

Лабораторная работа №1.  
Программа для шифрования и подписи GPG,  
пакет Gpg4win

Скрипаль Борис

28 марта 2016 г.

# Оглавление

1	Цель работы . . . . .	2
2	Описание лабораторной работы . . . . .	2
3	Ход работы . . . . .	2
3.1	Создание сертификата openPGP . . . . .	2
3.2	Экспорт сертификата . . . . .	4
3.3	Постановка ЭЦП на файл . . . . .	5
3.4	Импорт чужого сертификата . . . . .	6
3.5	Использование консольных команд . . . . .	7

## 1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

## 2 Описание лабораторной работы

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

В данной лабораторной работе для генерации ЭЦП будет использоваться набор утилит, реализующих стандарт OpenPGP (Kleopatra, GPG4win и др.).

## 3 Ход работы

### 3.1 Создание сертификата openPGP

Для создания новой ключевой пары OpenPGP необходимо открыть графическую оболочку "*Kleopatra*" и выполнить команду "*File → New Certificate*". После чего откроется помощник (рисунок 1).

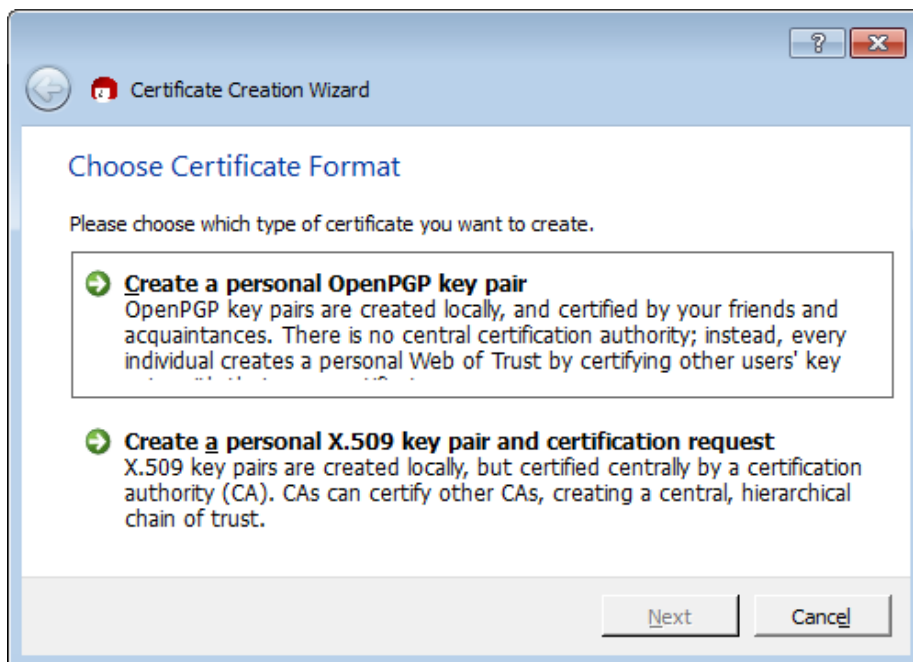


Рис. 1: Окно выбора типа сертификата безопасности.

В данном случае необходимо выбрать первый пункт (*Create a personal OpenPGP key pair*), после чего откроется окно ввода информации о пользователе (рисунок 2).

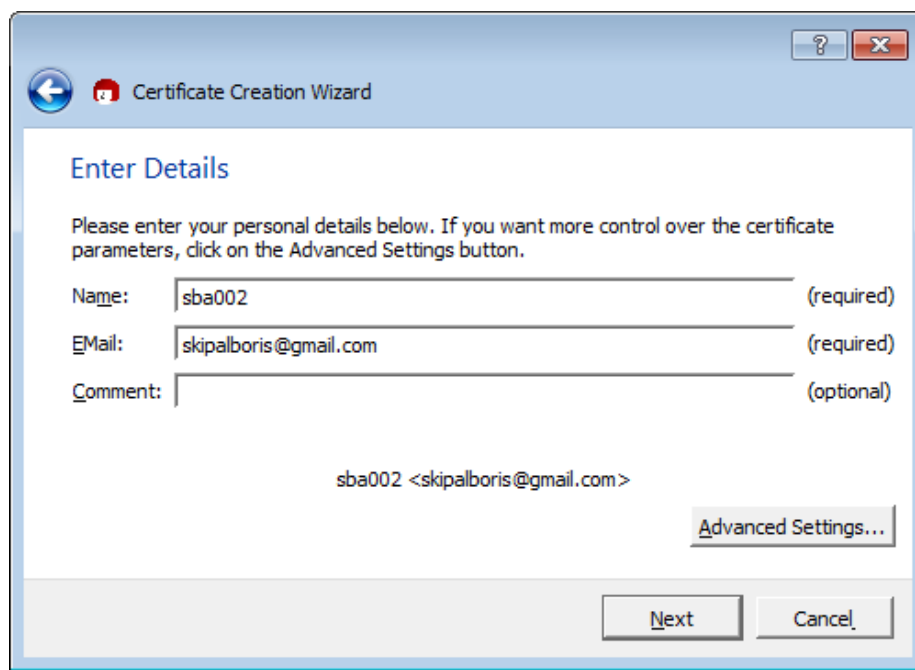
The image shows a Windows-style dialog box titled "Certificate Creation Wizard". It has a blue header bar with a back arrow icon and a red "X" icon. The main area is white with the title "Enter Details" in blue. Below the title, there is a paragraph of text: "Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button." There are three input fields: "Name:" with the value "sba002" and "(required)" to its right; "Email:" with the value "skipalboris@gmail.com" and "(required)" to its right; and "Comment:" which is empty and has "(optional)" to its right. Below these fields, the text "sba002 <skipalboris@gmail.com>" is displayed. To the right of this text is a button labeled "Advanced Settings...". At the bottom right of the dialog are two buttons: "Next" and "Cancel".

Рис. 2: Окно ввода информации о пользователе.

После ввода личных данных необходимо ввести фразу-пароль (рисунок 3).

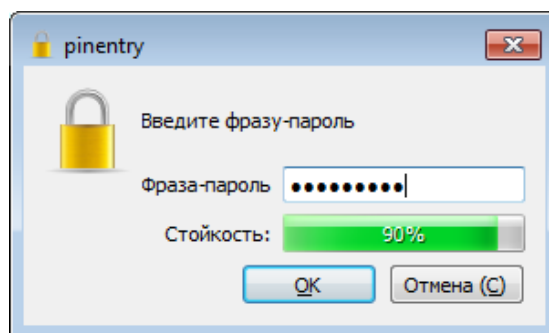
The image shows a small dialog box titled "pinentry". It has a yellow padlock icon on the left. The text "Введите фразу-пароль" (Enter a passphrase) is centered. Below it is a text input field containing several dots, representing a masked passphrase. Below the input field is a progress bar labeled "Стойкость:" (Strength:) with a green fill and the text "90%". At the bottom are two buttons: "ОК" and "Отмена (C)" (Cancel).

Рис. 3: Окно ввода фразы - пароля.

После выполнения данных шагов, помощник выведет сообщение об успешном создании ключевой пары (рисунок 4).

Так же новая ключевая пара появится в рабочем пространстве (рисунок 5).

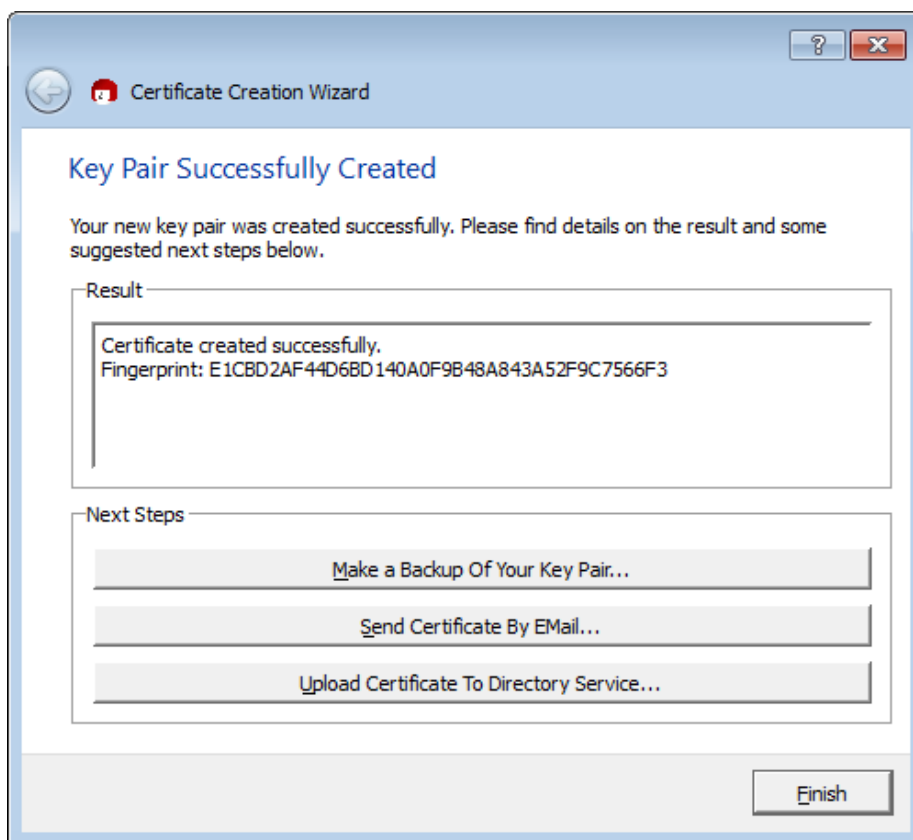


Рис. 4: Окно оповещения об успешном создании ключевой пары.

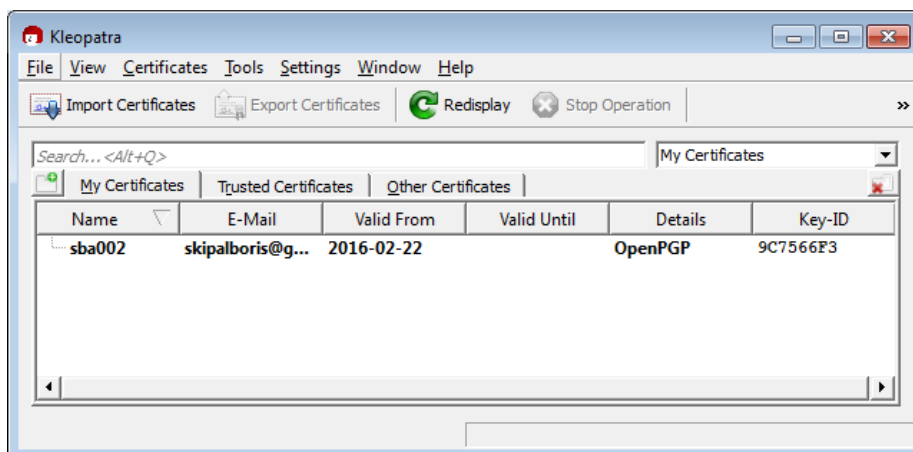


Рис. 5: Отображение новой ключевой пары.

### 3.2 Экспорт сертификата

Для экспорта сертификата необходимо в графической оболочке "Kleopatra" выполнить команду "File → Export Certificate". После чего откроется окно,

в котором будет предложено выбрать название файла, где будет храниться сертификат (рисунок 6)

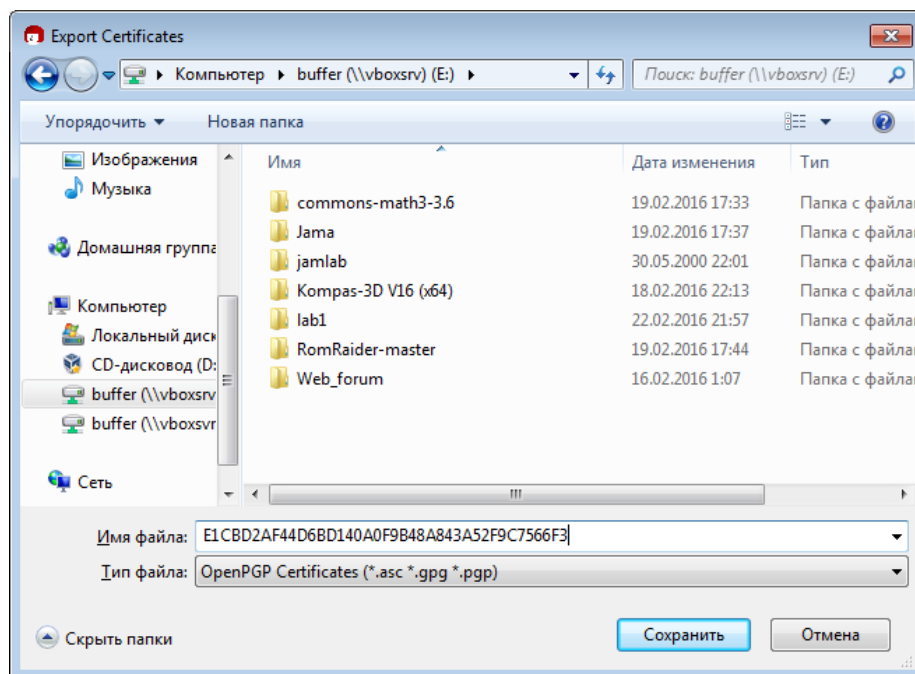


Рис. 6: Экспортирование сертификата.

В данном случае файл будет называться  
"E1CBD2AF44D6BD140A0F9B48A843A52F9C7566F3.asc"

### 3.3 Постановка ЭЦП на файл

Перед тем, как поставить электронную цифровую подпись на файл, создадим текстовый файл "test.txt". Для того, что бы поставить свою ЭЦП на файл, необходимо выполнить команду "*File → Sign/Encrypt Files*". После чего появится окошко, в котором необходимо выбрать файл, для которого будет создаваться ЭЦП (рисунок 7).

После чего помощника (рисунок 8), в котором необходимо выбрать пункт "*Sign*" - создание цифровой подписи.

После чего появляется окошко, где необходимо подтвердить сертификат, которым будет подписываться файл (рисунок 9).

Затем необходимо аутентифицироваться при помощи пароля, заданного при создании ключа (рисунок 10).

После чего появится сообщение об успешном создании подписи (рисунок 11), а так же появится файл *test.txt.sig*, в котором будет сохранена подпись.

Для проверки соответствия подписи выберем команду "*File → Describe/Verify Files*". После чего необходимо выбрать сертификат, файл, который мы хотим проверить (в нашем случае test.txt), а так же файл с подписью (в нашем случае test.txt.sig). В случае успеха появится окошко, представленное на рисунке 12.

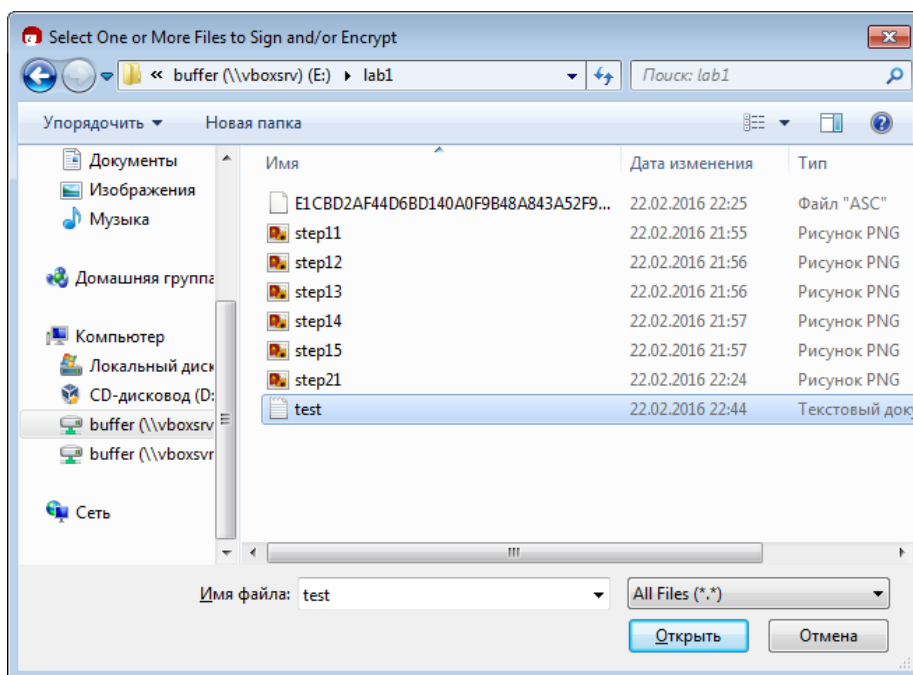


Рис. 7: Окно выбора файла.

### 3.4 Импорт чужого сертификата

Для импортирования чужого сертификата необходимо выполнить команду *"File → Import Certificates"*. После чего откроется окно проводника, в котором необходимо выбрать чужой сертификат (рисунок 13).

После этого новый сертификат можно увидеть во вкладке "Imported Certificates" (рисунок 14).

Для подписания чужого сертификата необходимо выполнить команду *"File → Sign/ Encrypt Files"*. После чего появится окошко, в котором необходимо выбрать файл, для которого будет создаваться ЭЦП (в нашем случае необходимо указать сертификат другого человека). После чего для проверки необходимо выполнить пункт *"File → Descript/ Verify Files"*. Результат представлен на рисунке 15.

Для того, что бы зашифровать файл открытым ключем, необходимо выбрать пункт *"File → Sign/ Encrypt Files"*, после чего выбрать необходимый файл и выбрать пункт "Sign/ Encrypt" (рисунок 16).

В следующем диалоговом окне нужно выбрать сертификат, при помощи которого будет подписываться и шифроваться файл (рисунок 17).

После чего выбрать стандарт шифрования (в нашем случае OpenPGP) и нажать на кнопку "Sign/ Encrypt". После чего появится новый файл с расширением gpg (в нашем случае файл будет называться Аня.txt.gpg). Данный файл будет возможно расшифровать только при помощи закрытого сертификата другого человека. При попытке расшифровать файл тем сертификатом, при помощи которого он был зашифрован, получаем ошибку расшифровки (рисунок 18).

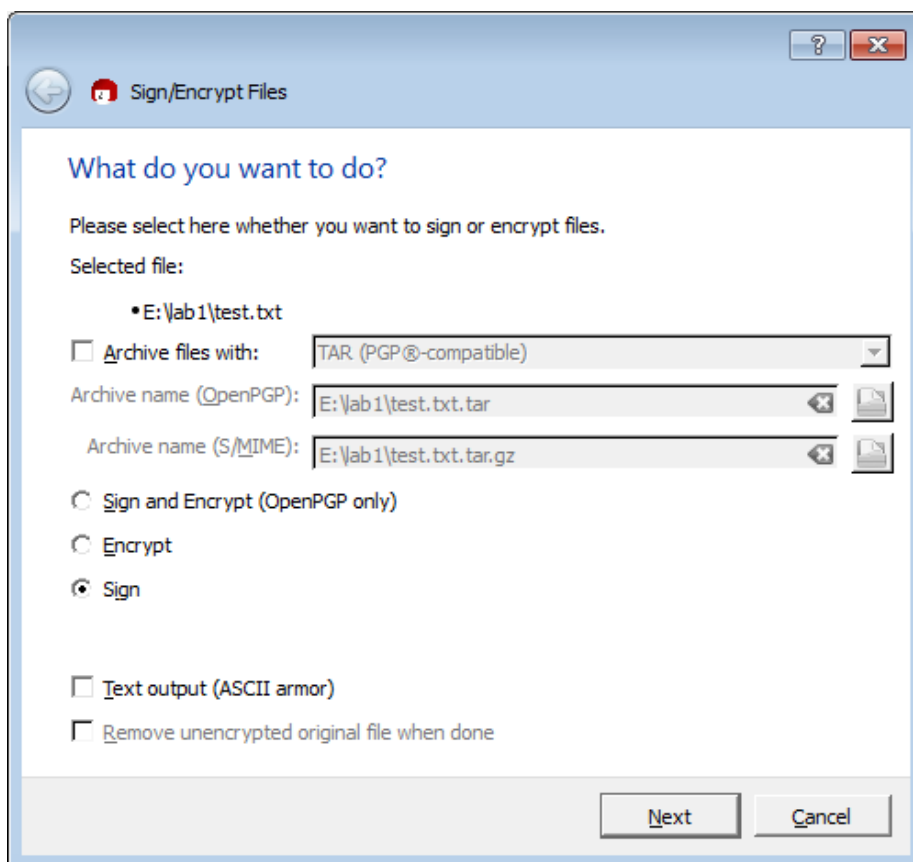


Рис. 8: Помощник создания ЭЦП.

Попробуем расшифровать файл, зашифрованный другим человеком при помощи нашего сертификата. Для этого выберем свой сертификат, после чего выберем пункт *"File → Descript/ Verify Files"* и нажмем на кнопку *"Descript/ Verify"*. После чего нам предложат ввести пароль для того, что бы аутентифицироваться. В случае успеха увидим следующее сообщение (рисунок 19), которое сообщает о удачном завершении операции, а так же о том, кто зашифровал данный файл (в данном случае *annet-girl@mail.ru*). Так же появляется расшифрованный файл (в данном случае *Боря.txt*).

### 3.5 Использование консольных команд

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

```
C:\Users\sba>gpg --list-keys
C:/Users/sba/AppData/Roaming/gnupg/pubring.gpg
-----
pub   2048R/9C7566F3  2016-02-22
uid   [абсолютное]  sba002 <skipalboris@gmail.com>
sub   2048R/00808598  2016-02-22
```



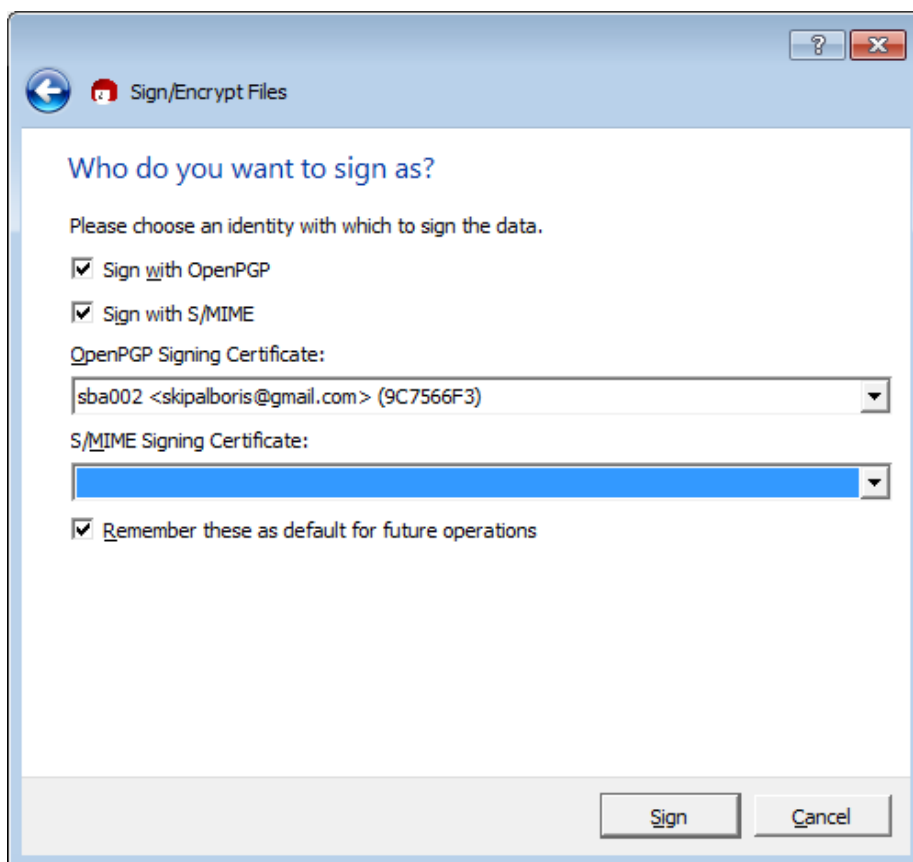


Рис. 9: Окно подтверждения сертификата.

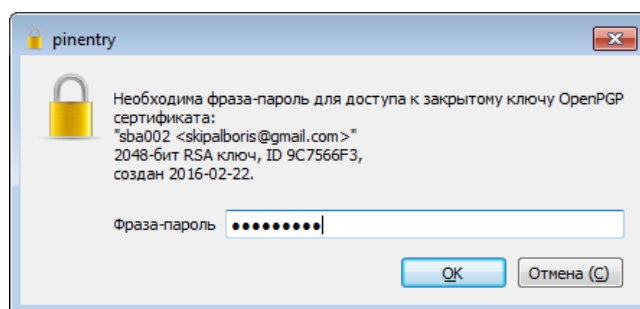


Рис. 10: Окно ввода пароля.

```
pub 2048R/7CD764F8 2016-02-25
uid [неизвестно] myKey <annet-girl@mail.ru>
sub 2048R/4BECA6BD 2016-02-25
```

Перед созданием сертификата необходимо создать ключевую пару при помощи ключа `-gen-key`". В качестве типа ключа выберем RSA и RSA (по умолчанию), длину ключа выберем равной 2048 (значение по умолчанию),

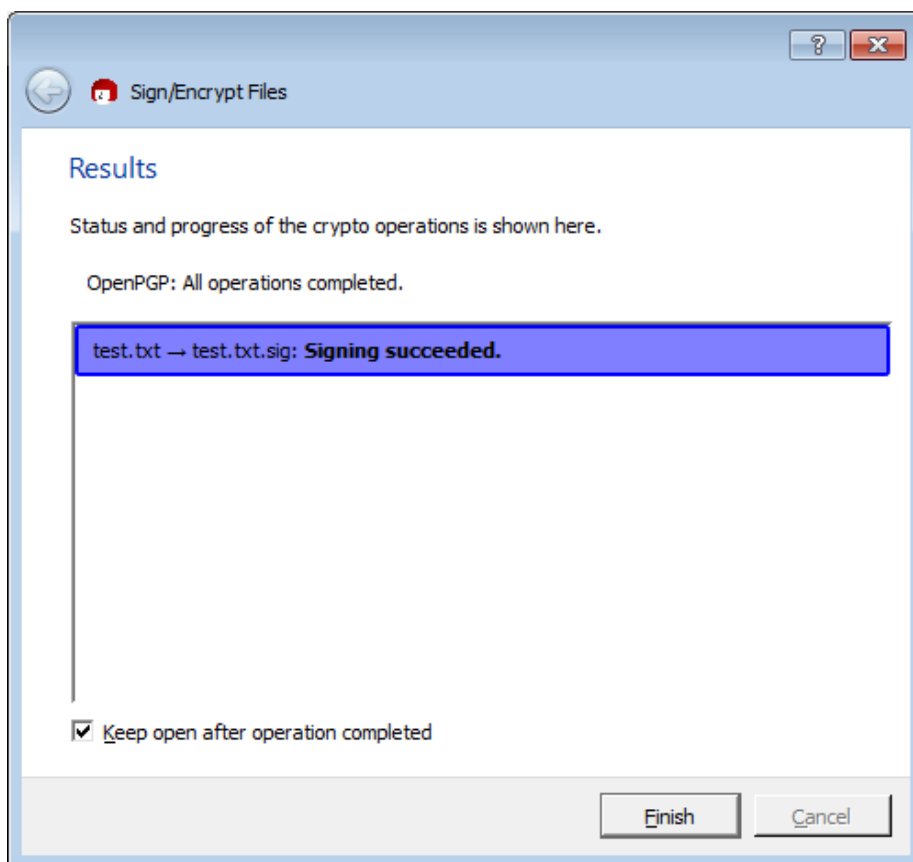


Рис. 11: Окно успешного создания подписи.

бесконечный срок действия. После этого нам будет предложено задать пароль для ключа и после этого ключевая пара будет создана.

```
C:\Users\sba\Downloads\lab1>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) 2048

Запрошенный размер ключа - 2048 бит

Выберите срок действия ключа.

0 = без ограничения срока действия

<n> = срок действия ключа - n дней

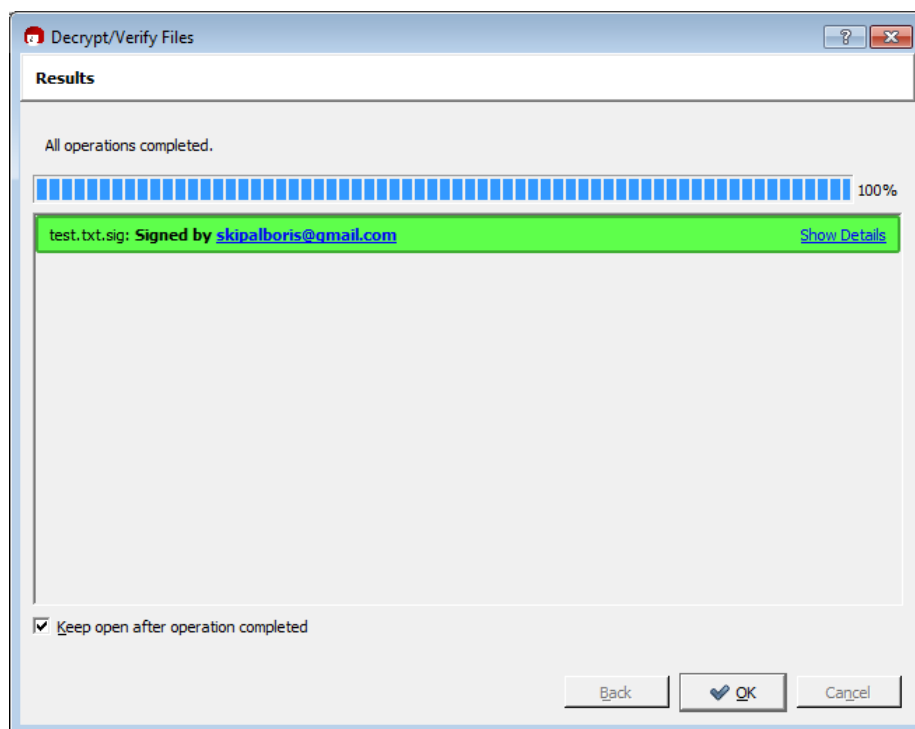


Рис. 12: Окно с результатами проверки подписи.

<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: SkripalBoris  
 Адрес электронной почты: skipalboris@yandex.ru  
 Комментарий: none  
 Вы выбрали следующий ID пользователя:  
 "SkripalBoris (none) <skipalboris@yandex.ru>"

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. Необходимо получить много случайных чисел. Желательно, чтобы Вы

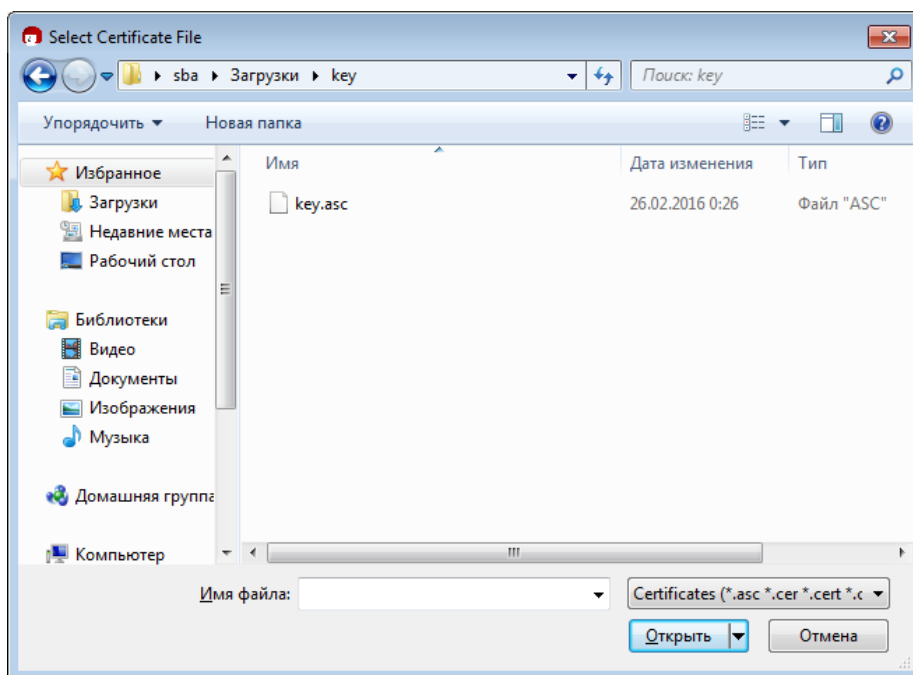


Рис. 13: Окно выбора файла сертификата.

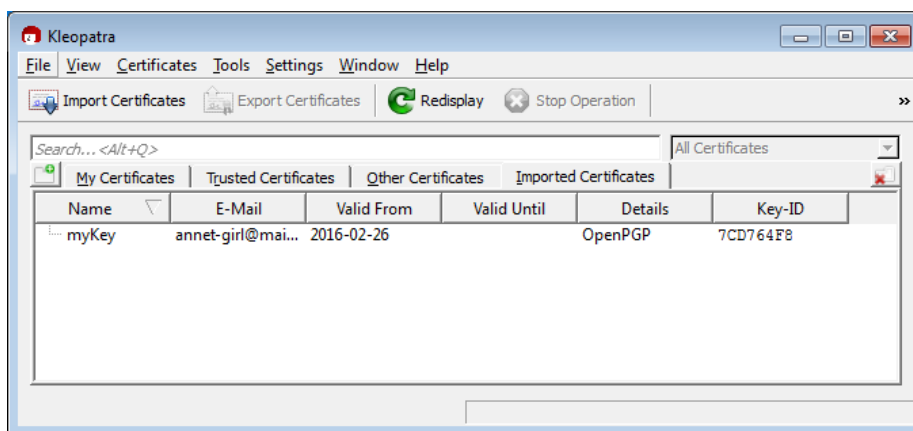


Рис. 14: Вкладка Imported Certificates.

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.  
 grg: ключ 3729EB59 помечен как абсолютно доверенный.  
 открытый и закрытый ключи созданы и подписаны.

grg: проверка таблицы доверия

grg: требуется 3 с ограниченным доверием, 1 с полным, модель доверия RGP

grg: глубина: 0 верных: 2 подписанных: 0 доверие: 0-, 0q, 0n, 0m, 0f, 2u

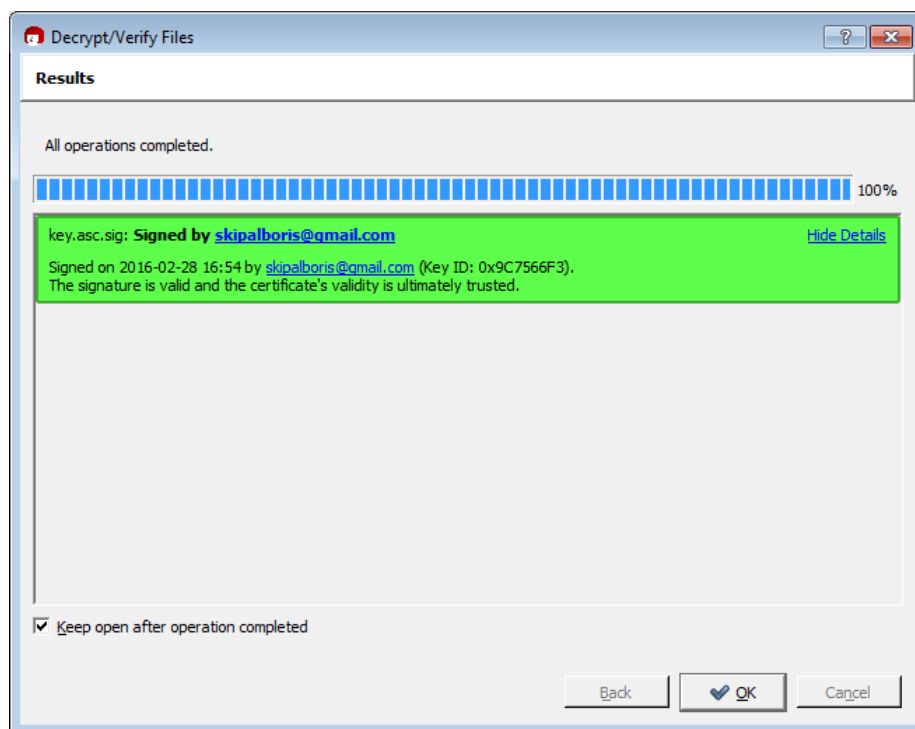


Рис. 15: Проверка подписи сертификата.

```
pub 2048R/3729EB59 2016-02-29
Отпечаток ключа = D675 32A4 0148 164D 1BBC C95C 6460 E810 3729 EB59
uid [абсолютное] SkripalBoris (none) <skipalboris@yandex.ru>
sub 2048R/100C8383 2016-02-29
```

```
C:\Users\sba\Downloads\lab1>gpg --list-keys
C:/Users/sba/AppData/Roaming/gnupg/pubring.gpg
```

```
-----
pub 2048R/9C7566F3 2016-02-22
uid [абсолютное] sba002 <skipalboris@gmail.com>
sub 2048R/00808598 2016-02-22
```

```
pub 2048R/7CD764F8 2016-02-25
uid [неизвестно] myKey <annet-girl@mail.ru>
sub 2048R/4BECA6BD 2016-02-25
```

```
pub 2048R/3729EB59 2016-02-29
uid [абсолютное] SkripalBoris (none) <skipalboris@yandex.ru>
sub 2048R/100C8383 2016-02-29
```

Для создания сертификата необходимо использовать два ключа: "-output" для задания выходного файла, и "-gen-revoke" для задания ключевой пары.

```
C:\Users\sba\Downloads\lab1>gpg --output Skripal.asc --gen-revoke SkripalBoris
```

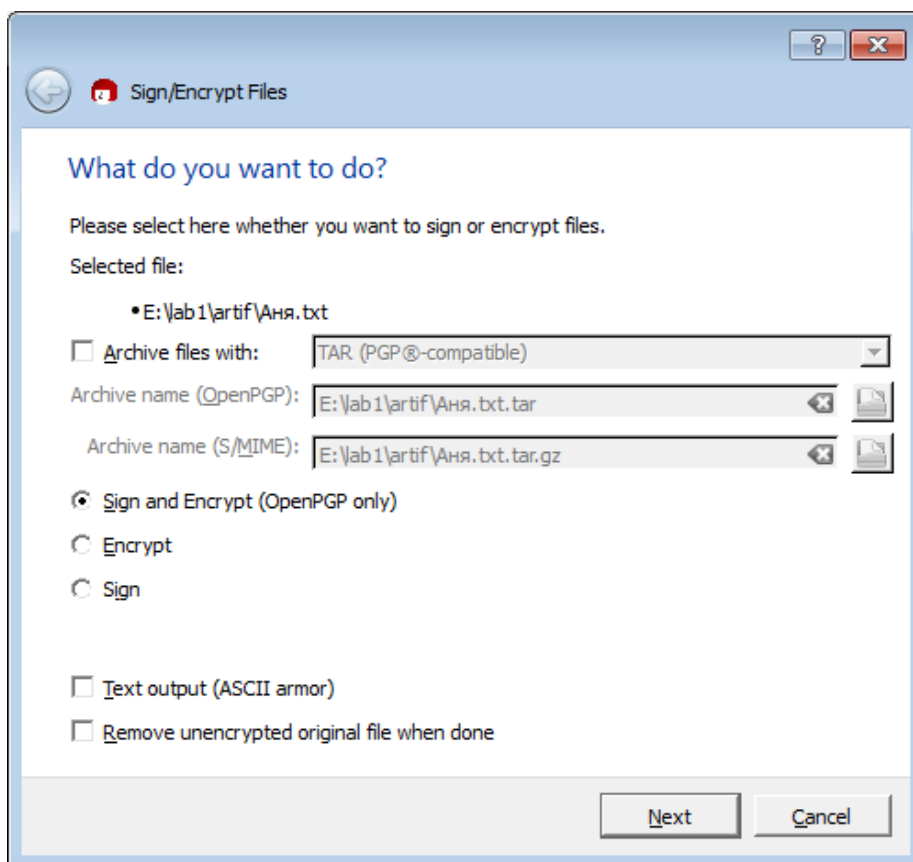


Рис. 16: Выбор параметров для шифрования файла.

```
sec 2048R/3729EB59 2016-02-29 SkripalBoris (none) <skripalboris@yandex.ru>
```

Создать сертификат отзыва данного ключа? (y/N) y

Укажите причину отзыва:

0 = Причина не указана

1 = Ключ был раскрыт

2 = Ключ заменен другим

3 = Ключ больше не используется

Q = Отмена

(Скорее всего, Вы здесь выберете 1)

Ваше решение? 0

Введите необязательное пояснение; закончите пустой строкой:

>

Причина отзыва: Причина не указана

(Пояснения отсутствуют)

Все правильно? (y/N) y

Необходима фраза-пароль для доступа к закрытому ключу пользователя: "SkripalBori

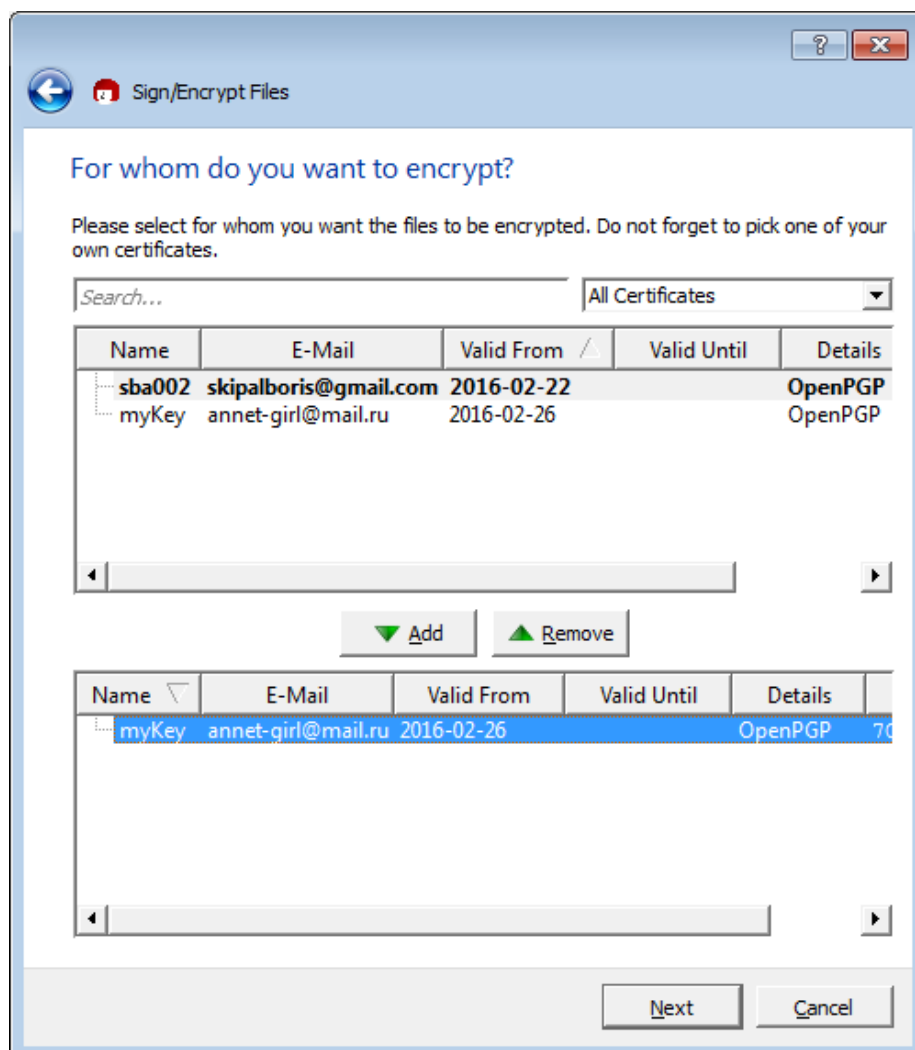


Рис. 17: Выбор сертификата для подписи и шифрования файла.

```
s (none) <skipalboris@yandex.ru>"
2048-битный ключ RSA, ID 3729EB59, создан 2016-02-29
```

Сертификат отзыва создан.

Для симметричного шифрования файла используется ключ "-symmetric".  
Создадим файл "SkrpalSec.txt" и зашифруем его при помощи закрытого ключа.

```
gpg --symmetric SkripalSec.txt
```

После этого в папке появится файл SkripalSec.txt.gpg

```
dir
```

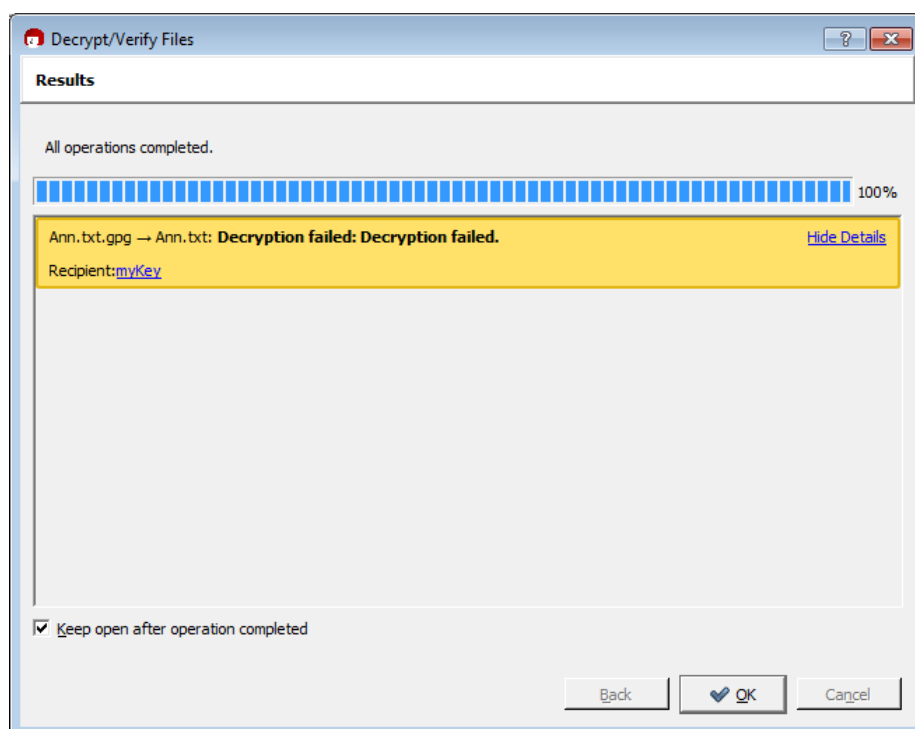


Рис. 18: Ошибка при попытке расшифровать файл открытым сертификатом другого человека.

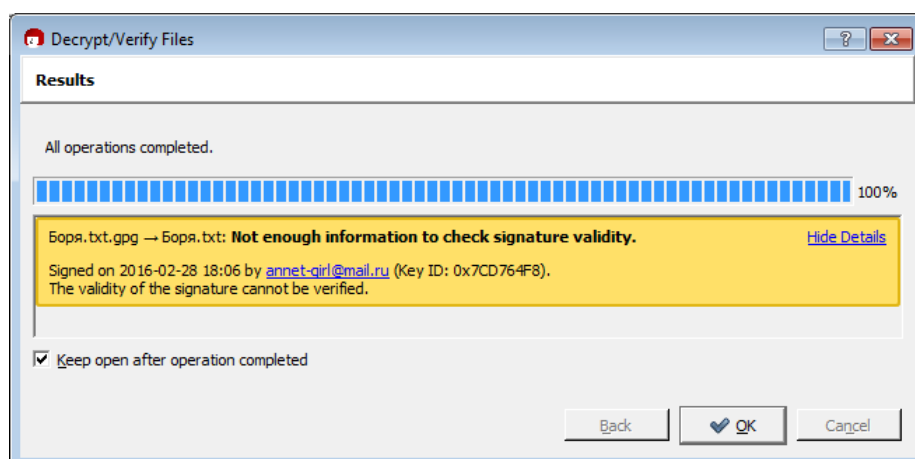


Рис. 19: Сообщение о удачной дешифровке файлов.

28.02.2016	17:20	<DIR>	.
28.02.2016	17:20	<DIR>	..
28.02.2016	16:52		7 SkripalSec.txt
28.02.2016	17:20		60 SkripalSec.txt.gpg



Для расшифровки файла необходимо использовать ключ "-decrypt".

```
C:\Users\sba\Downloads\lab1>gpg --decrypt SkripalSec.txt.gpg
gpg: данные зашифрованы алгоритмом CAST5
gpg: зашифровано одной фразой-паролем
Hello!
gpg: ВНИМАНИЕ: целостность сообщения не защищена
```