САНКТ-ПЕТЕРБУРГСИЙ 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»

Выполнили: студенты гр. 53501/2
Майоров А.П.
Ломтев Д.С.
Хазан Н.А.

Преподаватель
Вылегжанина К.Д.

Санкт-Петербург
2015

Содержание

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 сигнатурой

е) Импортировать сертификат, подписать его

ж) Проверить подпись

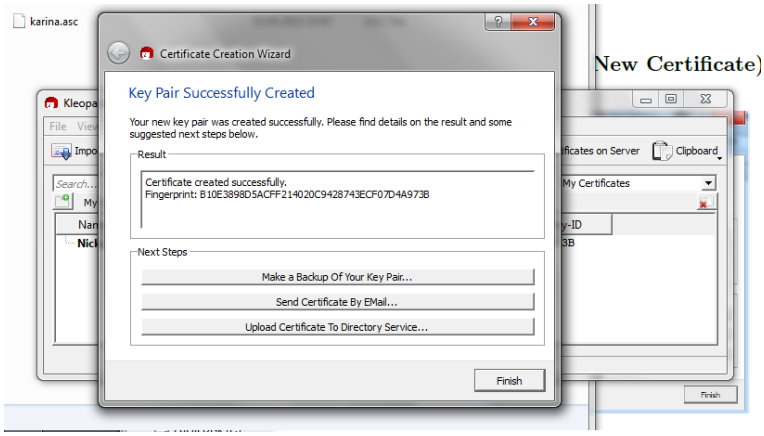
з) Взять сертификат кого-либо из коллег, зашифровать и подписать для него какой–либо текст, предоставить свой сертификат, убедиться, что ему удалось получить открытый текст, проверить подпись

и) Предыдущий пункт наоборот

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

2 Выполнение

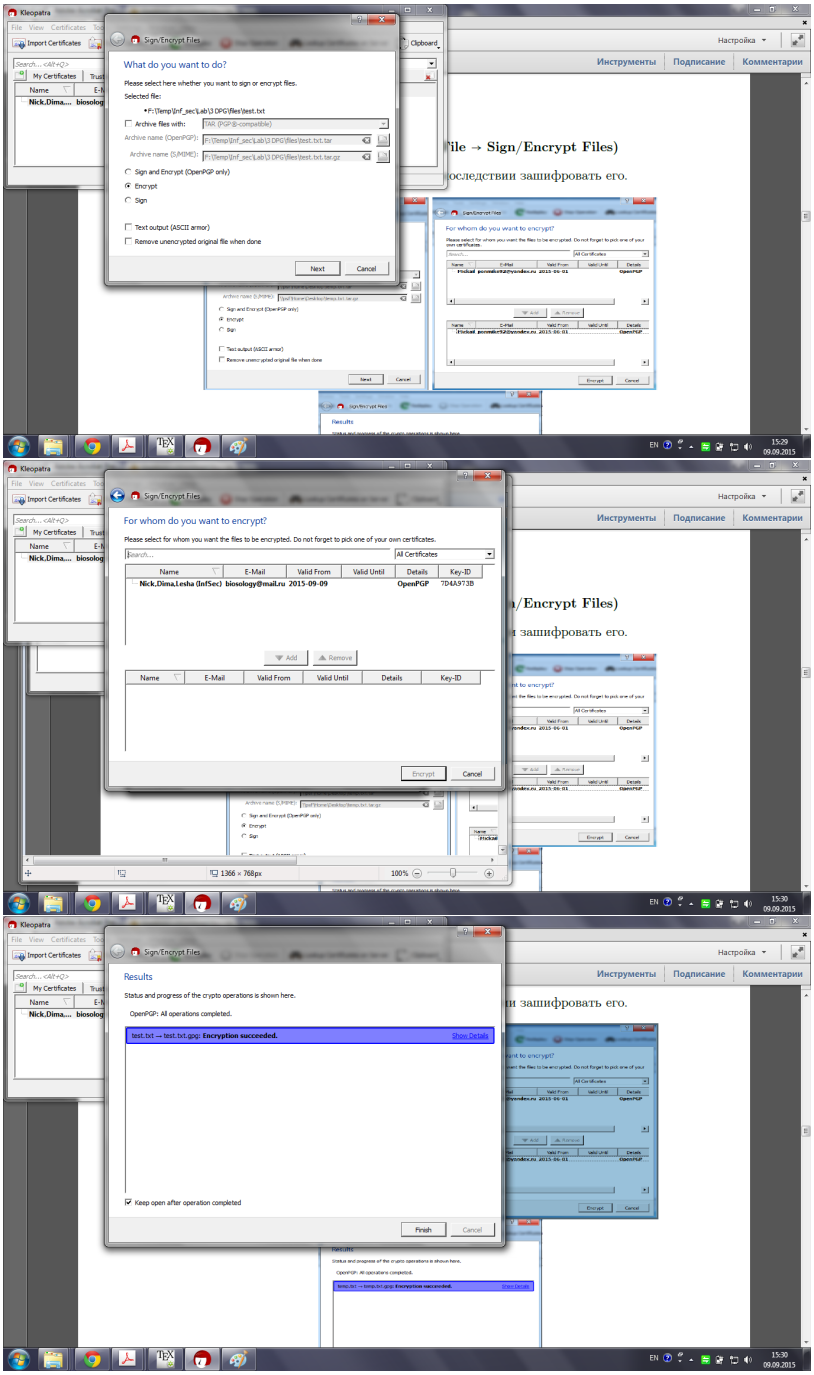
2.1 Создать ключевую пару OpenPGP (File → New Certificate)



New Certificate)

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

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

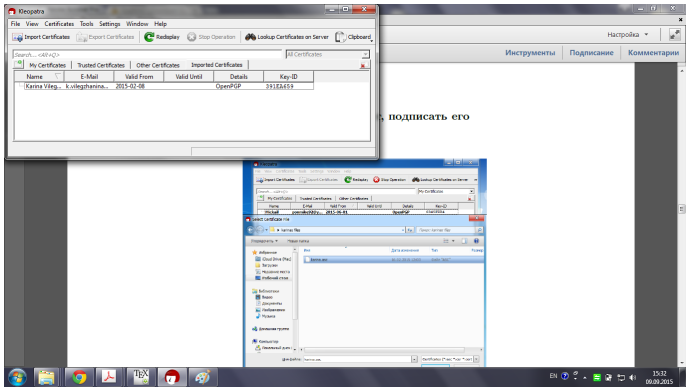


В ходе шифрования нас попросят ввести фразу–пароль.

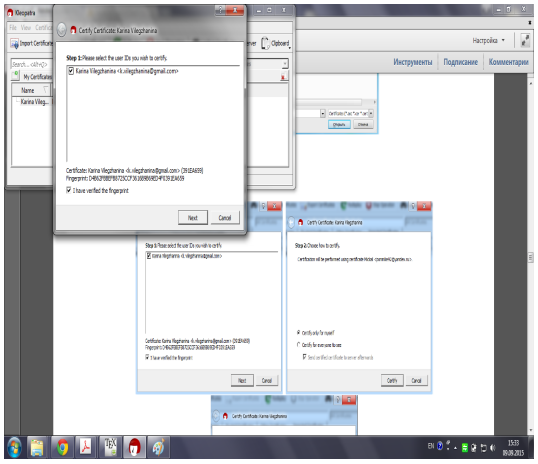
2.3 Получить чужой сертификат из репозитория, файл с данными и файл с сигнатурой

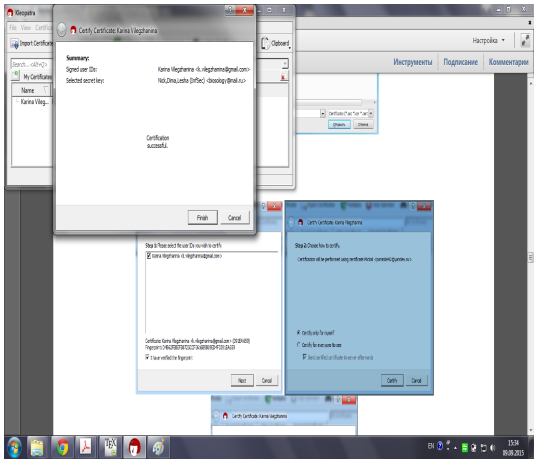
2.4 Импортировать сертификат, подписать его

Импортируем сертификат:

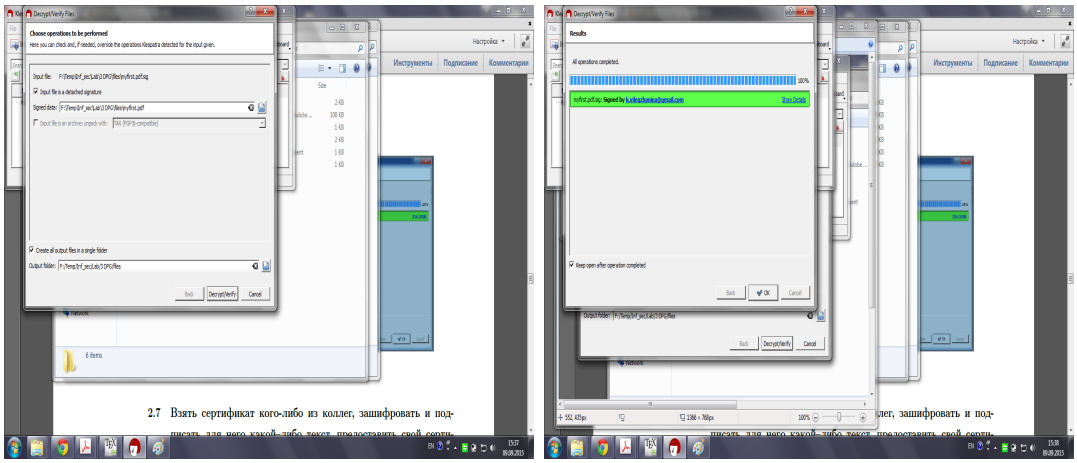


Подпишем сертификат:





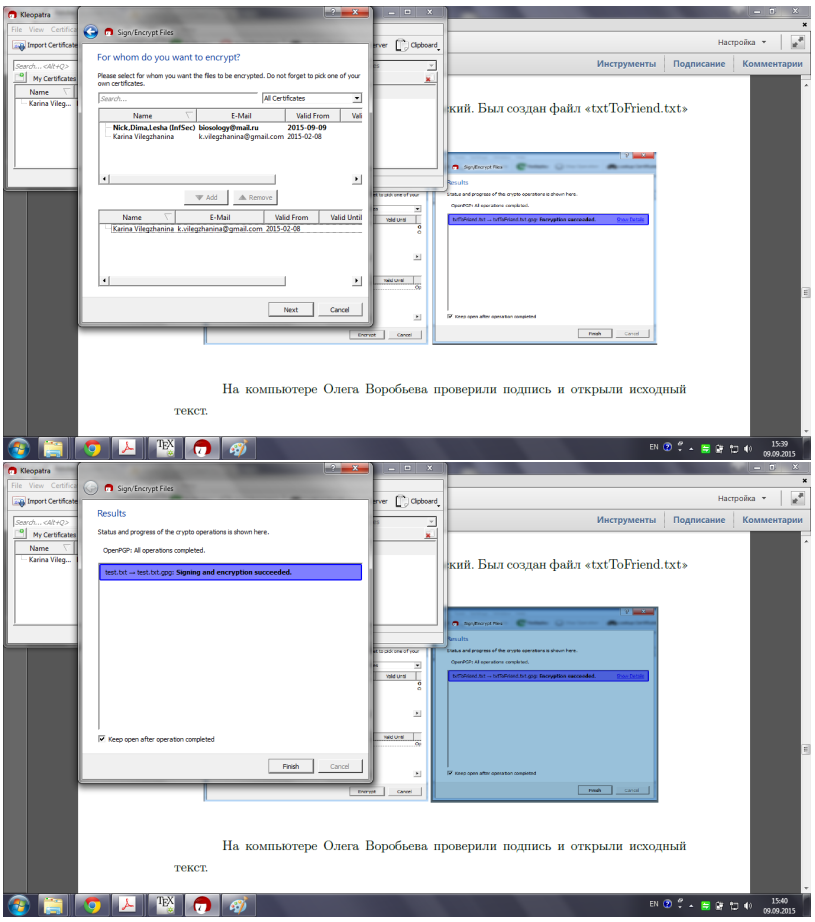
2.5 Проверить подпись



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.



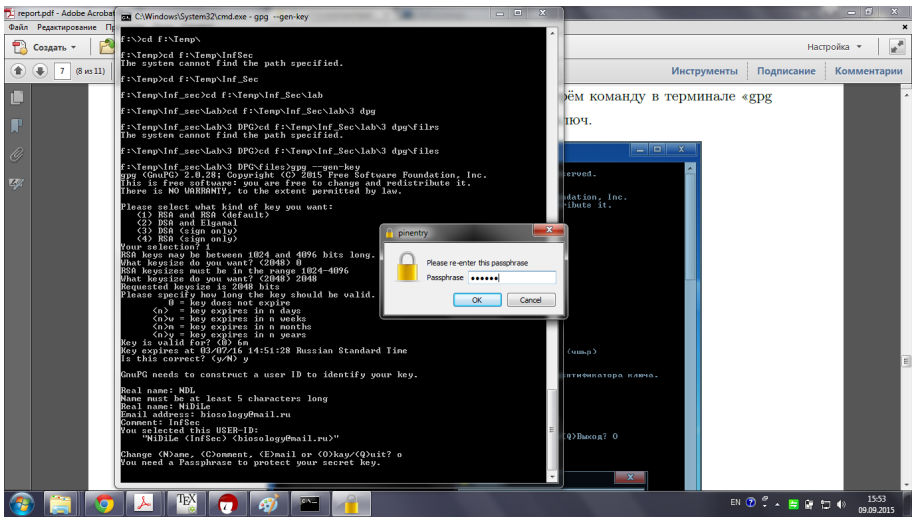
2.7 Используя GNU Privacy handbook (ссылка в материалах) потренироваться в использовании gpg через интерфейс командной строки, без использования графических оболочек.

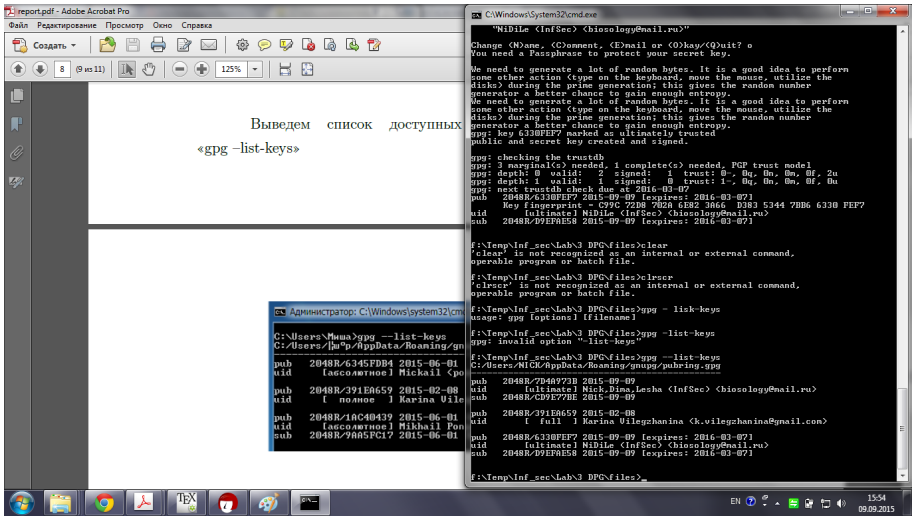
Были изучены следующие команды:

— –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

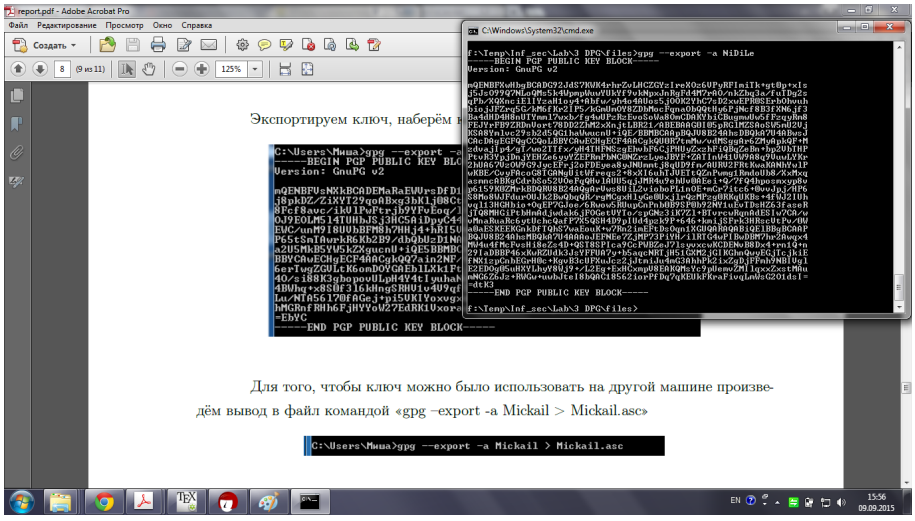
Создадим пару GPG ключей, для этого наберём команду в терминале «gpg –gen-key» в той папке, в которой мы хотим создать ключ.

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

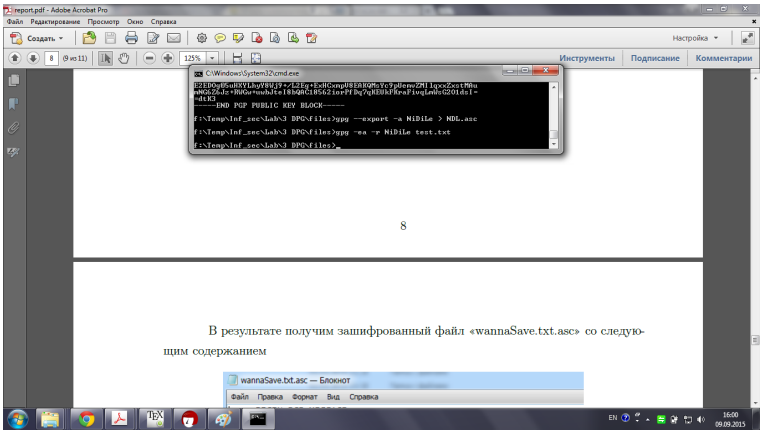




Экспортируем ключ



Для того, чтобы ключ можно было использовать на другой машине произведём вывод в файл


report.pdf - Adobe Acrobat Pro
Файл Редактирование Просмотр Окно Справка
Создать
Настройка
Инструменты
Подписание
Комментарии
C:\Windows\System32\cmd.exe
-----END PGP PUBLIC KEY BLOCK-----
F:\Temp\Inf_sec\Lab\3 BPG\files>gpg --export -a NiDiLe > NDL.asc
F:\Temp\Inf_sec\Lab\3 BPG\files>gpg -ea -r NiDiLe test.txt
F:\Temp\Inf_sec\Lab\3 BPG\files>
8
В результате получим зашифрованный файл «wannaSave.txt.asc» со следующим содержанием
wannaSave.txt.asc — Блокнот
Файл Правка Формат Вид Справка

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.