Федеральное государственное автономное образовательное учреждение Высшего профессионального образования

Санкт-Петербургский политехнический университет

Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

Лабораторная работа №2

Программа для шифрования и подписи GPG, пакет Gpg4win

Выполнил студент
группы 53501/3

_____
П. П. Жук
«____» _____ 2016 г.

Проверил преподаватель

_____
К. Д. Вылегжанина
«____» _____ 2016 г.

Санкт-Петербург
2016 г.

Содержание

1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

2 Задание

1. Изучить документацию, запустить графическую оболочку Kleopatra.
2. Создать ключевую пару OpenPGP (*File* → *New Certificate*).
3. Экспортировать сертификат (*File* → *Export Certificate*).
4. Поставить ЭЦП на файл (*File* → *Sign/Encrypt Files*).
5. Импортировать сертификат, подписать его.
6. Проверить подпись.
7. Взять сертификат кого-либо из коллег, зашифровать и подписать для него какой-нибудь текст, предоставить свой сертификат, убедиться, что ему удалось получить открытый текст, проверить подпись.
8. Предыдущий пункт наоборот.
9. Используя GNU Privacy handbook потренироваться в использовании gpg через интерфейс командной строки без использования графических оболочек.

3 Ход работы

Работа проводилась в ОС Windows 8. Предварительно был установлен пакет Gpg4win.

3.1 Изучить документацию, запустить графическую оболочку Kleopatra

GPG или GNU Privacy Guard — это реализация стандарта OpenPGP, который определен в документе RFC4880. GPG — это свободная программа для шифрования информации и создания электронных цифровых подписей, выпущена под свободной лицензией GNU General Public License.

GnuPG — программа, которая работает на почти всех операционных системах. Хотя в основном интерфейсом GnuPG является командная строка, существуют различные внешние дополнения, которые делают доступной функциональность этой программы через графический интерфейс пользователя. Для пользователей операционной системы Microsoft Windows GnuPG поставляется сразу с графическим интерфейсом. Начиная с 2005 года разработчиками проекта GnuPG выпускается инсталляционный пакет Gpg4win (GNU Privacy Guard for Windows). Gpg4win — это официальная версия GnuPG для платформы Windows и все включённые в этот пакет компоненты также свободны.

GnuPG шифрует сообщения, используя асимметричные пары ключей, генерируемые пользователями GnuPG. Открытыми ключами можно обмениваться с другими пользователями различными путями, в том числе и через Интернет с помощью серверов ключей. Также GnuPG позволяет добавлять криптографическую цифровую подпись к сообщению, при этом целостность и отправитель сообщения могут быть проверены.

GnuPG не использует запатентованное или иначе ограниченное программное обеспечение и/или алгоритмы. GnuPG использует такие непатентованные алгоритмы как: CAST5, 3DES, AES, Blowfish и Twofish.

GnuPG — это гибридное криптографическое программное обеспечение, которое использует комбинацию стандартного шифрования с помощью симметричных ключей и шифрования с открытым ключом для безопасного обмена ключами, открытый ключ получателя необходим для шифрования ключа сессии, используемого единожды.

3.2 Создать ключевую пару OpenPGP

Для создания ключевой пары запустим менеджер сертификатов Kleopatra и воспользуемся пунктом меню *File* → *New Certificate*. Предлаегается выбрать тип создаваемого сертификата, создадим ключевую пару OpenPGP (рис. 1).

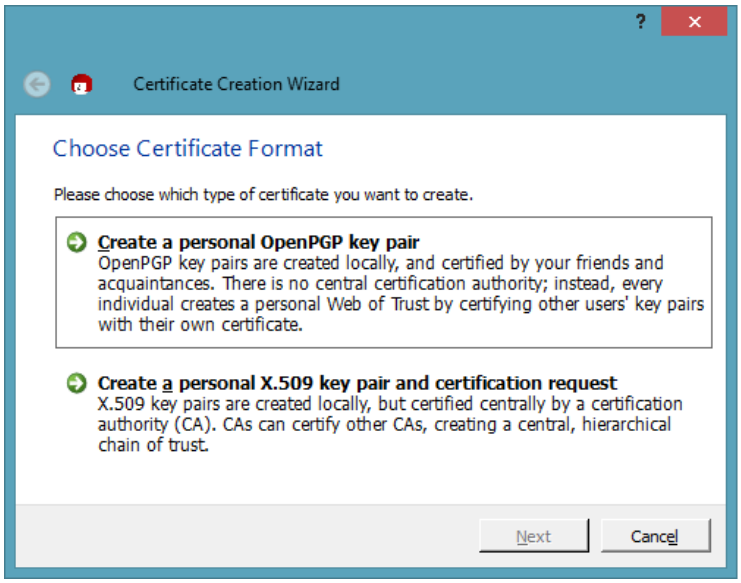

Рис. 1: Окно создания ключа.

Затем введем персональную информацию (рис. 2): имя, почтовый адрес, комментарий. Также есть возможность задать дополнительные настройки.

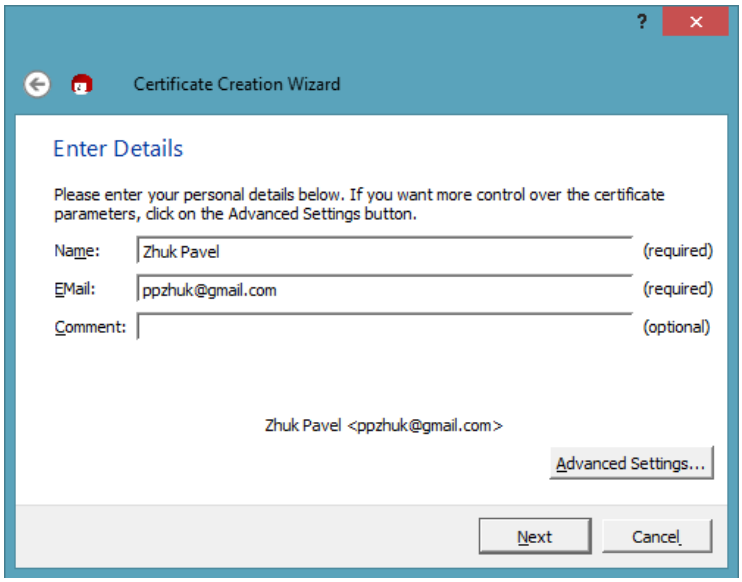

Рис. 2: Персональные данные.

Далее подтверждаем вверенную информацию (рис. 3) и дважды вводим фразу-пароль (рис. 4).

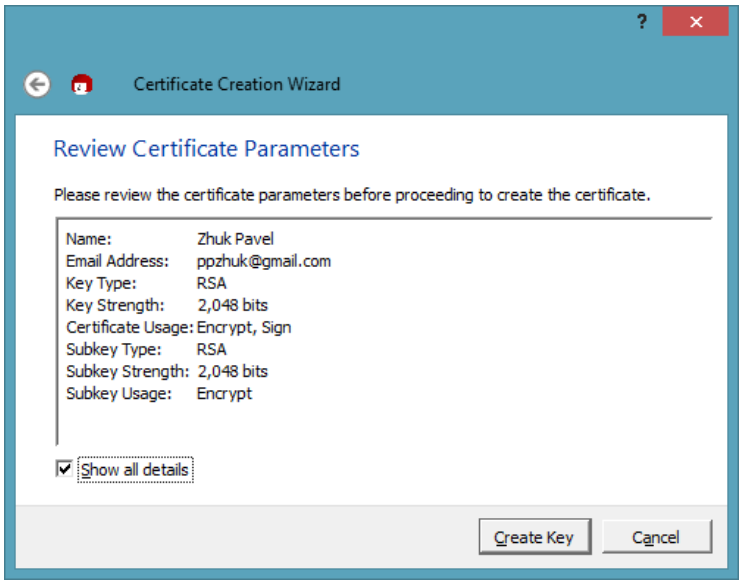

Рис. 3: Подтверждение персональных данных.

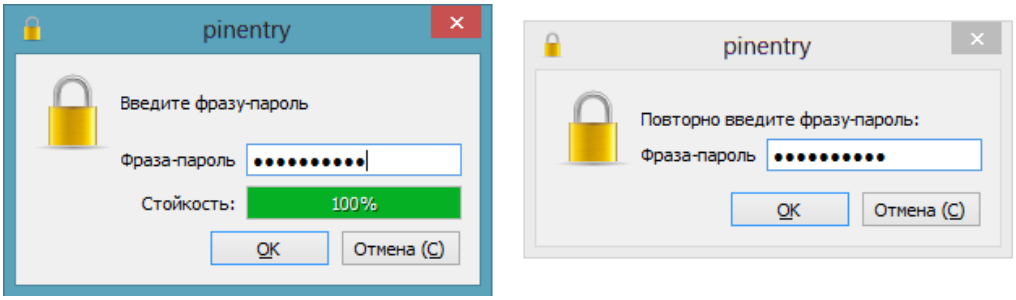

Рис. 4: Ввод пароля.

Ключ создан (рис. 5). При двойном нажатии на ключе можно посмотреть подробную информацию о нем.

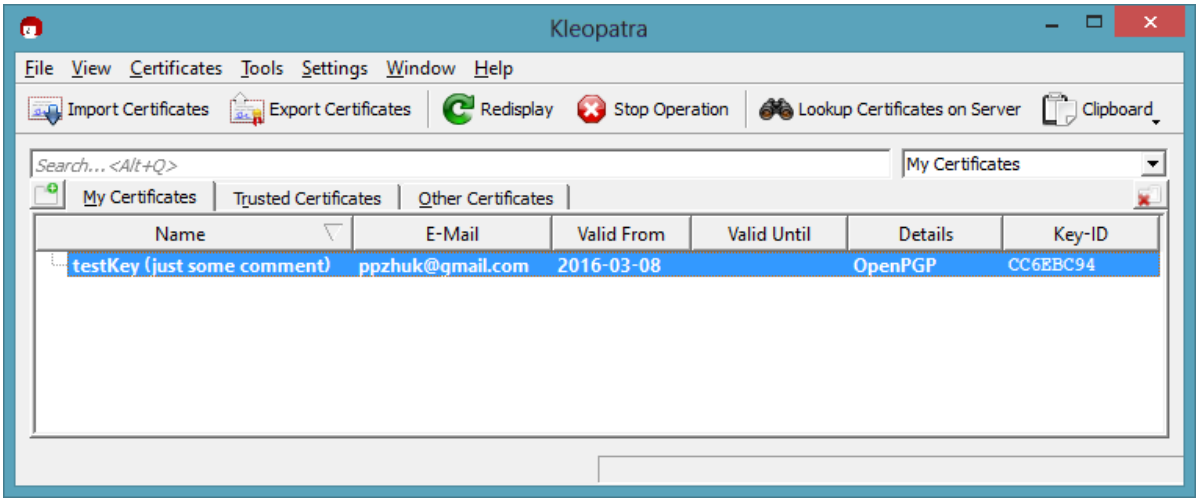

Рис. 5: Созданный ключ.

3.3 Экспортировать сертификат

Для экспорта сертификата выберем пункт меню *File* → *Export Certificate*. Далее выберем место сохранения сертификата и зададим название файла (рис. 6).

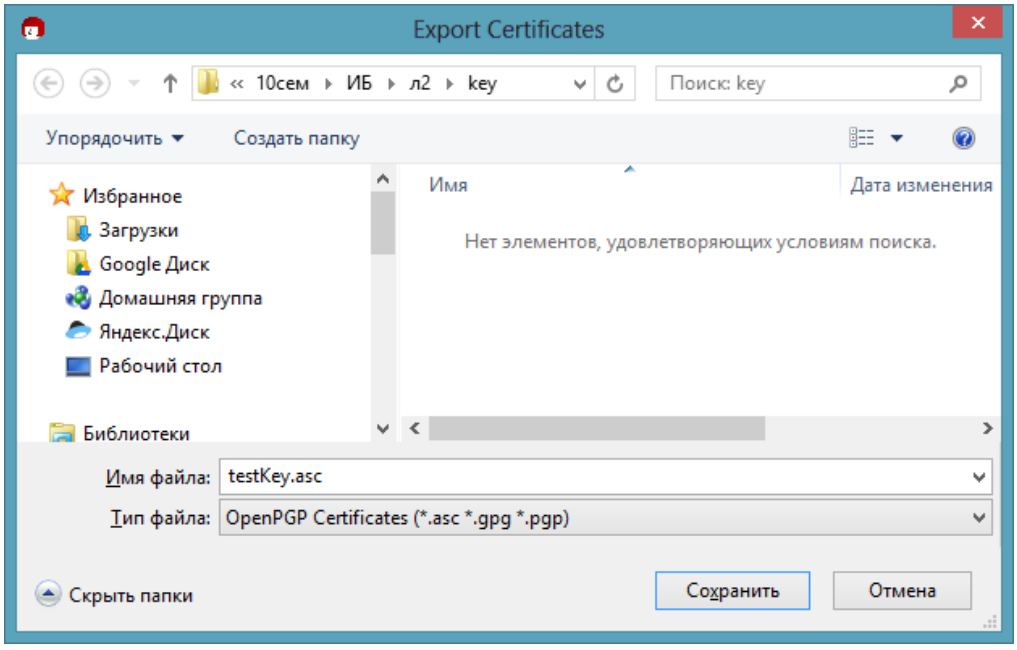

Рис. 6: Экспорт сертификата.

3.4 Поставить ЭЦП на файл

Для установки ЭЦП на файл выберем пункт меню *File* → *Sign/Encrypt Files* и выберем нужный файл. Пусть это будет файл *test.png* (рис. 7).

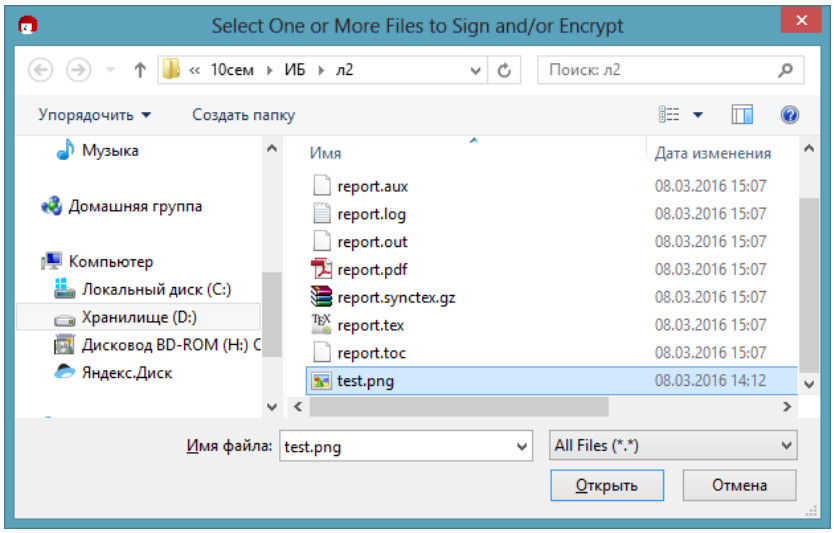

Рис. 7: Выбор файла.

Мы можем подписать файл (*Sign*), зашифровать его (*Encrypt*) или применить оба варианта вместе. Выберем вариант «подписать файл» (рис. 8).

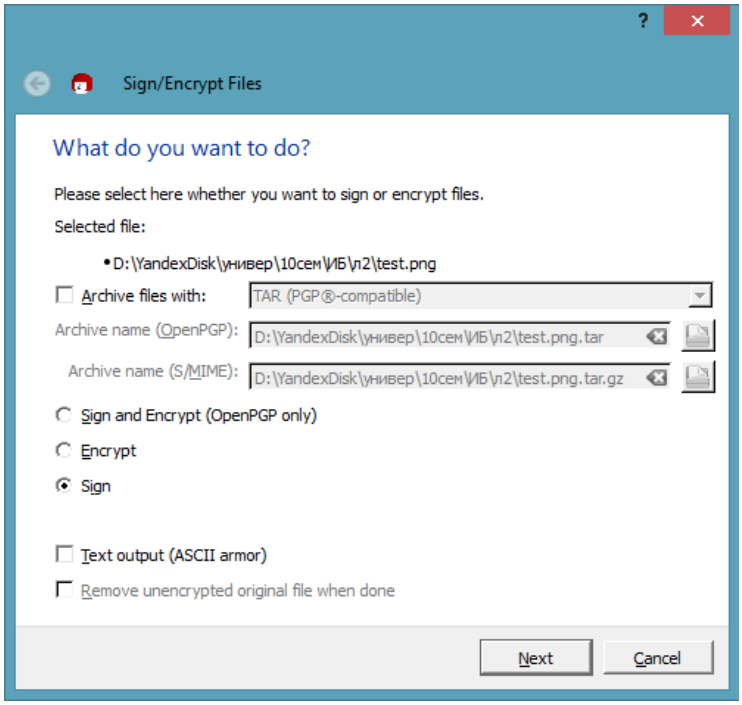

Рис. 8: Установка ЭЦП.

Затем выберем для подписи созданный ранее OpenPGP сертификат (рис. 9).

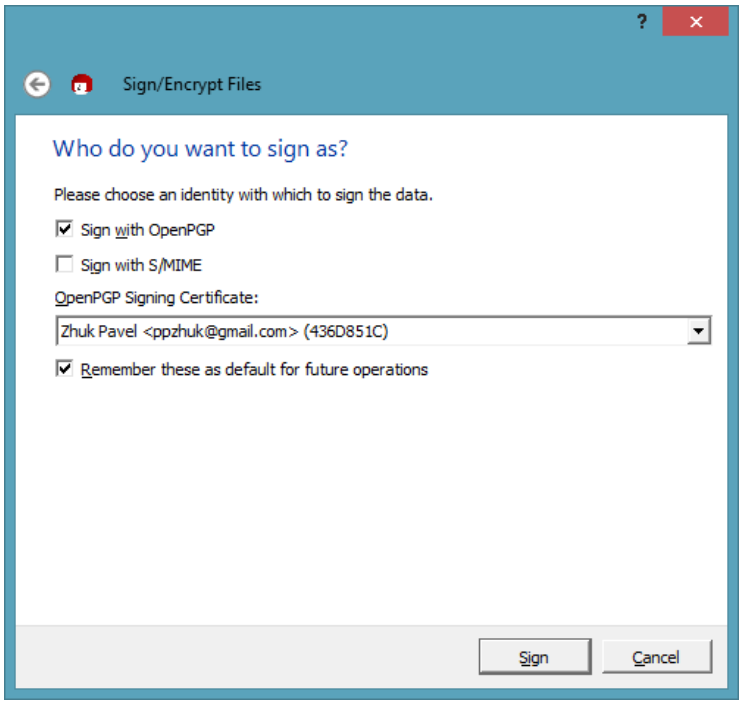

Рис. 9: Выбор сертификата.

После этого необходимо ввести пароль (рис. 10).

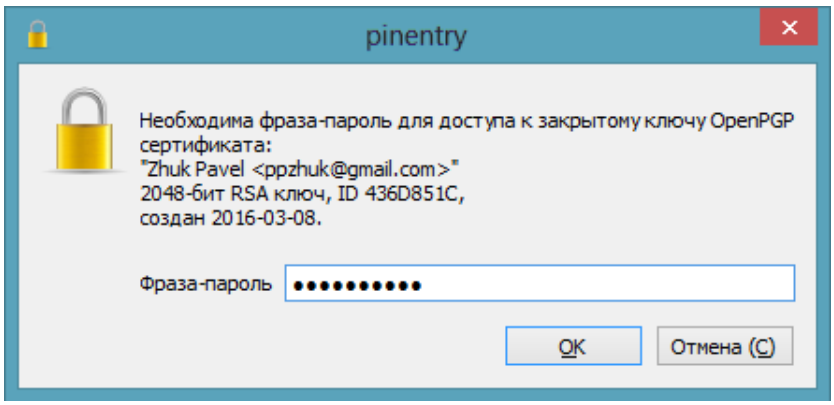

Рис. 10: Ввод пароля.

И в результате получаем окно о том, что файл успешно подписан (рис. 11).

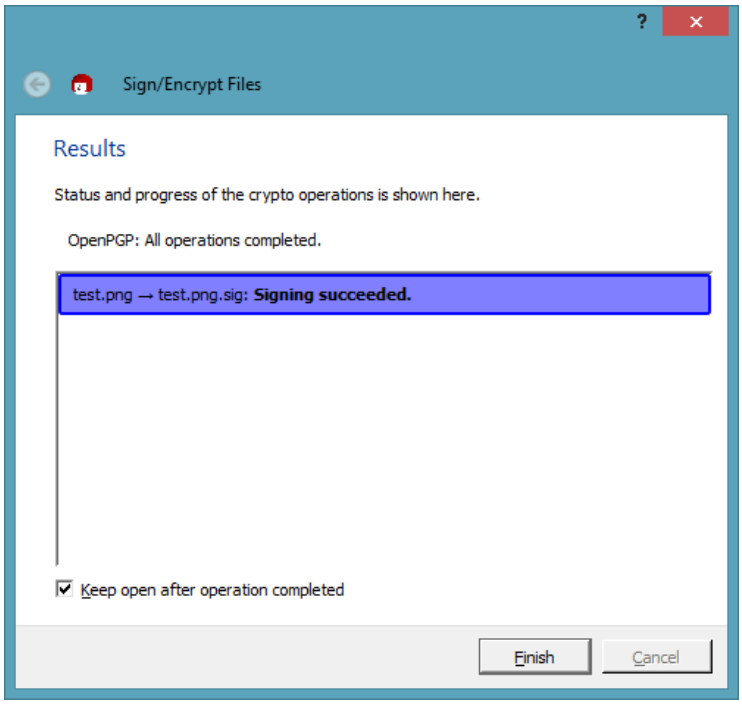

Рис. 11: ЭЦП установлена.

3.5 Импортировать сертификат, подписать его

Для импорта сертификата используется пункт меню *File* → *Import Certificates*. Выберем данный пункт меню и затем выберем сертификат для импорта (рис. 12).

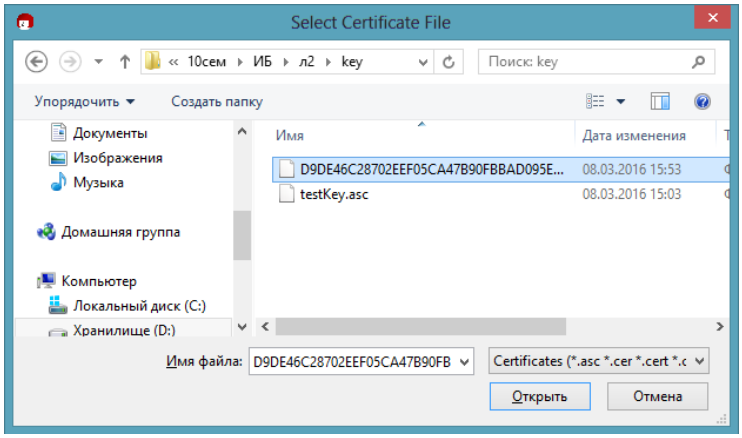

Рис. 12: Импорт сертификата.

После чего отображается соответсвующее окно с результатами импорта (рис. 13).

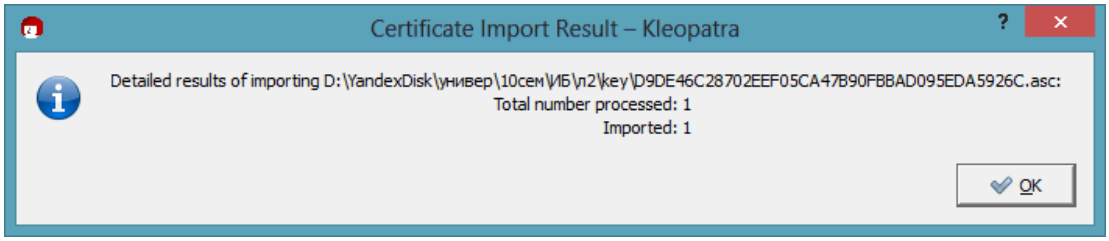

Рис. 13: Результат импорта.

Подпись осуществляется аналогично предыдущему пункту. Результат показан на mboxрисунке 12).

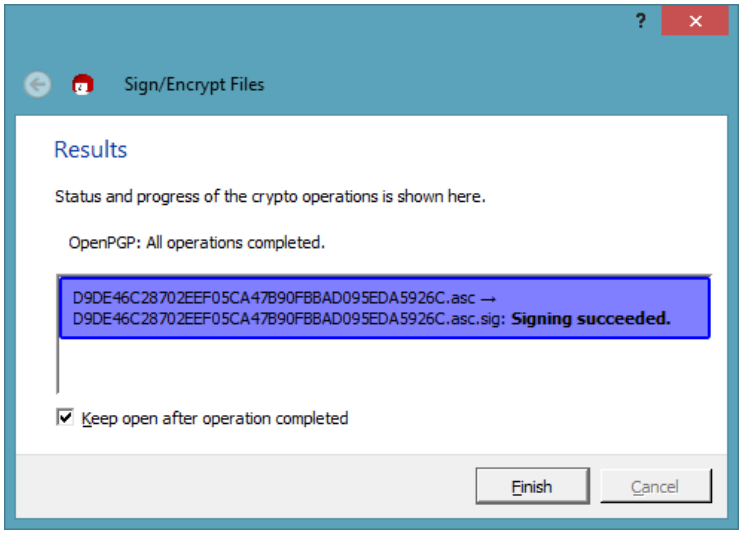

Рис. 14: Подпись сертификата.

3.6 Проверить подпись

Для проверки подписи воспользуемся командой *File → Decrypt/Verify Files* и выберем подписанный ранее сертификат (файл .asc.sig).

После нажатия на кнопку *Decrypt/Verify* осуществляется проверка, которая показывает, кем была осуществлена подпись (рис. 15).

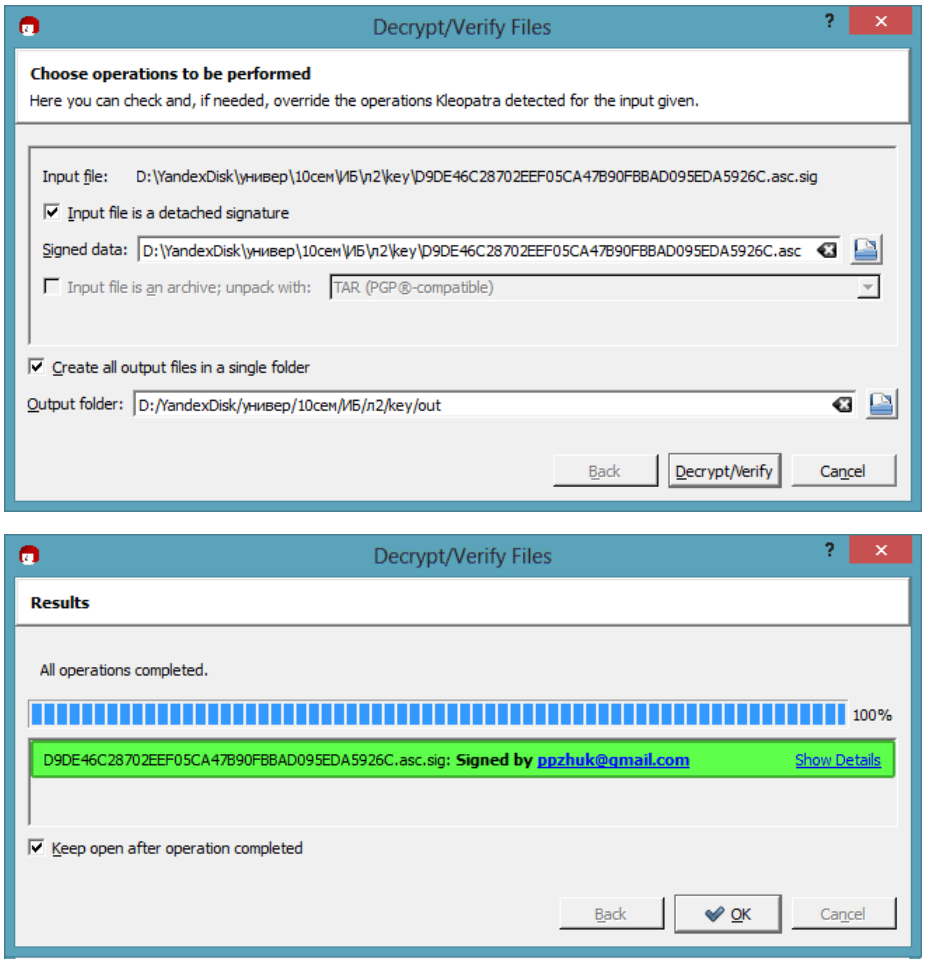

Рис. 15: Проверка подписи сертификата.

3.7 Зашифровать и подписать текст чужим сертификатом.

Был получен и импортирован способом, описанным выше, чужой сертификат под назвнием *another.asc*.

Для шифрования был выбран файл *testMessage.txt*, который содержит текст: *There is an encrypted test message for you!*

Для шифрования и подписи файла был выбран пункт меню *File* → *Sign/Encrypt Files*. В этот раз в настройках было выбрано *Sign and Encrypt* (рис. 16).

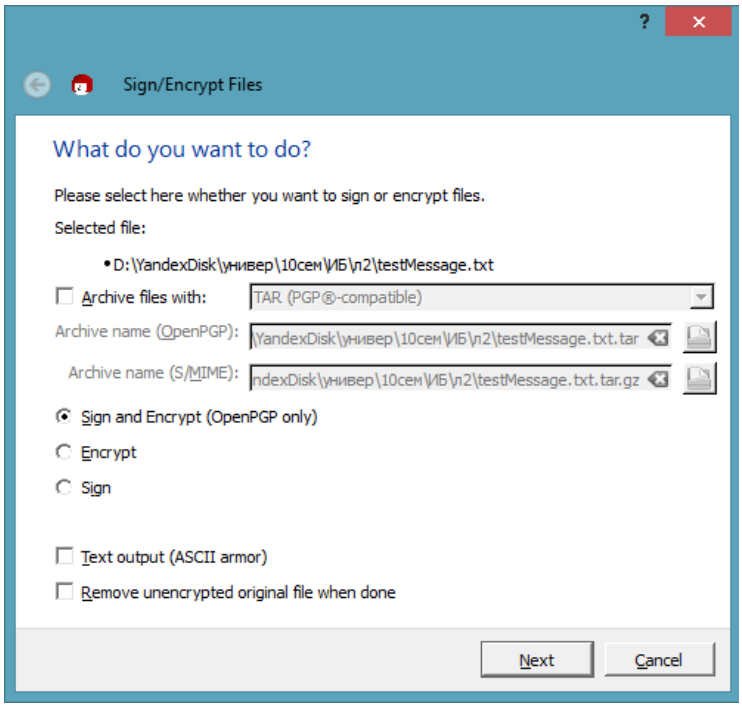

Рис. 16: Шифрование и подпись.

В следующем окне необходимо выбрать сертификат пользователя, для которого будет производиться шифрование (рис. 17). Подпись происходит, как описано выше.

В результате получаем сообщение о том, что файл зашифрован и подписан (рис. 18). А также файл *testMessage.txt.gpg*, который надо передать владельцу сертификата.

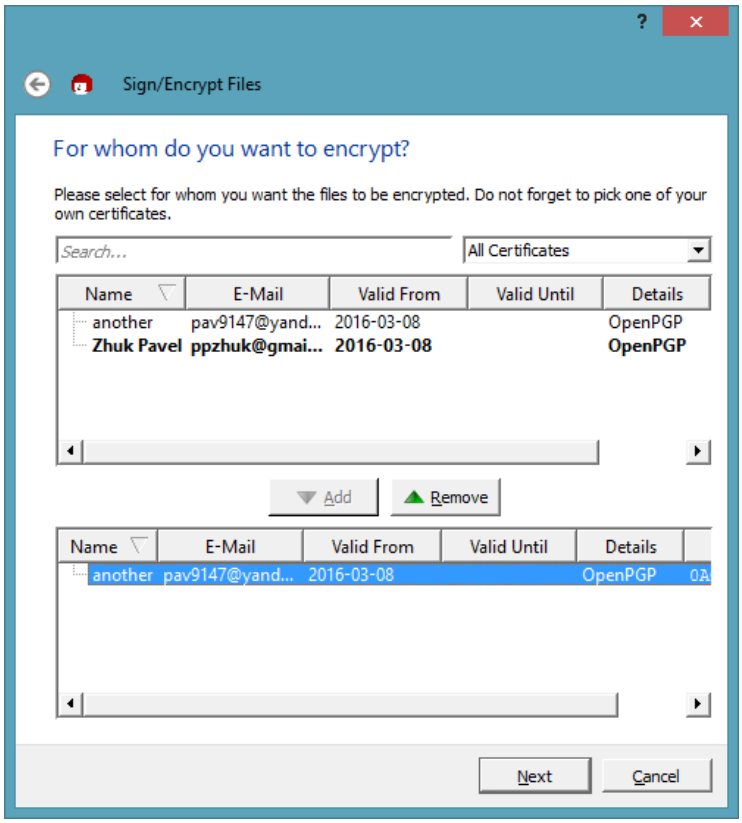

Рис. 17: Выбор сертификата.

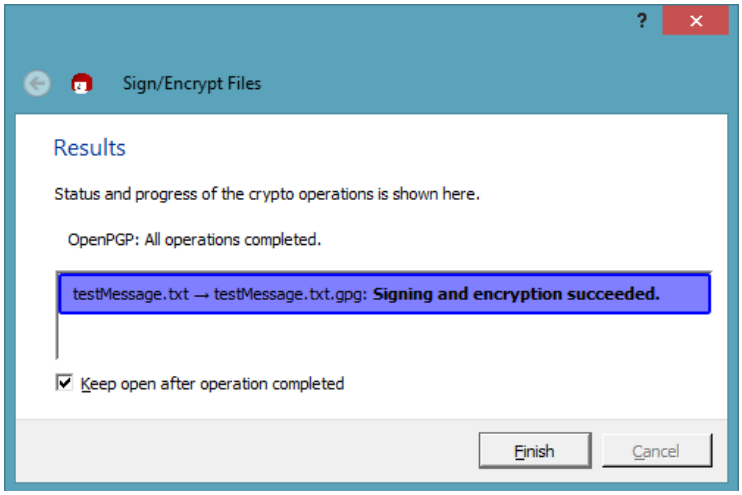

Рис. 18: Результат.

3.8 Расшифровать текст зашифрованный совим сертификатом

От коллеги был получен файл *another.txt.gpg*. Расшифруем его командой *File → Decrypt/Verify Files*.

В результате получился расшифрованный файл *another.txt.gpg*, который содержит фразу: *Hello Zhuk Pavel*.

3.9 Потренироваться в использовании gpg через интерфейс командной строки

Создание ключевой пары происходит с помощью ключа *–gen-key*. Далее следует серия вопросов, которые помогают настроить необходимые параметры.

```
C:\Users\Pavel\Desktop>gpg --gen-key
gpg (GnuPG) 2.0.29; 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
длина ключей RSA может быть 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 ключа - n дней
      <n>w = срок действия ключа - n недель
      <n>m = срок действия ключа - n месяцев
      <n>y = срок действия ключа - n лет
Срок действия ключа? (0) 0
Срок действия ключа не ограничен
Все верно? (y/N) y

GnuPG необходимо составить ID пользователя в качестве идентификатора ключа.

Ваше настоящее имя: Pavel Zhuk
Адрес электронной почты: ppzhuk@gmail.com
Комментарий: The only way to survive a mad world is to embrace the madness
Вы выбрали следующий ID пользователя:
    "Pavel Zhuk (The only way to survive a mad world is to embrace the madness)
<ppzhuk@gmail.com>"

Сменить (N)Имя, (C)Комментарий, (E)Адрес или (O)Принять/(Q)Выход? O
Для защиты закрытого ключа необходима фраза-пароль.

Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропии.
gpg: ключ BF2B89B2 помечен как абсолютно доверенный.
открытый и закрытый ключи созданы и подписаны.

gpg: проверка таблицы доверия
gpg: требуется 3 с ограниченным доверием, 1 с полным, модель доверия PGP
gpg: глубина: 0  верных:   2  подписанных:   0  доверие: 0-, 0q, 0n, 0m, 0f, 2u
pub   2048R/BF2B89B2 2016-03-08
      Отпечаток ключа = 72F2 669C BA06 AC90 BD7C  31BD 65F1 66EA BF2B 89B2
uid     [абсолютное] Pavel Zhuk (The only way to survive a mad world is to embra
ce the madness) <ppzhuk@gmail.com>
sub   2048R/E3ABA2A3 2016-03-08

C:\Users\Pavel\Desktop>
```

Вывод всех сертификатов происходит при помощи ключа *–list-keys*.

```
C:\Users\Pavel\Desktop>gpg --list-keys
C:/Users/Pavel/AppData/Roaming/gnupg/pubring.gpg
------------------------------------------------
pub   2048R/436D851C 2016-03-08
uid      [абсолютное] Zhuk Pavel <ppzhuk@gmail.com>
sub   2048R/3FD692D3 2016-03-08

pub   2048R/0ACB54CC 2016-03-08
uid      [неизвестно] another <pav9147@yande.ru>
sub   2048R/8B2DA3AE 2016-03-08

pub   2048R/BF2B89B2 2016-03-08
uid      [абсолютное] Pavel Zhuk (The only way to survive a mad world is to embra
ce the madness) <ppzhuk@gmail.com>
sub   2048R/E3ABA2A3 2016-03-08
```

Для симметричного шифрования файла используется ключ *–symmetric*. Зашифруем файл *testMessage.txt* при помощи закрытого ключа.

```
C:\Users\Pavel\Desktop>gpg --symmetric testMessage.txt
```

Получили зашифрованный файл *testMessage.txt.gpg*. Для расшифровки файла необходимо использовать ключ *–decrypt*.

```
C:\Users\Pavel\Desktop>gpg --decrypt testMessage.txt.gpg
gpg: данные зашифрованы алгоритмом CAST5
gpg: зашифровано одной фразой-паролем
There is an encrypted test message for you!
gpg: ВНИМАНИЕ: целостность сообщения не защищена
```

Также существует множество других команд, подробнее с которыми можно знакомиться в The GNU Privacy Handbook.

4 Выводы

Пакет **GPG4win** предоставляет удобное и простое в использовании средство для надежного шифрования файлов и органицации безопасного общения между пользователями. В данной работе были опробованы основные возможности программы. Все действия легко производятся как из командной строки, так и из графической оболочки **Kleopatra**.