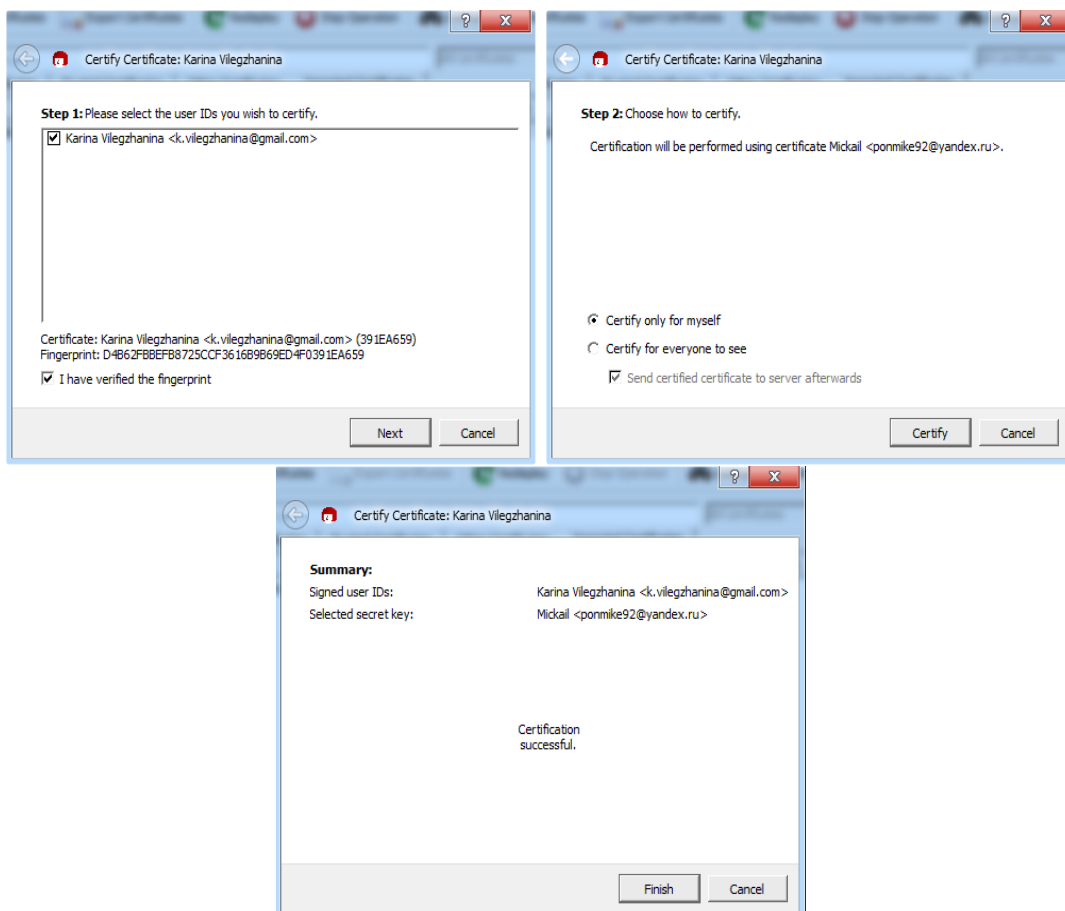
Name	Date Modified
files	Today 14:19
karina.asc	16 Feb 2015 11:03
myfirst.pdf	16 Feb 2015 11:03
myfirst.pdf.sig	16 Feb 2015 11:03

2.5 Импортировать сертификат, подписать его

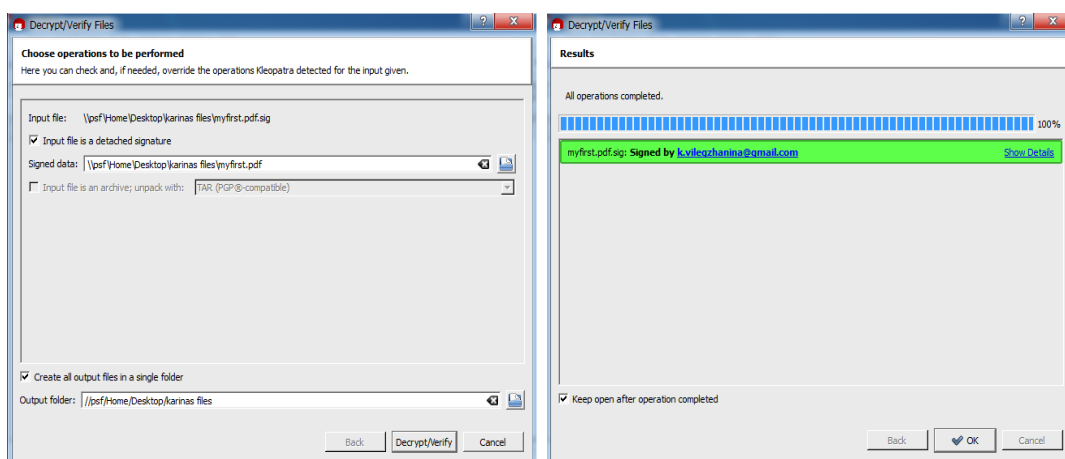
Импортируем сертификат:



Подпишем сертификат:

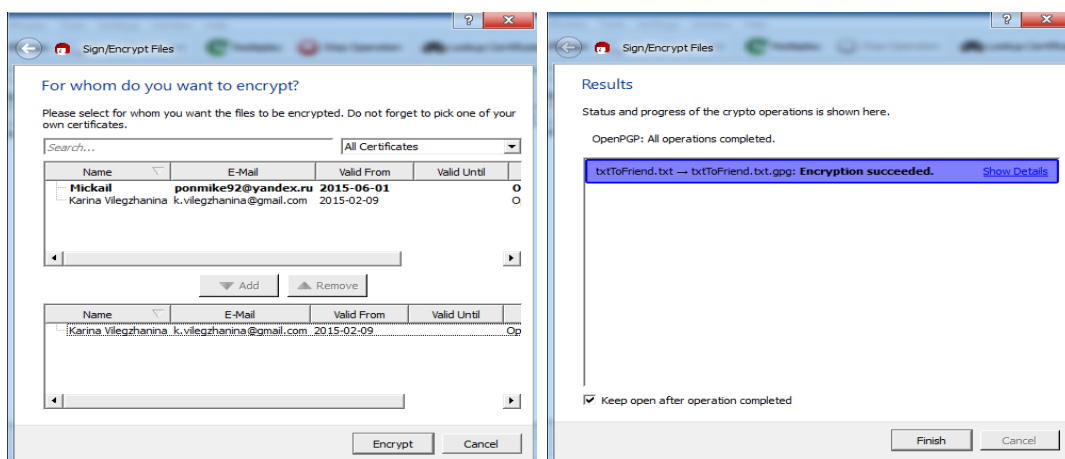


2.6 Проверить подпись



2.7 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

Сертификат был взят преподавательский. Был создан файл «txtToFriend.txt» для дальнейшего шифрования.



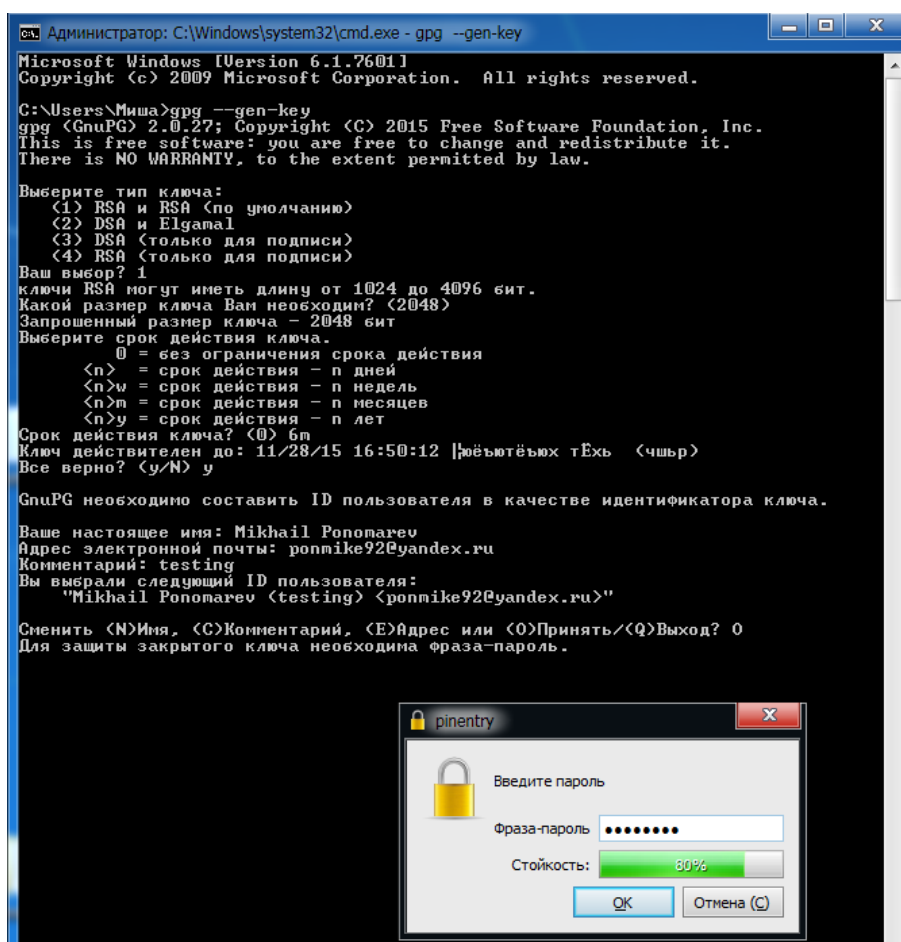
На компьютере Олега Воробьева проверили подпись и открыли исходный текст.

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

Были изучены следующие команды:

- `--gen-key` — создание новой пары ключей
- `--sign` — создает подпись для указанных файлов
- `--encrypt` — указывает на то, что данные надо зашифровать
- `--symmetric` — используется для шифрования файла
- `--decrypt` — расшифровывает указанные файлы и сохраняет результат
- `--verify` — проверяет подписи для указанных файлов
- `--list-keys` — выводит список всех открытых ключей
- `--delete-key` — удаляет открытый ключ из списка.
- `--export` (`--import`) — экспорт/импорт ключей

Создадим пару GPG ключей, для этого наберём команду в терминале «`gpg --gen-key`» в той папке, в которой мы хотим создать ключ.



Выведем список доступных ключей, для этого наберём команду «`gpg --list-keys`»


```
Администратор: C:\Windows\system32\cmd.exe

C:\Users\Миша>gpg --list-keys
C:/Users/Миша/AppData/Roaming/gnupg/pubring.gpg
-----
pub   2048R/6345FDB4 2015-06-01
uid   [абсолютное] Mickail <ponmike92@yandex.ru>

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

pub   2048R/1AC40439 2015-06-01 [срок действия истекает: 2015-11-28]
uid   [абсолютное] Mikhail Ponomarev (testing) <ponmike92@yandex.ru>
sub   2048R/9AA5FC17 2015-06-01 [срок действия истекает: 2015-11-28]
```

Экспортируем ключ, наберём команду «gpg –export -a Mickail»

```
C:\Users\Миша>gpg --export -a Mickail
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFUsNXkBCADEMaRaEWUrsDfD1z3PdHfZOWMbXWouBQib0TILKZ1jUBzawF9t
j8pkDZ/ZiXYT29qoABxg3bKlj08CtdlniizC/IO+UE18Ifbfaih62bGKq3Nom1YZ
8Pcf8avc/ikU1PwFtrjb9YFvEoq/10L/NuJKwzmW+fU+ISP1CDh2Ud2HP4mfUw4/
OJ9EOLMS14TUNbJSj3HC5AidpyC44C4rp7IocEPQUBMd0ITxIhOR30BibuygArsr
EWC/unM9I8UUbBFM8h7HHj4+hRI5UN7K003KLPJUd970zUjnYR7M1lsz8CNQxMYy
P65tSmTawrkR6Kb2B9/dbQbUzD1NA5K4JKWTABEBAAGOHU1pY2thaWwgPHBubm1p
a2U5MkBSYUW5kZKguenU+iQE5BBMBCAAjBQJUBDU5AhsPBwsJCAcDAgEGFQgCCQoL
BBYCAwECHgECF4AAcGkQQ7ain2NF/bSfrgf/f+A3J+RGnu4fMyttgq0e/5o+YoQB
6erTwgZGULtK6omDOYGAEBLLXkiFtj28LOUYwUxaitFai0lalvFEK694buYuhUUv
40/si88K3ghopovULpH4Y4tIyuhaNctkG78Fmh5Y90o7ysvFUt2+vv20hxT0AuUG
4BWhq+xsS0f3l6kHngSRHU1v4U9qfDdiuI55eqnMgJrrLwI8Kn9fyxntTlUkcZ+q
Lu/NTA56170fAGej+pi5UKIYoxvge7SDidFcbJCI GHEpUGYfHSSRTkofQgCft3a
hMGRnfRHH6FjHYyW27EdRK1Uxoraw69i57UynnaiJqk8K46UwHwgQCS PQ==
=EbYC
-----END PGP PUBLIC KEY BLOCK-----
```

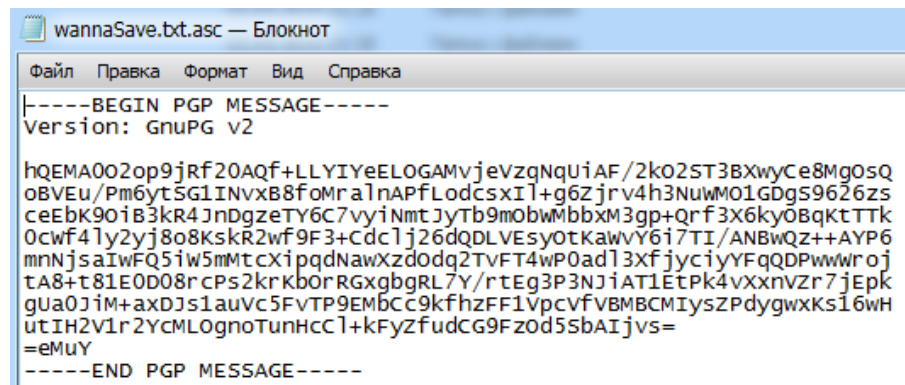
Для того, чтобы ключ можно было использовать на другой машине произведём вывод в файл командой «gpg –export -a Mickail > Mickail.asc»

```
C:\Users\Миша>gpg --export -a Mickail > Mickail.asc
```

Зашифруем файл «wannaSave.txt» командой «gpg -ea -r Mickail wannaSave.txt»

```
C:\Users\Миша>gpg -ea -r Mickail wannaSave.txt
```

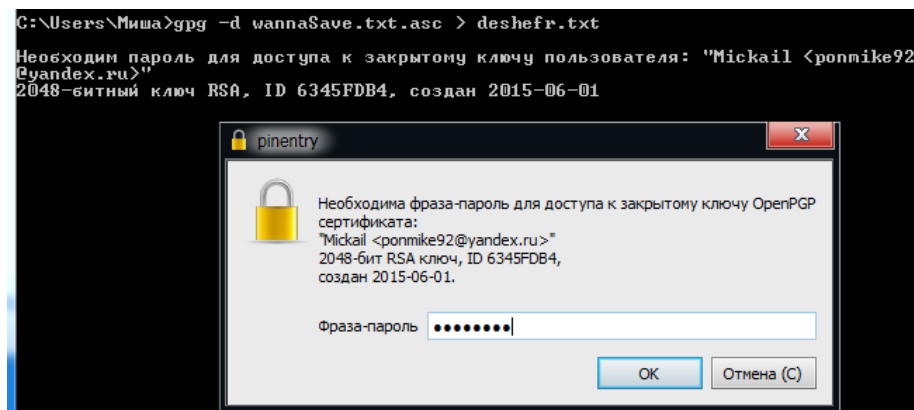
В результате получим зашифрованный файл «wannaSave.txt.asc» со следующим содержанием



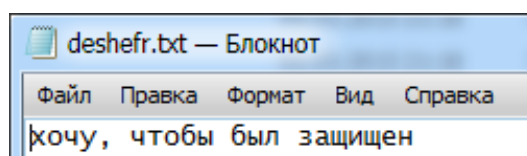
```
wannaSave.txt.asc — Блокнот
Файл  Правка  Формат  Вид  Справка
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA002op9jRf20AQf+LLYIYeELOGAMvjevzqNquiAF/2ko2ST3BXwyCe8MgoSQ
oBVEu/Pm6yt5G1INvx88fomralnAPfLodCsxI1+g6Zjrv4h3NuWM01GDgs9626zs
ceEbK90iB3kR4JnDgzeTY6C7vyiNmtJyTb9m0bWmbbXm3gp+Qrf3X6ky0BqktTTk
0cwf41y2yj8o8KskR2wf9F3+Cdc1j26dQDLVEsyotKawvY6i7TI/ANBwQz++AYP6
mnNjsaIwFQ5iw5mMtCXipqdNawXzdodg2TvFT4wP0ad13xfjyciyyFqQDPwwroJ
tA8+t81E0D08rcPs2krKbOrRGxgbgRL7Y/rTEg3P3NjiAT1EtPk4vxxnVZr7jEpK
gUa0JiM+axDJs1auVc5FvTP9EMbCC9kfHzFF1VpcvfVMBMCMiysZPdygwxks16wH
utIH2V1r2YcMLognoTunHccl+kFyzfudCG9Fz0d5SbAIjvs=
=eMuY
-----END PGP MESSAGE-----
```

Расшифруем полученный файл командой «`gpg -d wannaSave.txt.asc > deshefr.txt`»



Получаем расшифрованный файл с исходным содержимым.



3 Выводы

В ходе выполнения лабораторной работы была изучена программа Kleopatra, используемая для шифрования и подписи GPG. Познакомился с возможностями шифрования с помощью терминала. Появилось представление об электронной подписи файла, ключа и шифрования в целом.