

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
Федоров Е.М.

Преподаватель
Вылегжанина К.Д.

Санкт-Петербург
2015

Содержание

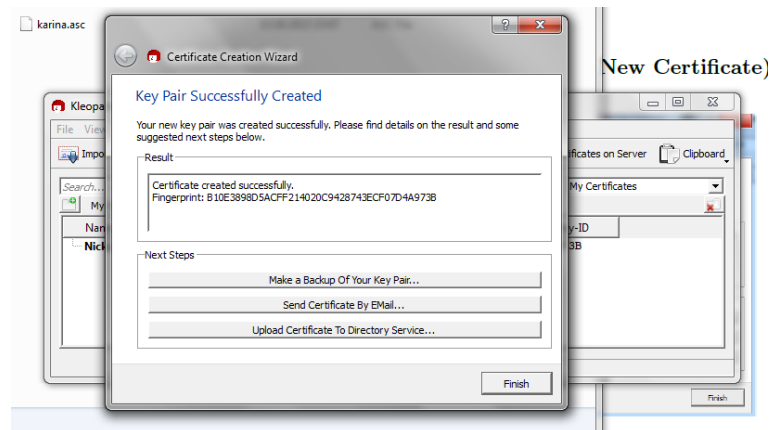
1	Задание	2
2	Выполнение	3
2.1	Создать ключевую пару OpenPGP (File → New Certificate)	3
2.2	Поставить ЭЦП на файл (File → Sign/Encrypt Files)	4
2.3	Получить чужой сертификат из репозитория, файл с данными и файл с сигнатурой	4
2.4	Импортировать сертификат, подписать его	5
2.5	Проверить подпись	6
2.6	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	6
2.7	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.

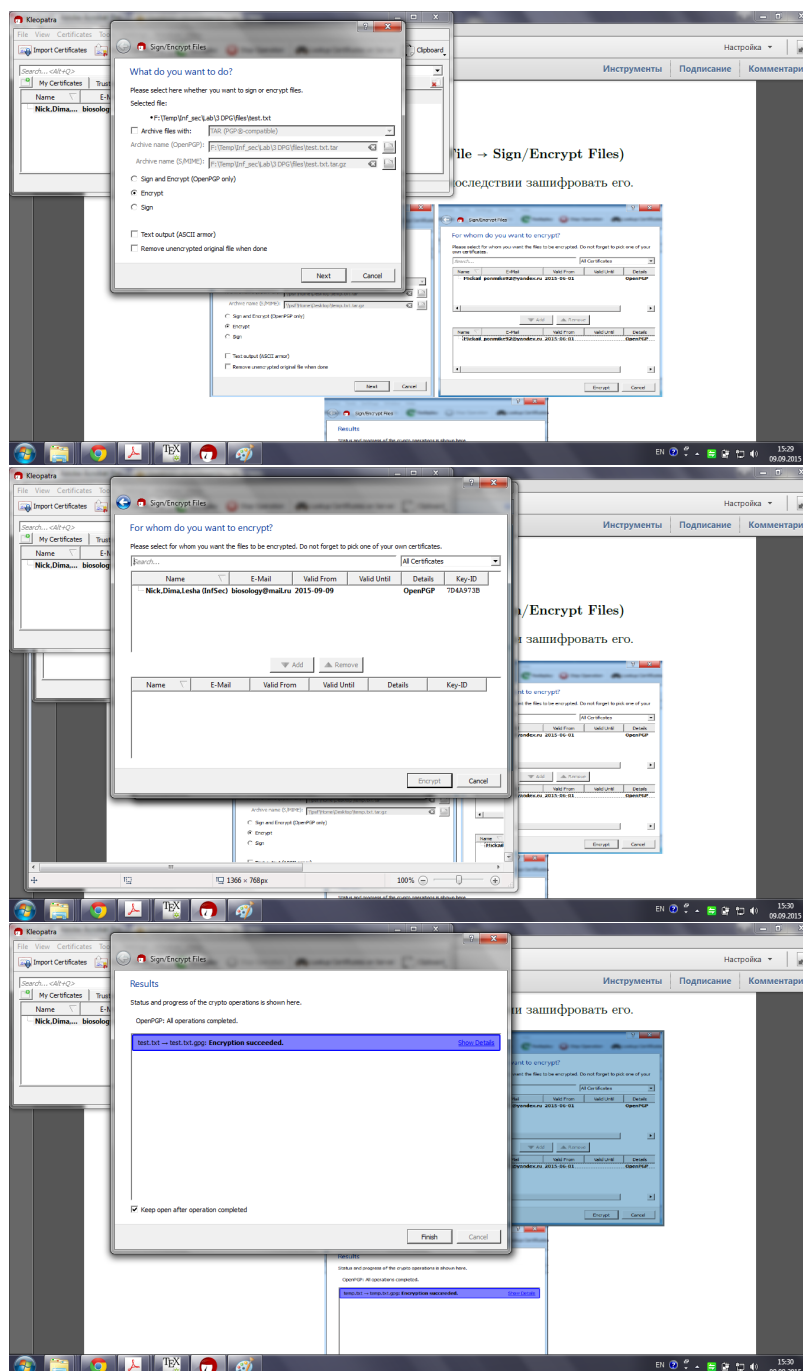
2 Выполнение

2.1 Создать ключевую пару OpenPGP (File → New Certificate)



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

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

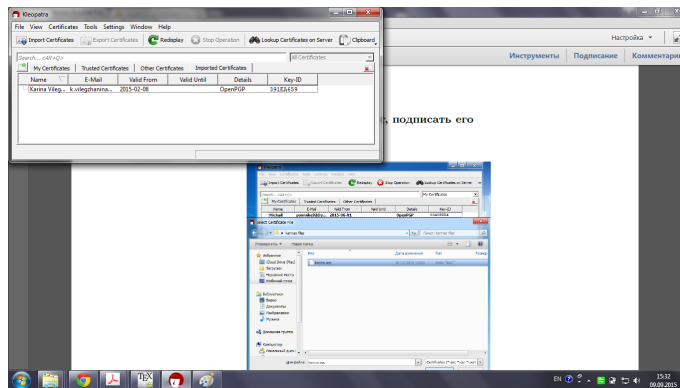


В ходе шифрования нас попросят ввести фразу-пароль.

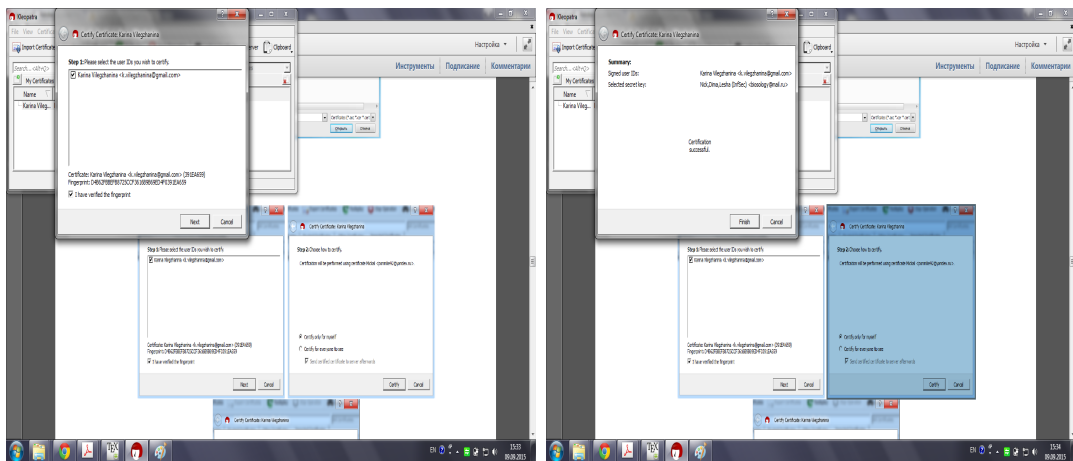
2.3 Получить чужой сертификат из репозитория, файл с данными и файл с сигнатурой

2.4 Импортировать сертификат, подписать его

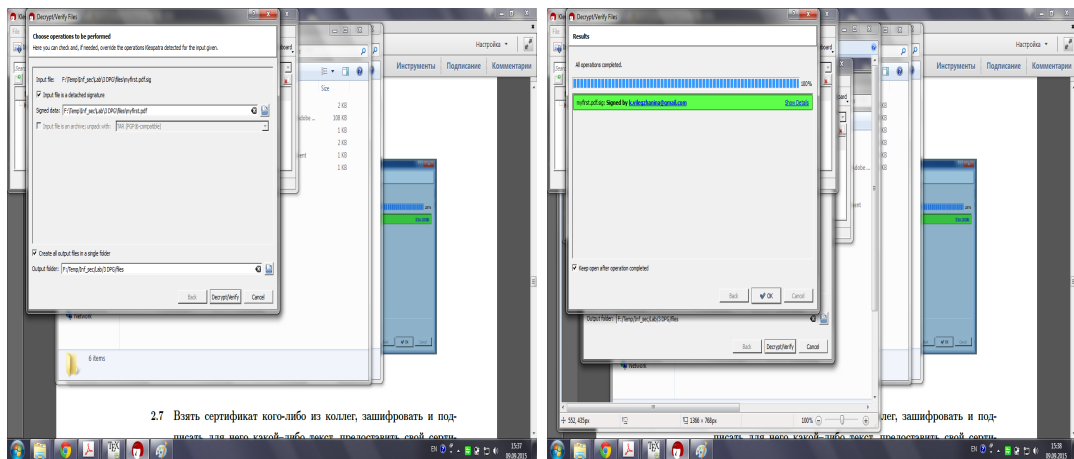
Импортируем сертификат:



Подпишем сертификат:



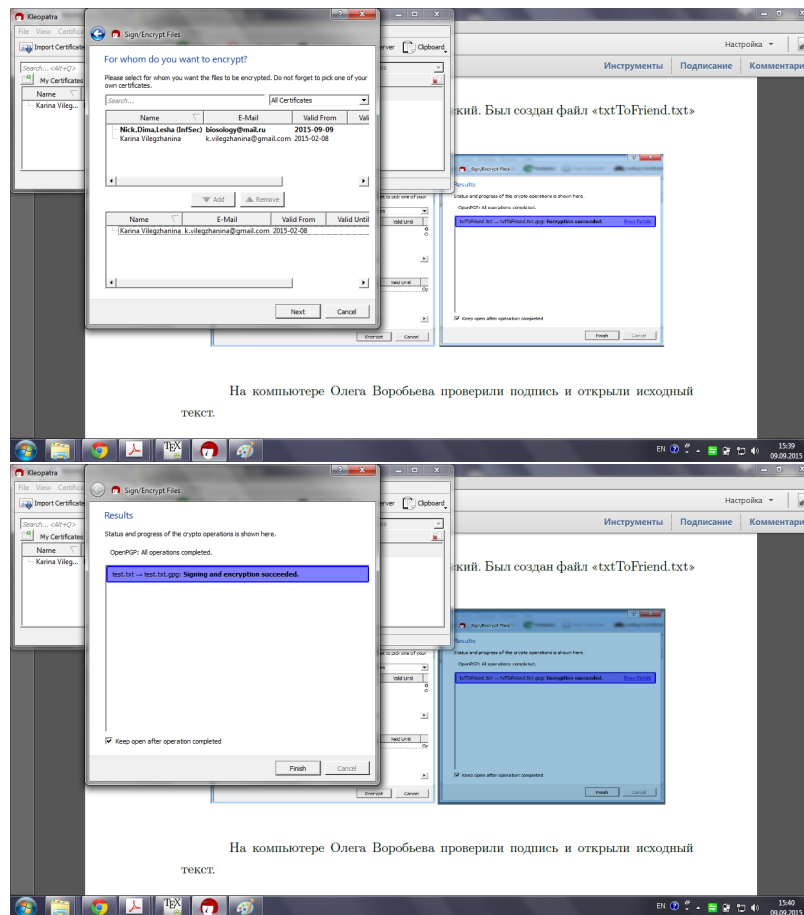
2.5 Проверить подпись



2.6 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. Для дальнейшего шифрования был использован файл «test.txt».

На другом компьютере проверили подпись и открыли исходный текст.



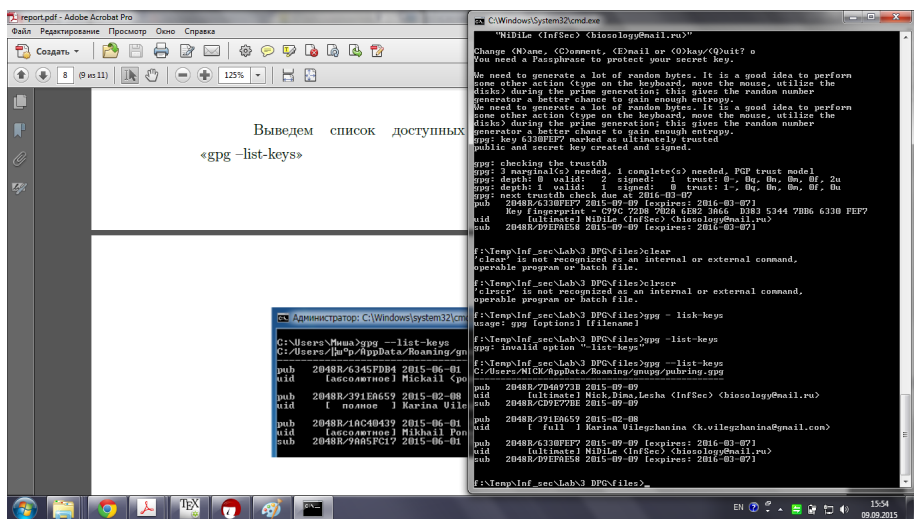
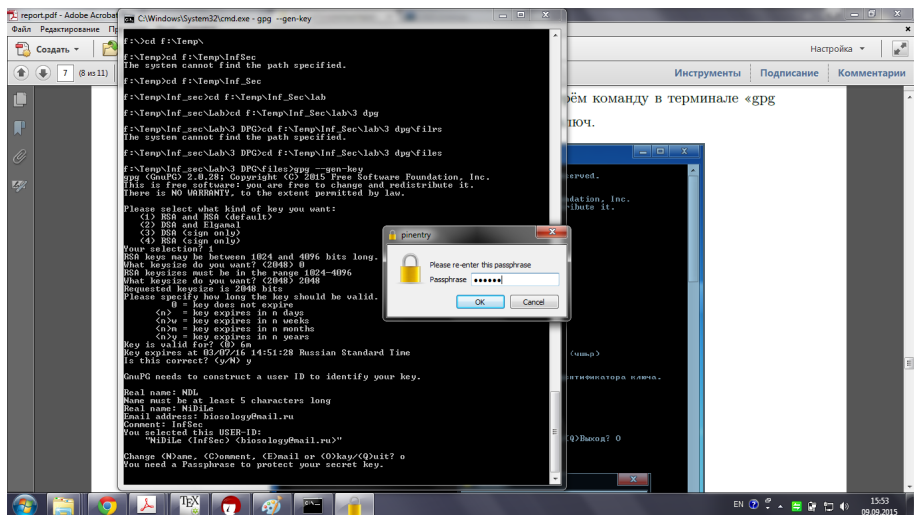
2.7 Используя GNU Privacy handbook (ссылка в материалах) потренироваться в использовании gpg через интерфейс командной строки, без использования графических оболочек.

Были изучены следующие команды:

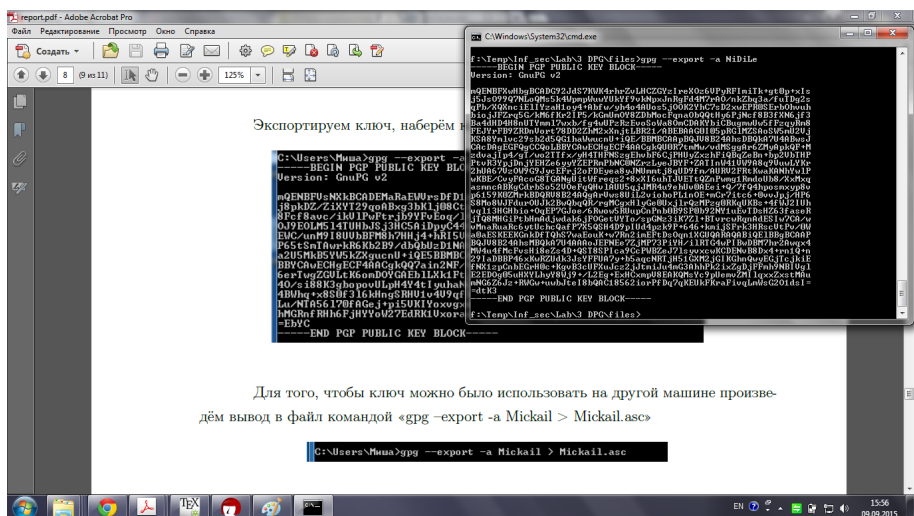
- `-gen-key` — создание новой пары ключей
- `-sign` — создает подпись для указанных файлов
- `-encrypt` — указывает на то, что данные надо зашифровать
- `-symmetric` — используется для шифрования файла
- `-decrypt` — расшифровывает указанные файлы и сохраняет результат
- `-verify` — проверяет подписи 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`»



Экспортируем ключ



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

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.