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»

Выполнил: студент гр. 53501/2
Пономарев М.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

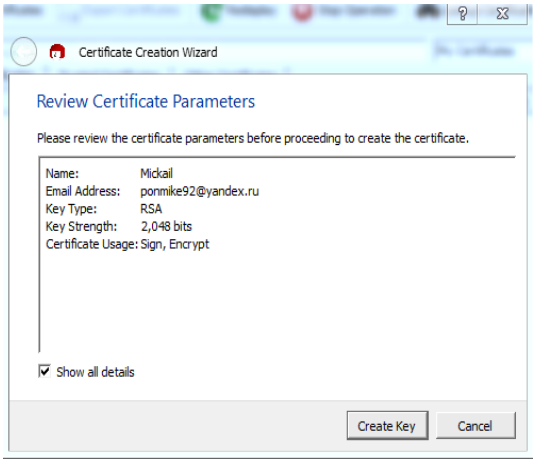
з) Взять сертификат кого-либо из коллег, зашифровать и подписать для него какой–либо текст, предоставить свой сертификат, убедиться, что ему удалось получить открытый текст, проверить подпись

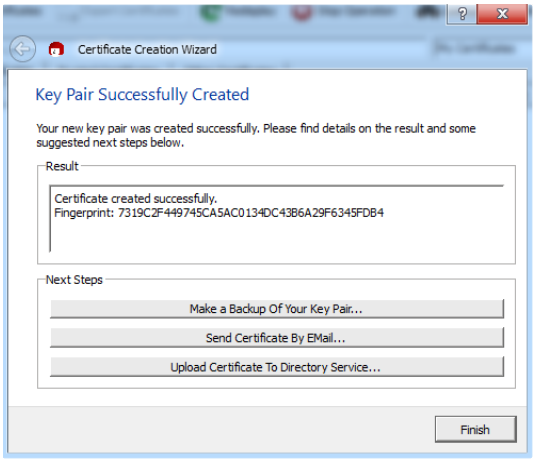
и) Предыдущий пункт наоборот

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

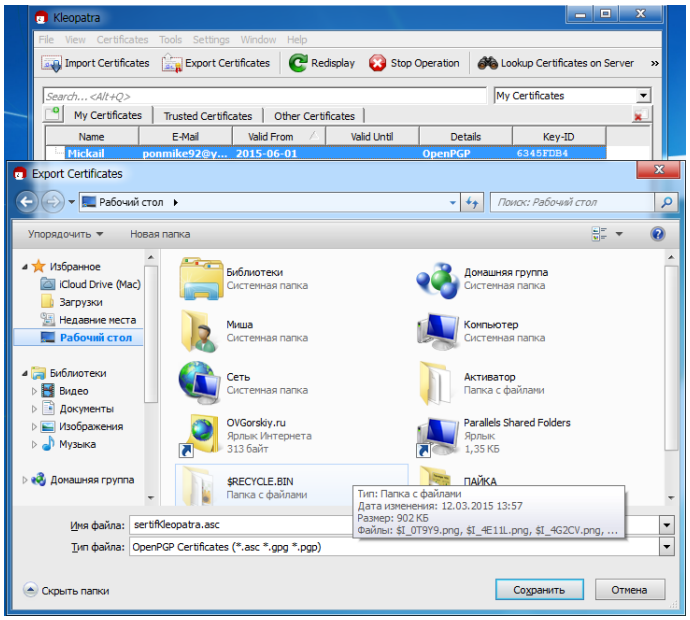
2 Выполнение

2.1 Создать ключевую пару OpenPGP (File → New Certificate)



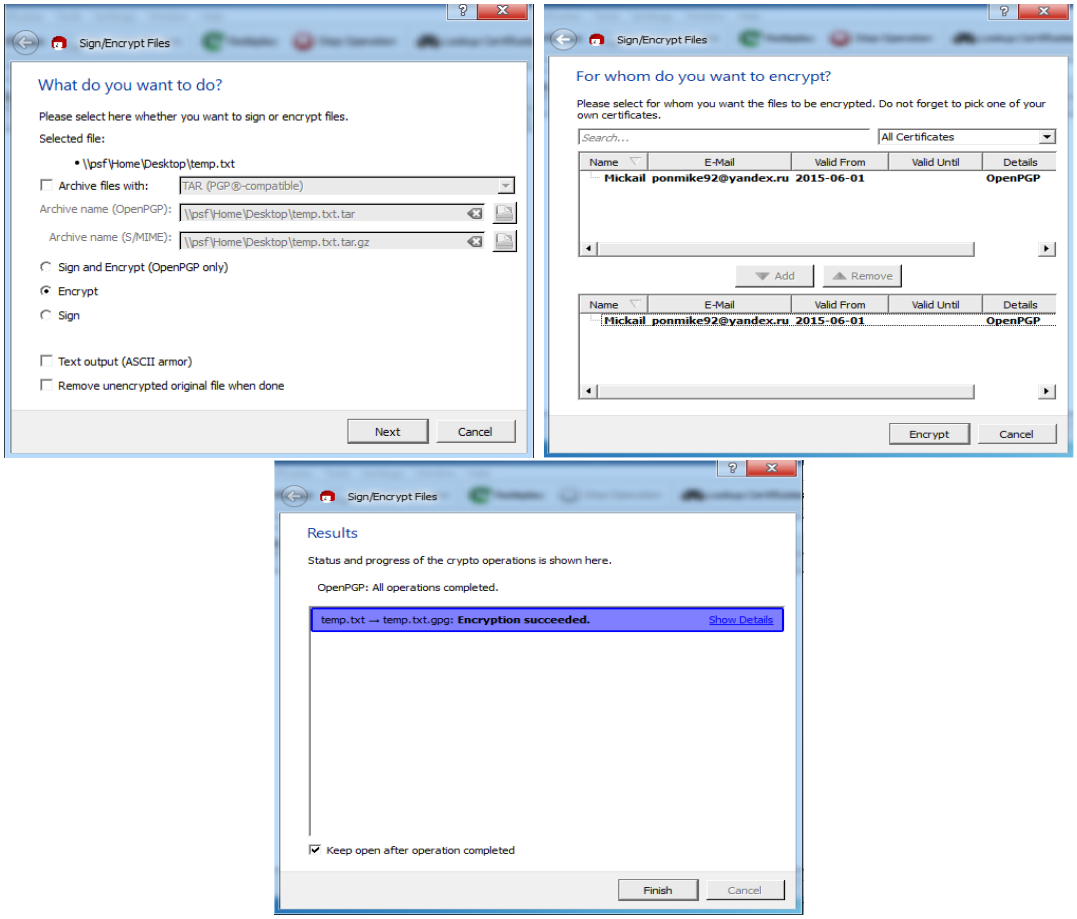


2.2 Экспортировать сертификат (File → Export Certificate)



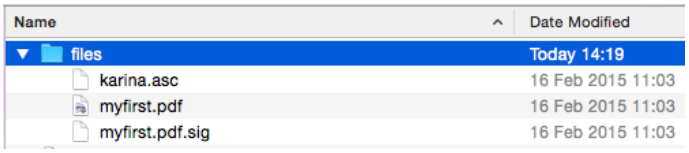
2.3 Поставить ЭЦП на файл (File → Sign/Encrypt Files)

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



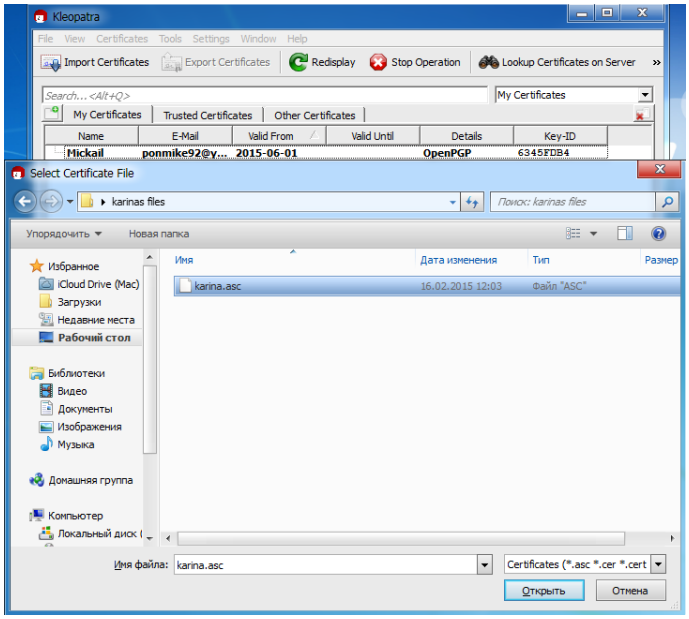
В ходе шифрования нас попросят ввести фразу–пароль.

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

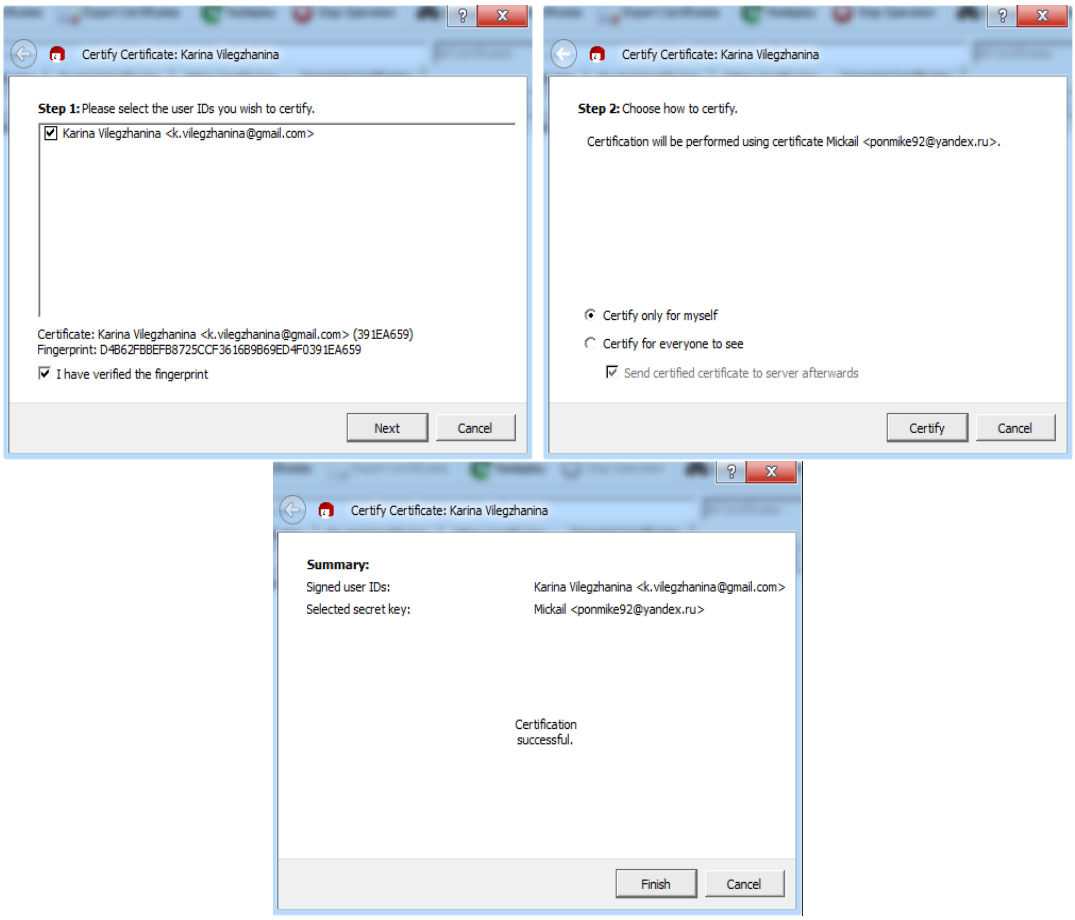


2.5 Импортировать сертификат, подписать его

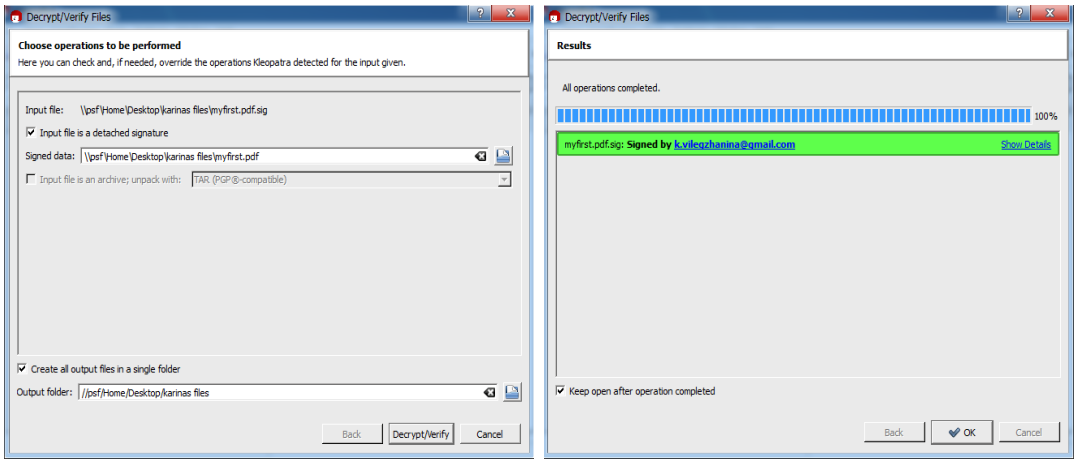
Импортируем сертификат:



Подпишем сертификат:

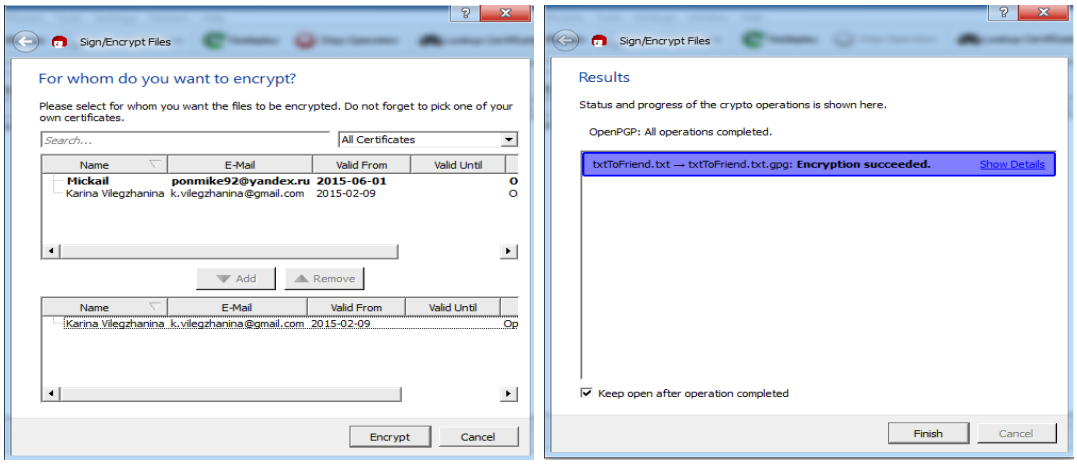


2.6 Проверить подпись



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

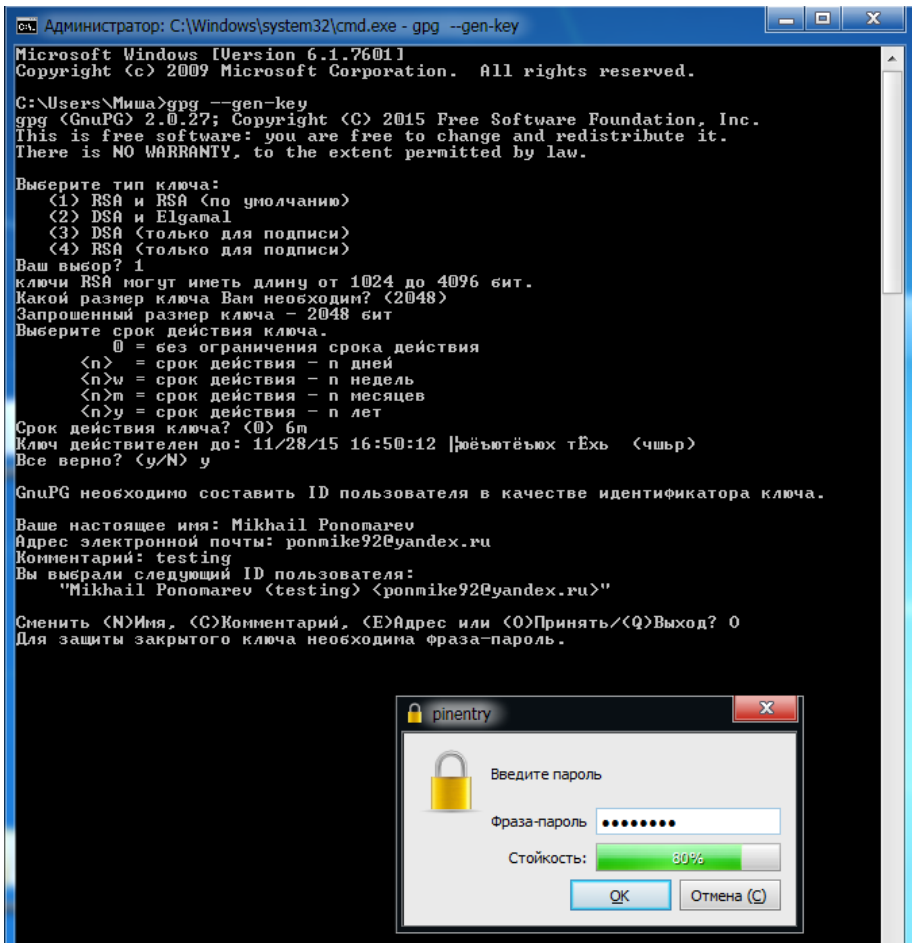
Сертификат был взят преподавательский. Был создан файл «txtToFriend.txt» для дальнейшего шифрования.



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.

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»