Санкт-Петербургский государственный политехнический университет

Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

ОТЧЕТ

о лабораторной работе №1

по дисциплине: «Информационная безопасность»

Тема работы: «Программа для шифрования и подписи GPG»

Работу выполнил студент

53501/3 *Алексюк Артём*

Преподаватель

_____ *Вылегжанина Карина Дмитриевна*

Санкт-Петербург
2016

1. Цель работы

1) Установить и настроить пакет GPG 2
2) Создать набор ключей в Kleopatra
3) Экспортировать свой ключ, импортировать ключ другого участника эксперимента
4) Зашифровать файл и отправить другому человеку, расшифровать чужой файл
5) Выполнить те же пункты, используя консольный интерфейс

2. Ход работы

2.1. Использование GPG с помощью интерфейса Kleopatra

Установим необходимые инструменты:

```
[language=bash,caption={Установка GPG}]
artyom@gpg:~$ sudo apt-get install kleopatra gnupg2
```

Запустим Kleopatra. Перед нами появится главное окно:

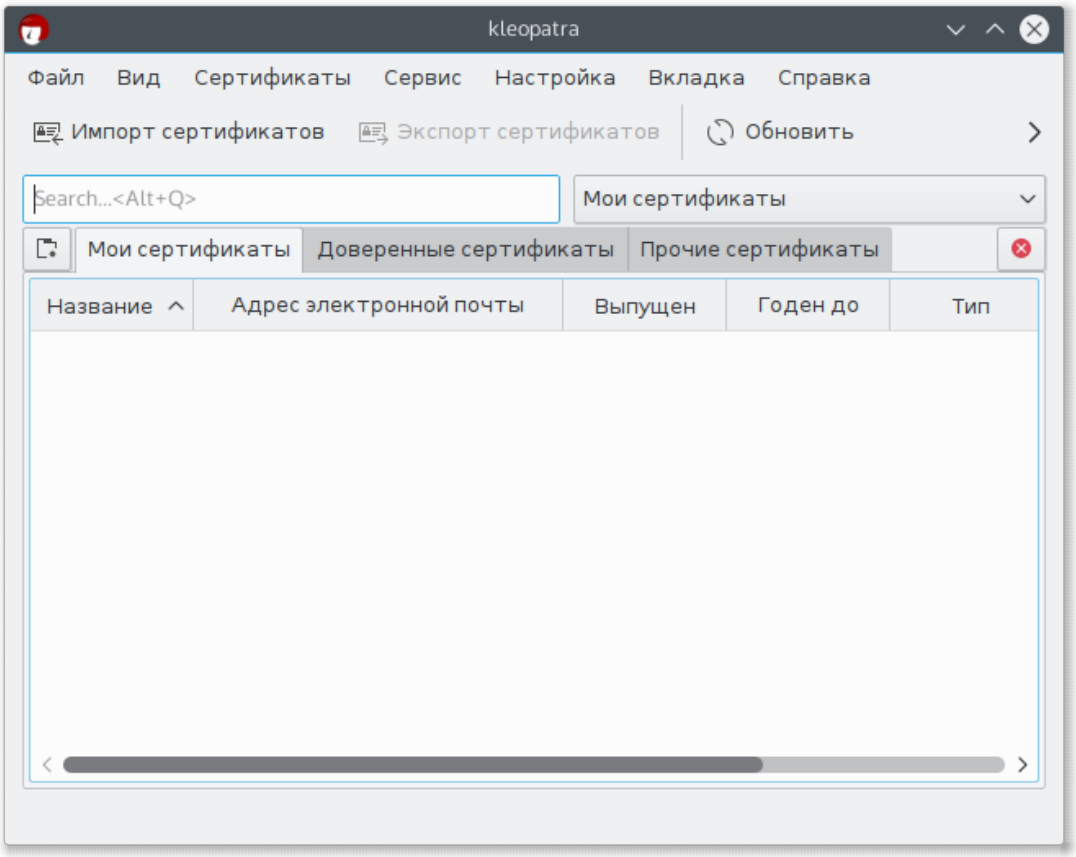

Рис. 1: Главное окно программы Kleopatra

Через меню «Файл» запустим мастер создания ключа

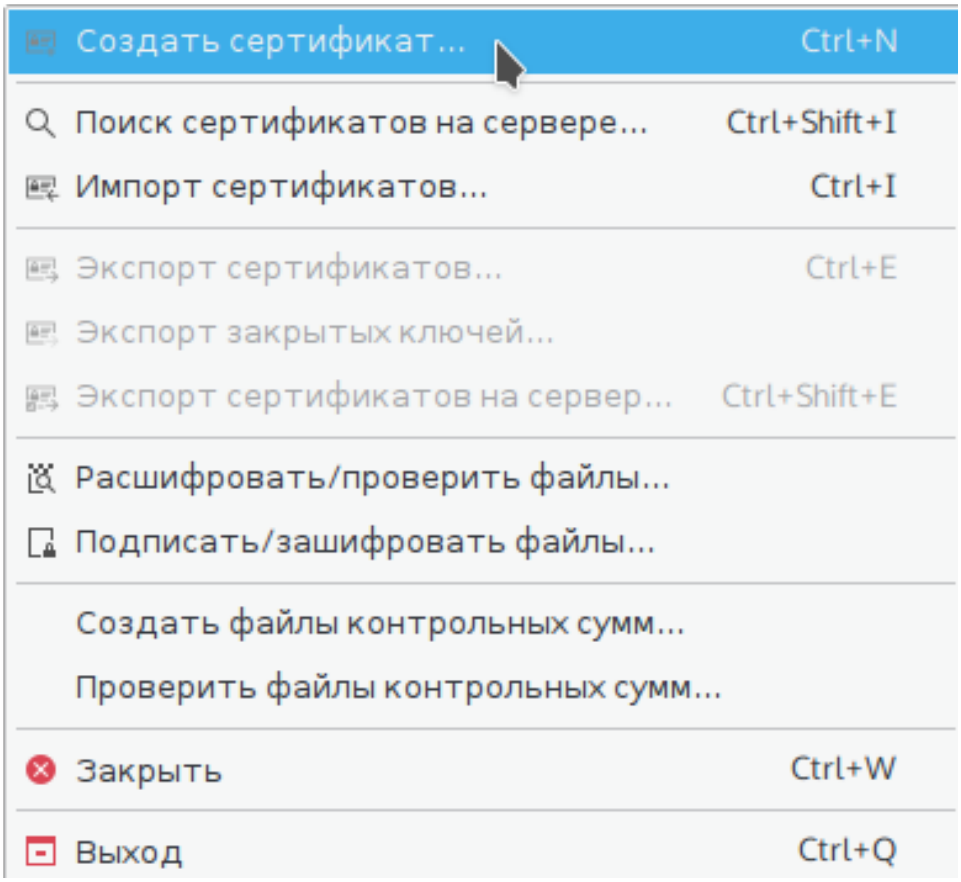

Рис. 2: Меню «Файл»

В данной работе нас интересуют ключи PGP, поэтому выберем первый пункт.

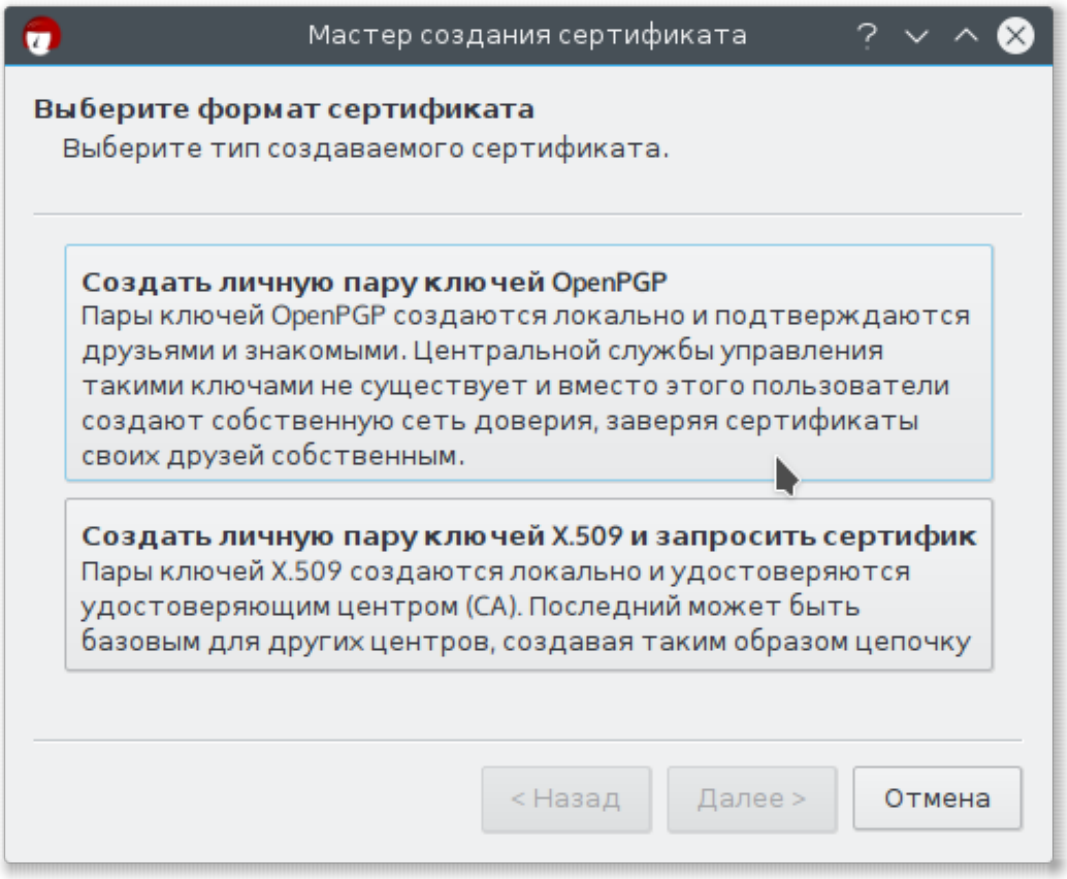

Рис. 3: Создание ключа

Укажем свои реквизиты

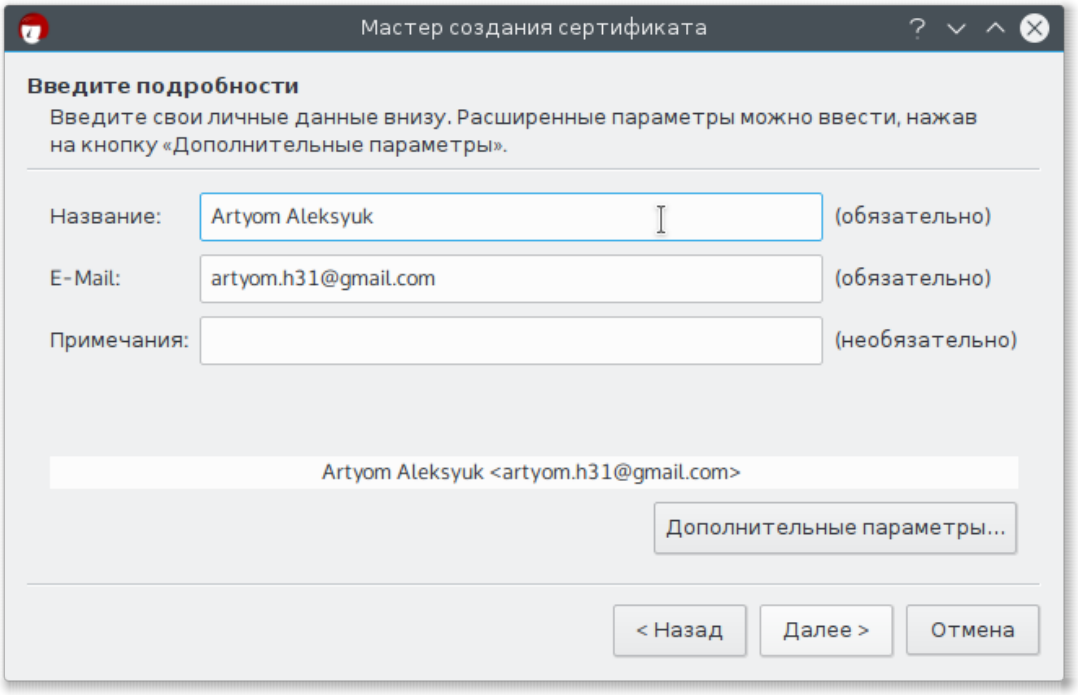

Рис. 4: Создание ключа

В дополнительных параметрах проверим, что используются достаточная длина ключа, а также ограничим срок годности ключа.

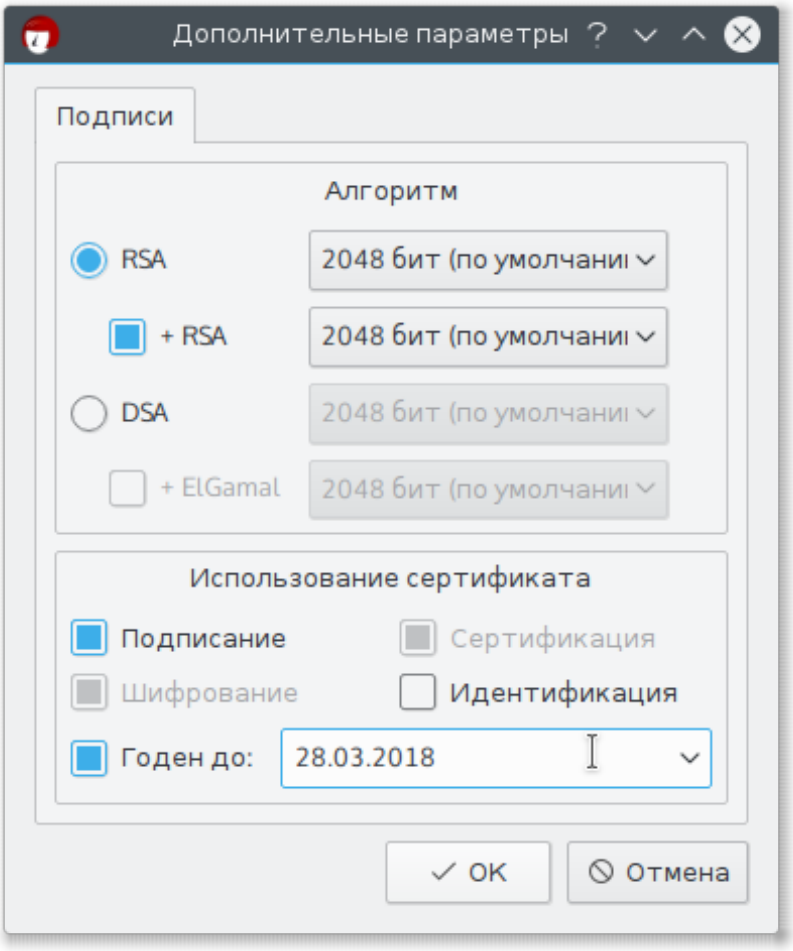

Рис. 5: Создание ключа

Введем пароль

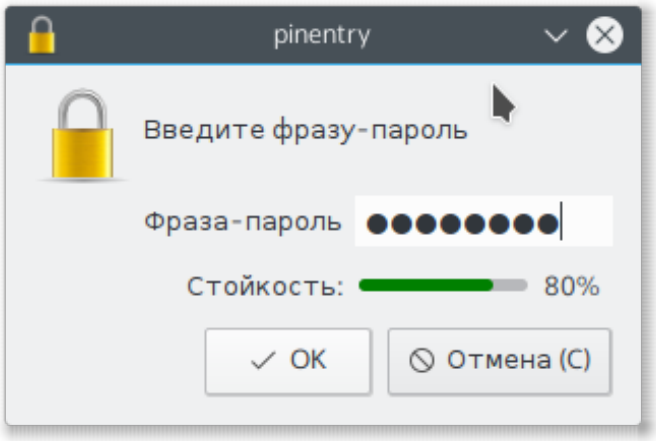

Рис. 6: Создание ключа

Voilà!

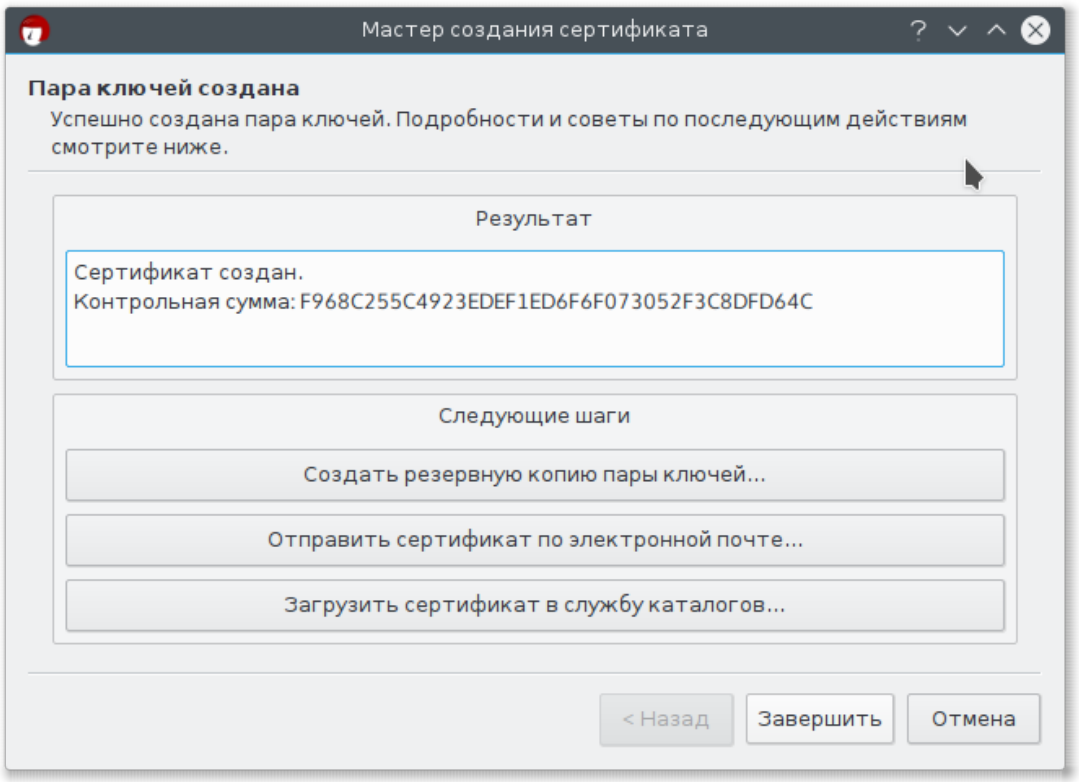

Рис. 7: Создание ключа

Наш ключ появился в списке

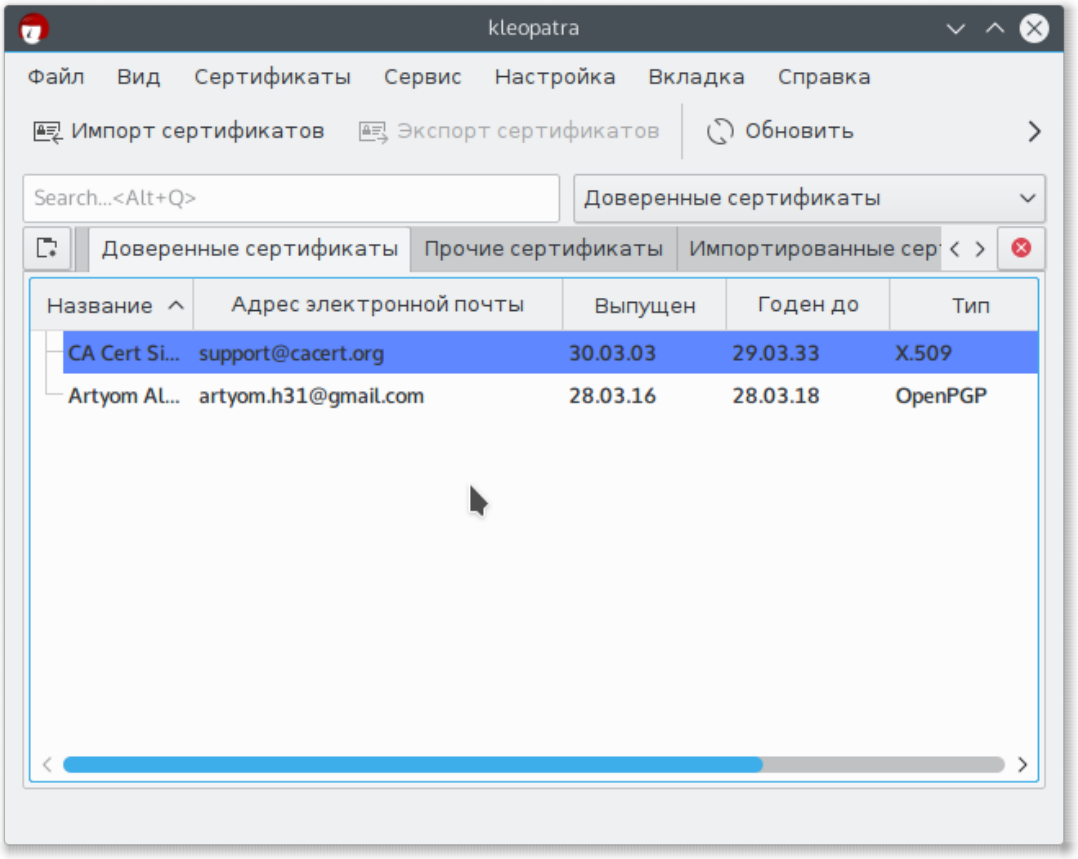

Рис. 8: Ключи

Получим сертификат от другого участника эксперимента, импортируем его.

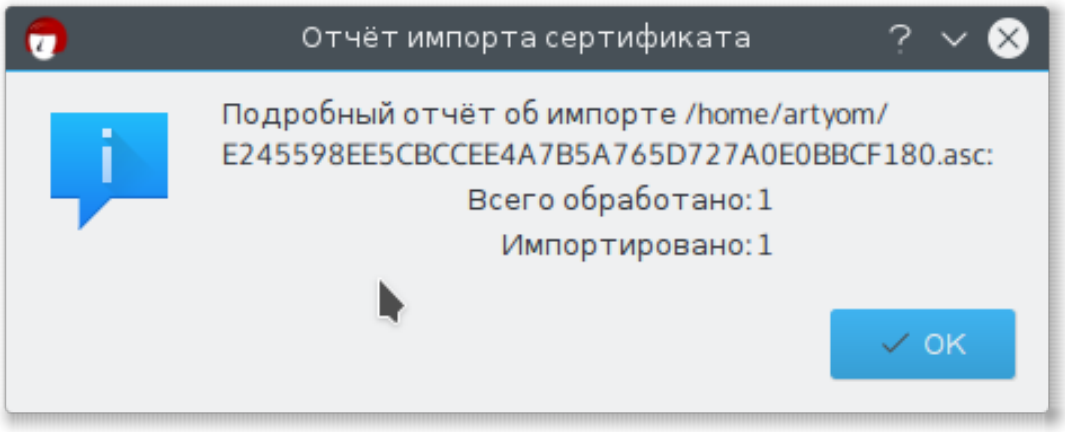

Рис. 9: Импорт сертификата

Видим его в списке

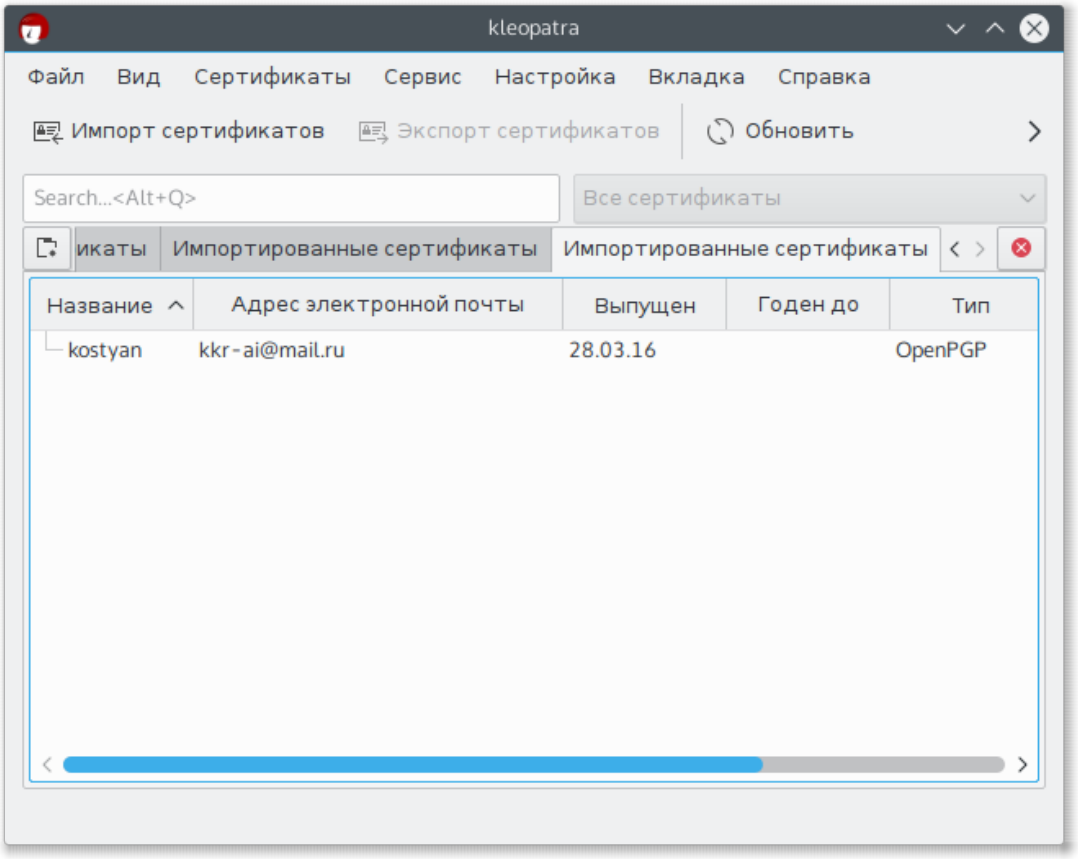

Рис. 10: Сертификаты

Зашифруем файл. Для удобства обмена включим использование текстового представления зашифрованных данных.

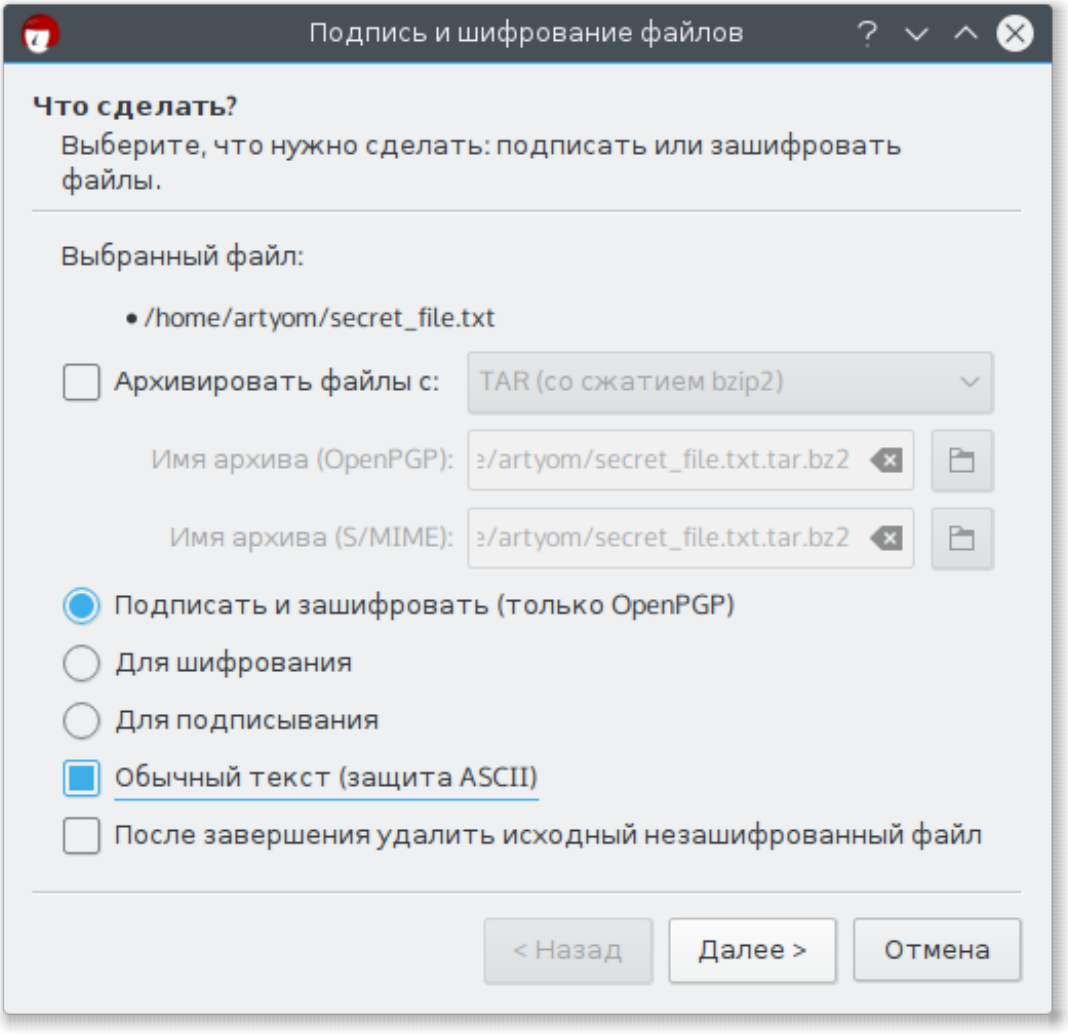

Рис. 11: Шифрование

Выберем свой и чужой ключ

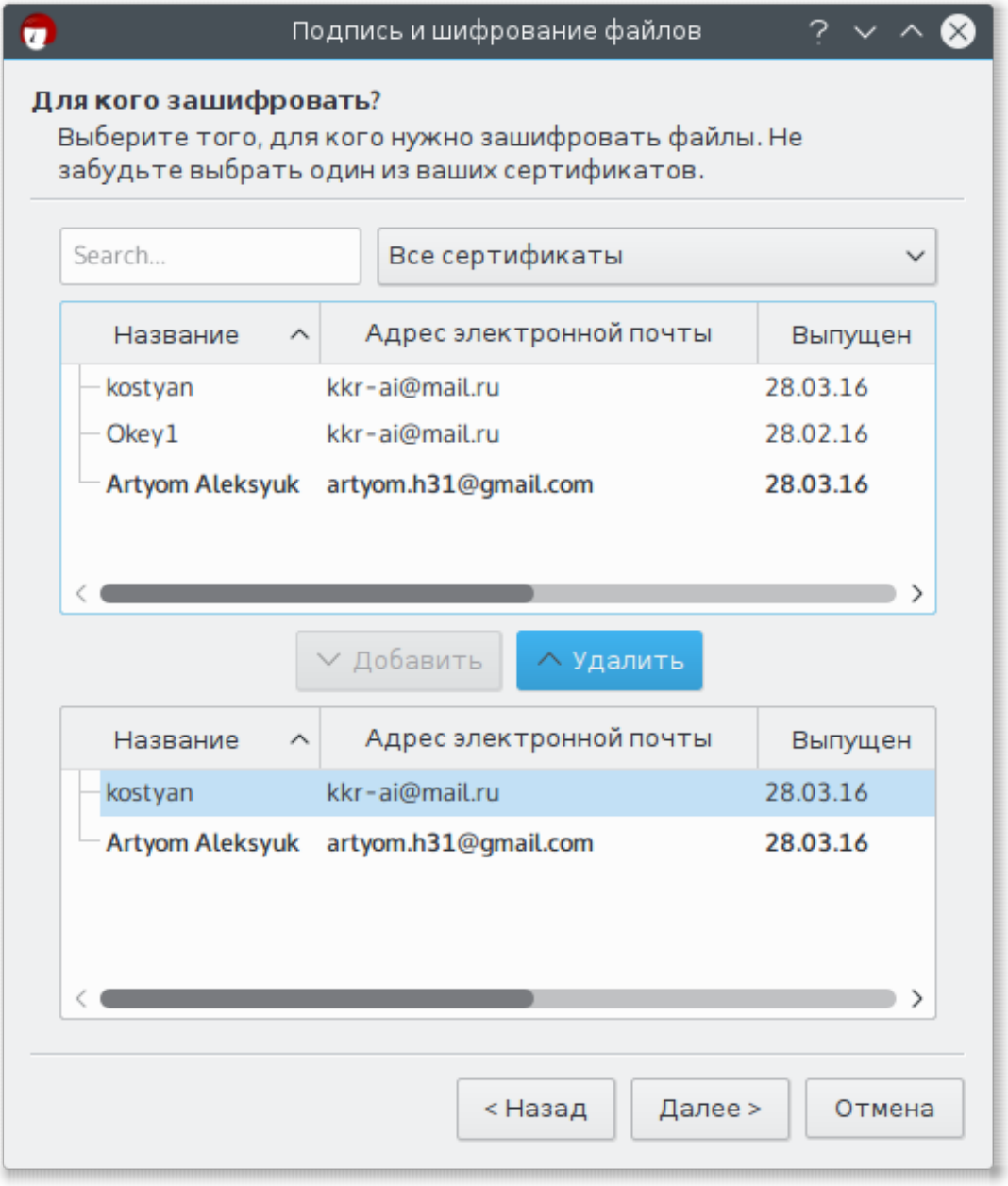

Рис. 12: Шифрование

Выберем открытый ключ, с помощью которого будем шифровать

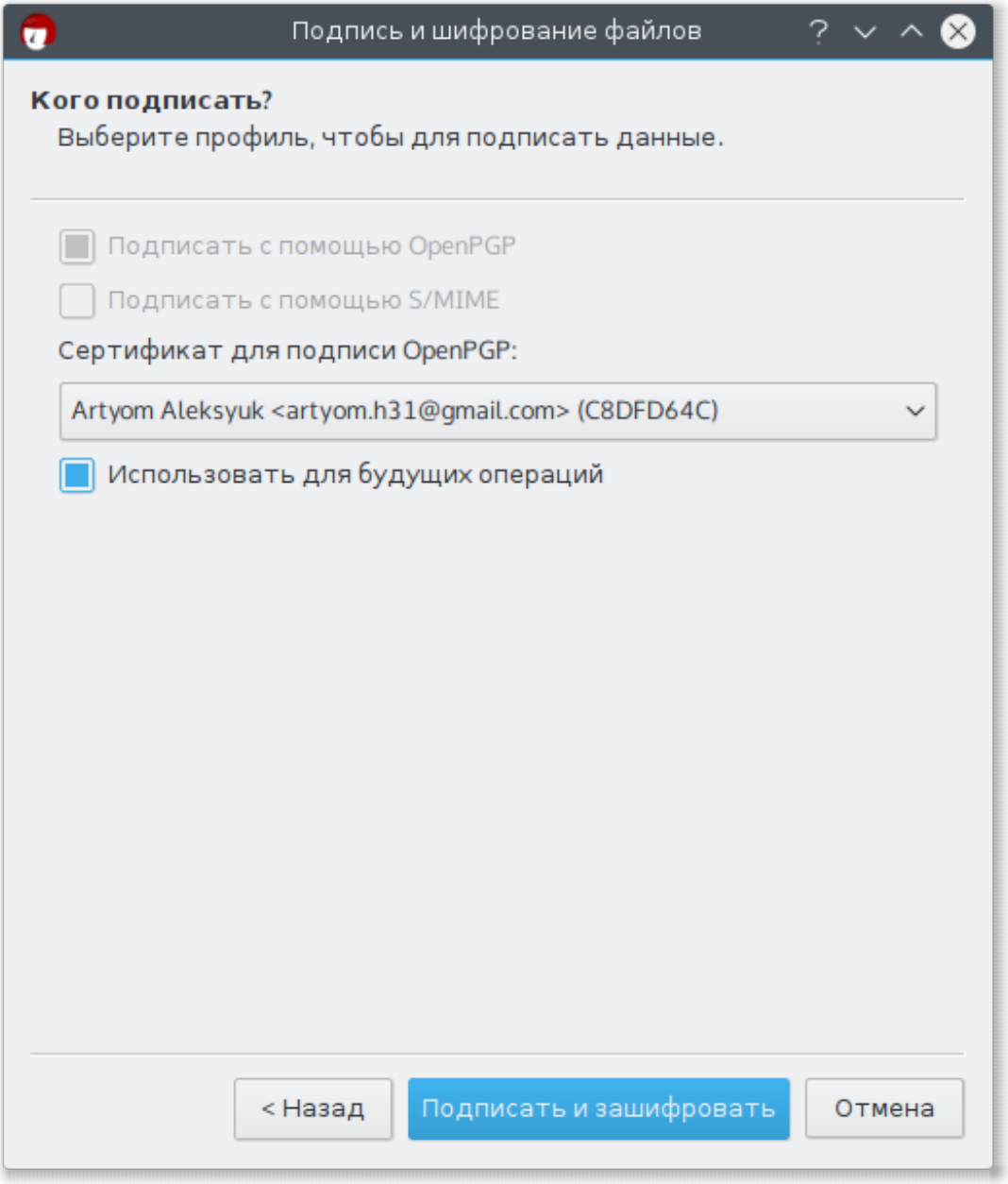

Рис. 13: Шифрование

Сообщение об успехе

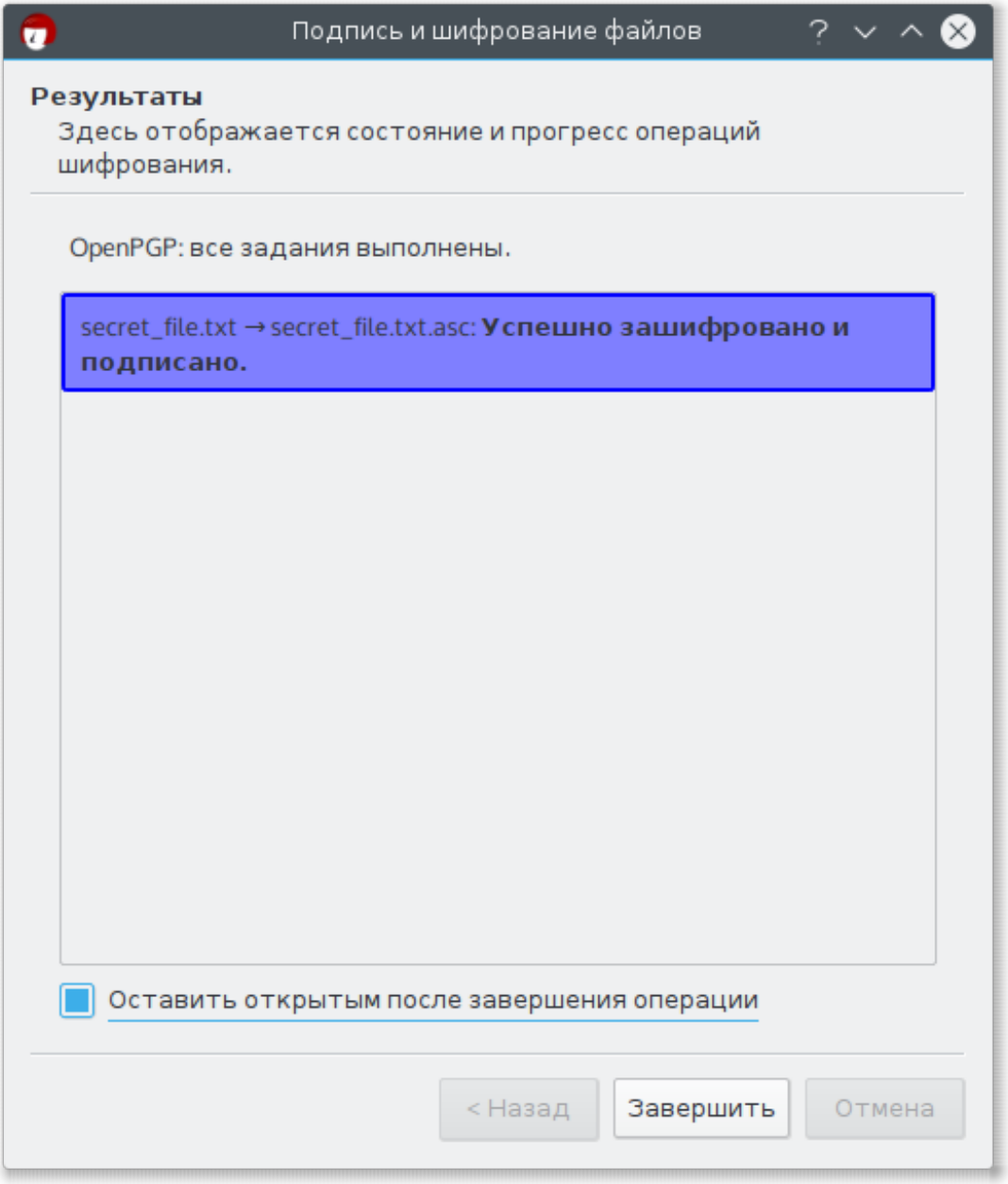

Рис. 14: Шифрование

Так выглядит зашифрованный файл

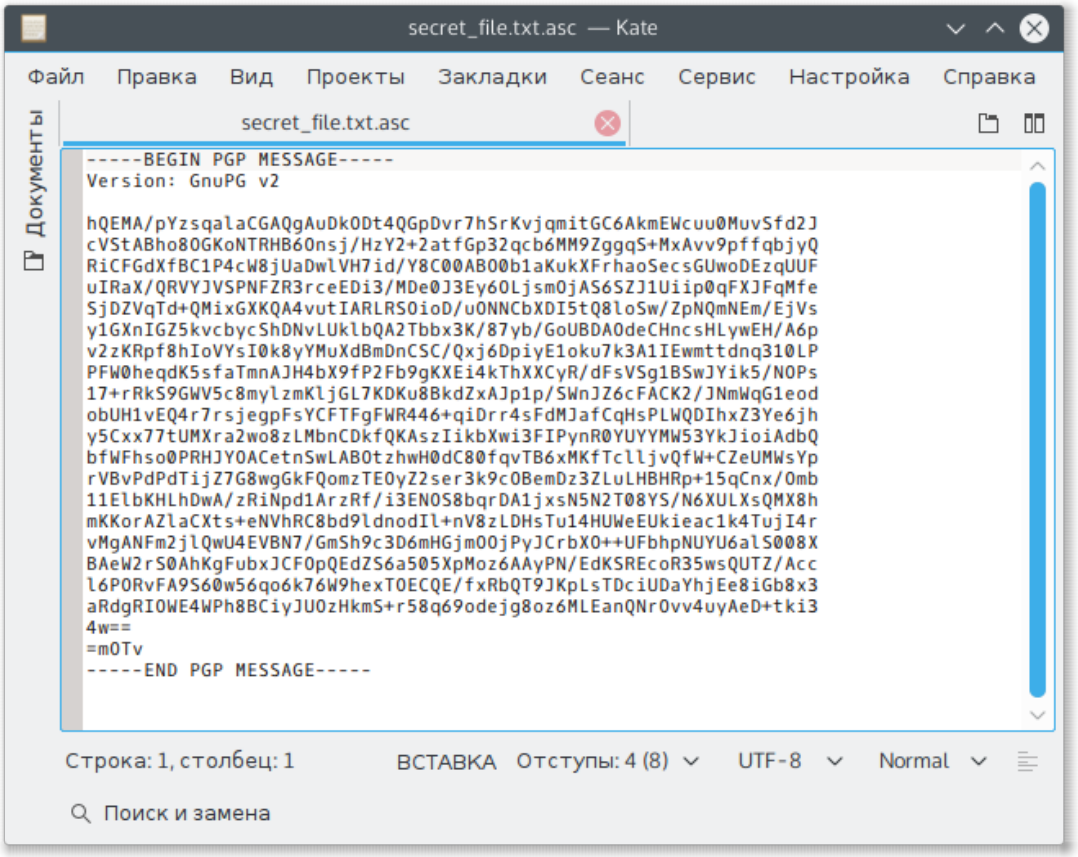

Рис. 15: Зашифрованный файл

Теперь попробуем расшифровать файл, для этого запустим мастер из меню «Файл».

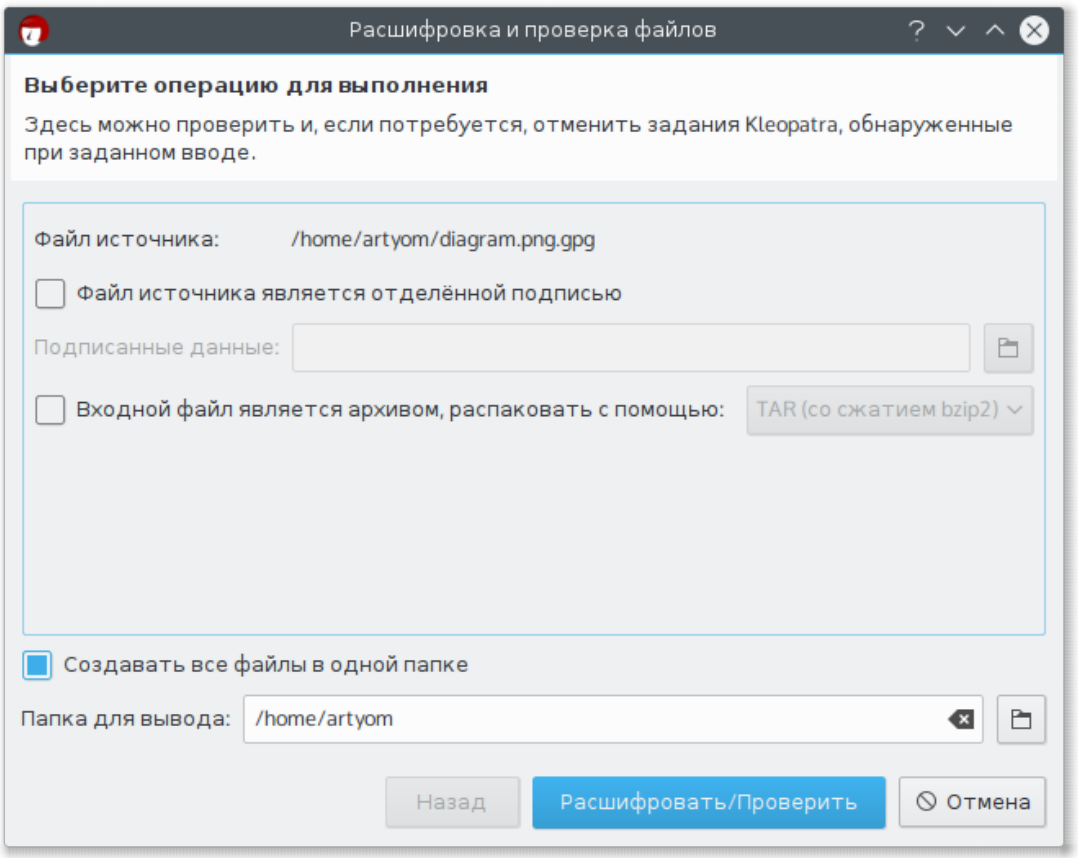

Рис. 16: Расшифровка

Так быстро?

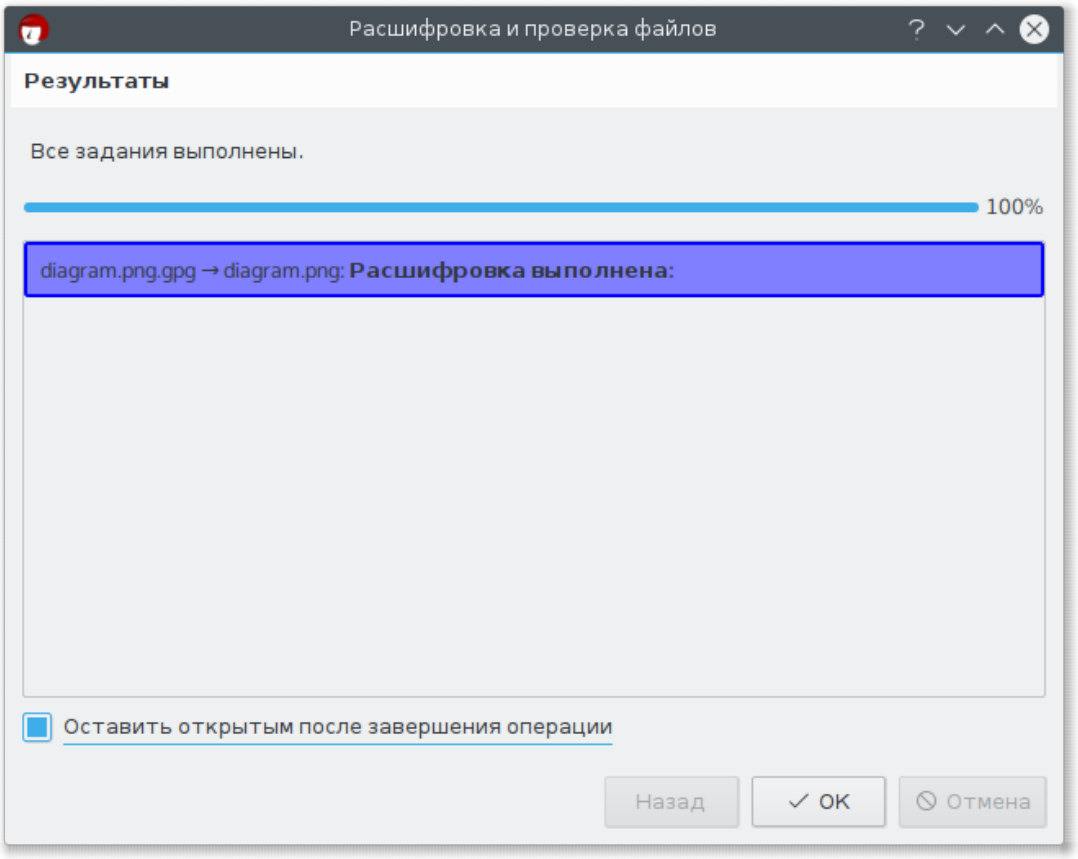

Рис. 17: Расшифровка

Ниже представлено расшифрованное изображение

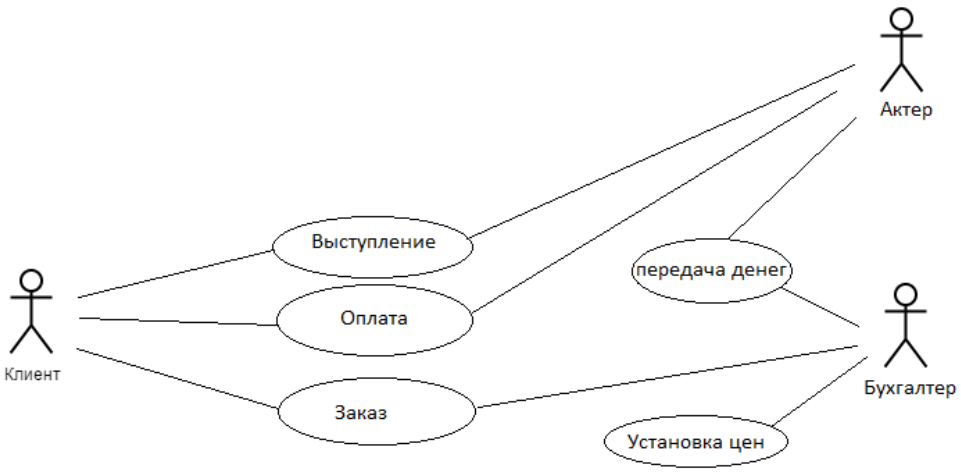

Рис. 18: Расшифрованное изображение

2.2. Использование GPG с помощью консольного интерфейса

Эксперименты будут проводиться на другой машине. Попробуем вывести список ключей.

```
artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --list-keys
```

Пусто. Нужно создать новый ключ.

```
artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --gen-key
gpg (GnuPG) 2.0.28; 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) 2y
Ключ действителен до Ср. 28 марта 2018 00:55:57 MSK
Все верно? (y/N) y

GnuPG необходимо составить ID пользователя в качестве идентификатора
 ключа.

Ваше настоящее имя: Artyom Aleksyuk
Адрес электронной почты: artyom.h31@gmail.com
Комментарий:
Вы выбрали следующий ID пользователя:
"Artyom Aleksyuk <artyom.h31@gmail.com>"

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


(process:22404): GLib-WARNING **: /build/glib2.0-MuyBSS/glib2.0-2.46.2/
./glib/gmem.c:482: custom memory allocation vtable not supported

(process:22412): GLib-WARNING **: /build/glib2.0-MuyBSS/glib2.0-2.46.2/
./glib/gmem.c:482: custom memory allocation vtable not supported
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
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 92682E10 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:   1  подписанных:   0  доверие: 0-, 0q, 0n,
 0m, 0f, 1u
gpg: срок следующей проверки таблицы доверия 2018-03-27
pub   2048R/92682E10 2016-03-27 [годен до: 2018-03-27]
Отпечаток ключа = 3642 F44F 0375 4B21 A4A1  F188 2704 20BB 9268 2E10
uid     [абсолютное] Artyom Aleksyuk <artyom.h31@gmail.com>
sub   2048R/9AAC34E0 2016-03-27 [годен до: 2018-03-27]
artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --list-keys
/home/artyom/.gnupg/pubring.gpg
------------------------------
pub   2048R/92682E10 2016-03-27 [годен до: 2018-03-27]
uid     [абсолютное] Artyom Aleksyuk <artyom.h31@gmail.com>
sub   2048R/9AAC34E0 2016-03-27 [годен до: 2018-03-27]
```

В списке появился новый ключ:

```
artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --list-keys
/home/artyom/.gnupg/pubring.gpg
------------------------------
pub   2048R/92682E10 2016-03-27 [годен до: 2018-03-27]
uid     [абсолютное] Artyom Aleksyuk <artyom.h31@gmail.com>
sub   2048R/9AAC34E0 2016-03-27 [годен до: 2018-03-27]
```

Экспортируем его.

```
artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --export
 --armor 92682E10
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2
...
```

Попробуем зашифровать файл. Связь с другим участником эксперимента прервалась (вероятно, владельцы переданного ему секрета уже приехали за ним), поэтому в качестве получателя будет машина, на которая проводилась первая часть экспериментов.

Импортируем ключ:

```
artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2
 --import ~/Downloads/F968C255C4923EDEF1ED6F6F073052F3C8DFD64C.asc
gpg: ключ C8DFD64C: импортирован открытый ключ "Artyom Aleksyuk
 <artyom.h31@gmail.com>"
gpg: Всего обработано: 1
gpg:               импортировано: 1  (RSA: 1)
artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --list-keys
/home/artyom/.gnupg/pubring.gpg
------------------------------
pub   2048R/92682E10 2016-03-27 [годен до: 2018-03-27]
uid     [абсолютное] Artyom Aleksyuk <artyom.h31@gmail.com>
sub   2048R/9AAC34E0 2016-03-27 [годен до: 2018-03-27]

pub   2048R/C8DFD64C 2016-03-27 [годен до: 2018-03-28]
uid     [неизвестно] Artyom Aleksyuk <artyom.h31@gmail.com>
sub   2048R/72C1CBCB 2016-03-27 [годен до: 2018-03-28]
```

Запустим шифрование:

```
artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --armor
 --encrypt secret.txt
Не задан ID пользователя (можно использовать "-r").

Текущие получатели:

Введите ID пользователя. Пустая строка для завершения: C8DFD64C
gpg: 72C1CBCB: Нет свидетельств того, что данный ключ принадлежит
 названному пользователю

pub  2048R/72C1CBCB 2016-03-27 Artyom Aleksyuk <artyom.h31@gmail.com>
Отпечаток главного ключа: F968 C255 C492 3EDE F1ED  6F6F 0730 52F3
 C8DF D64C
Отпечаток подключа: 93B0 41C2 D4F3 17DC 0E25  3252 9D78 21E7 72C1 CBCB

Нет уверенности в том, что ключ принадлежит человеку, указанному
в ID пользователя ключа. Если Вы ТОЧНО знаете, что делаете,
можете ответить на следующий вопрос утвердительно.

Все равно использовать данный ключ? (y/N) y

Текущие получатели:
2048R/72C1CBCB 2016-03-27 "Artyom Aleksyuk <artyom.h31@gmail.com>"

Введите ID пользователя. Пустая строка для завершения:
```

В директории появился новый файл

```
artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ ls
log.txt  report.tex  secret.txt  secret.txt.asc
```

Импортируем открытый ключ на другой машине

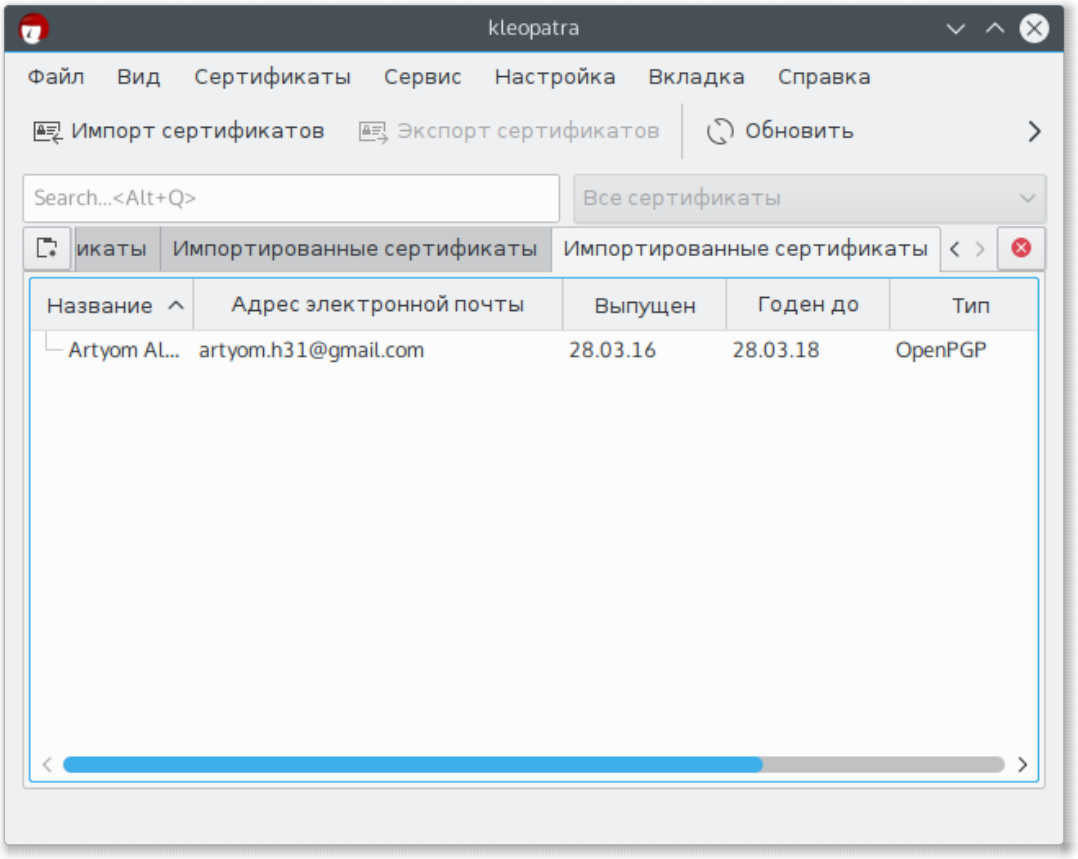

Рис. 19: Импорт ключа

Запустим расшифровку

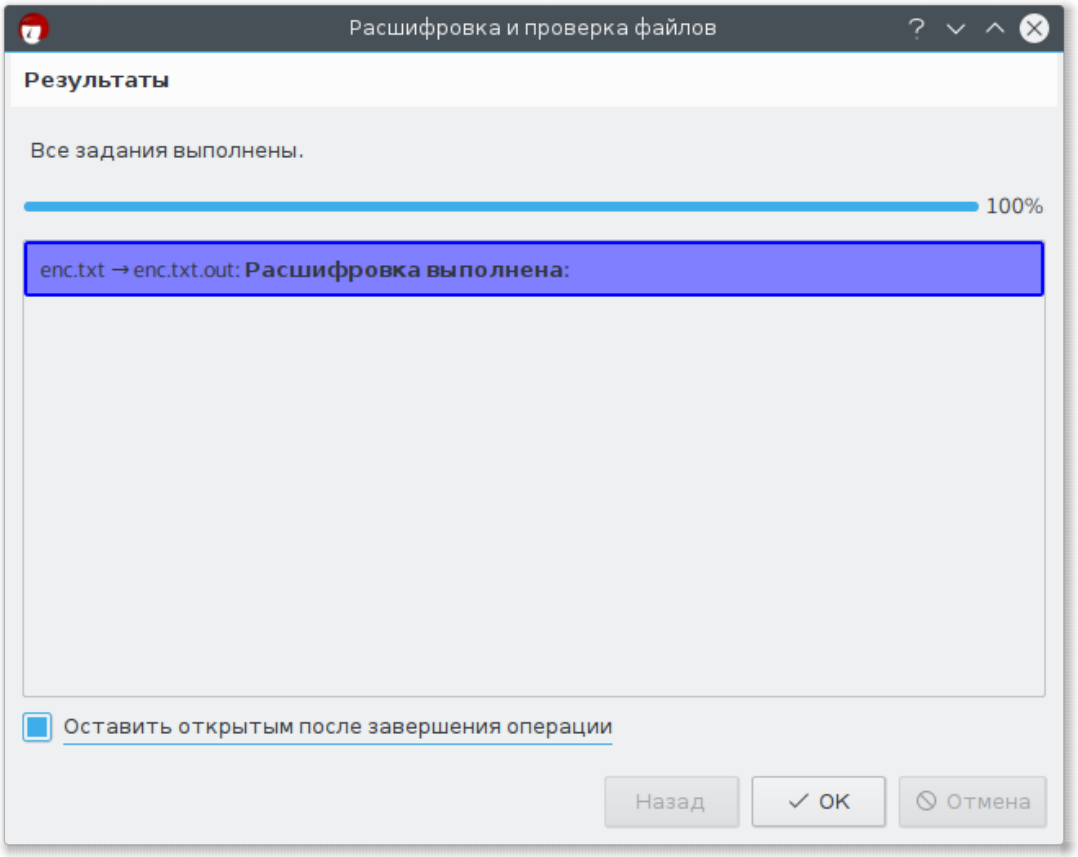

Рис. 20: Расшифровка

Проверим, что файл успешно расшифрован:

```
artyom@gpg:~$ cat enc.txt.out
Do you really expect to find a secret here?
```