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:

Листинг 1: Установка GPG

```
1 artyom@gpg:~$ sudo apt-get install kleopatra gnupg2
```

Запустим Kleopatra. Перед нами появится главное окно:

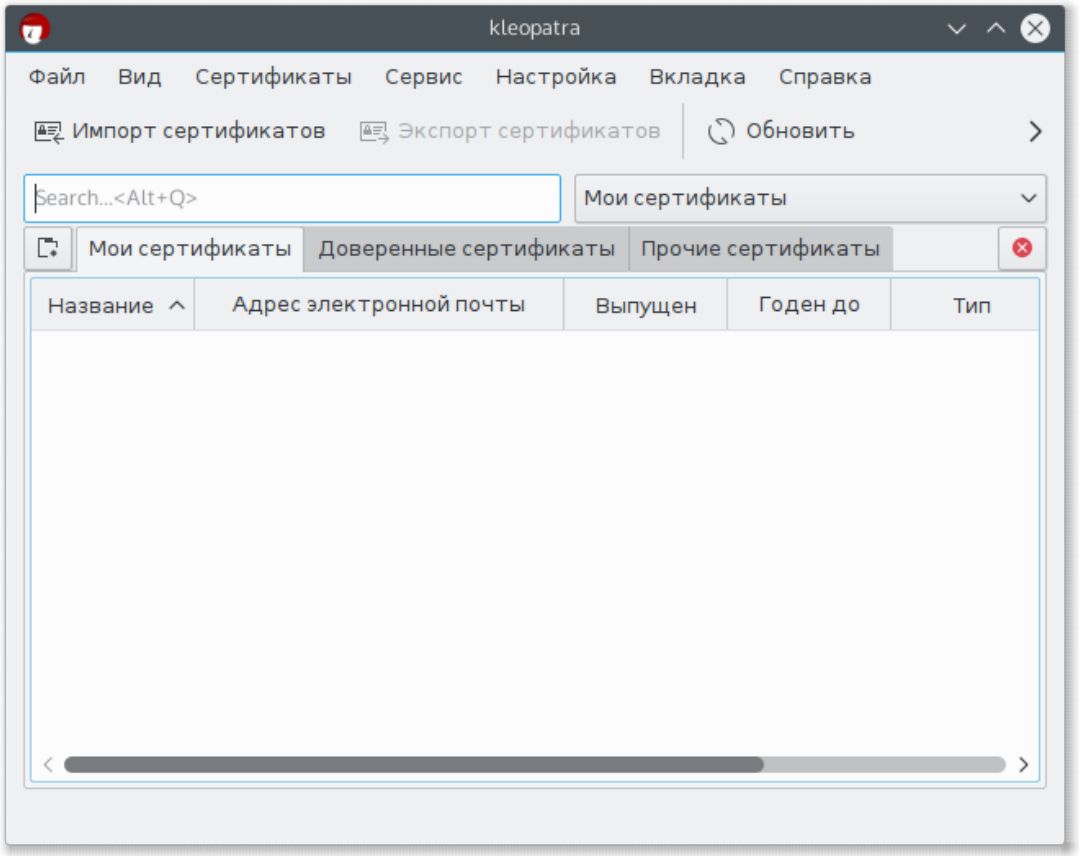

Рис. 1: Главное окно программы Kleopatra

Через меню «Файл» запустим мастер создания ключа

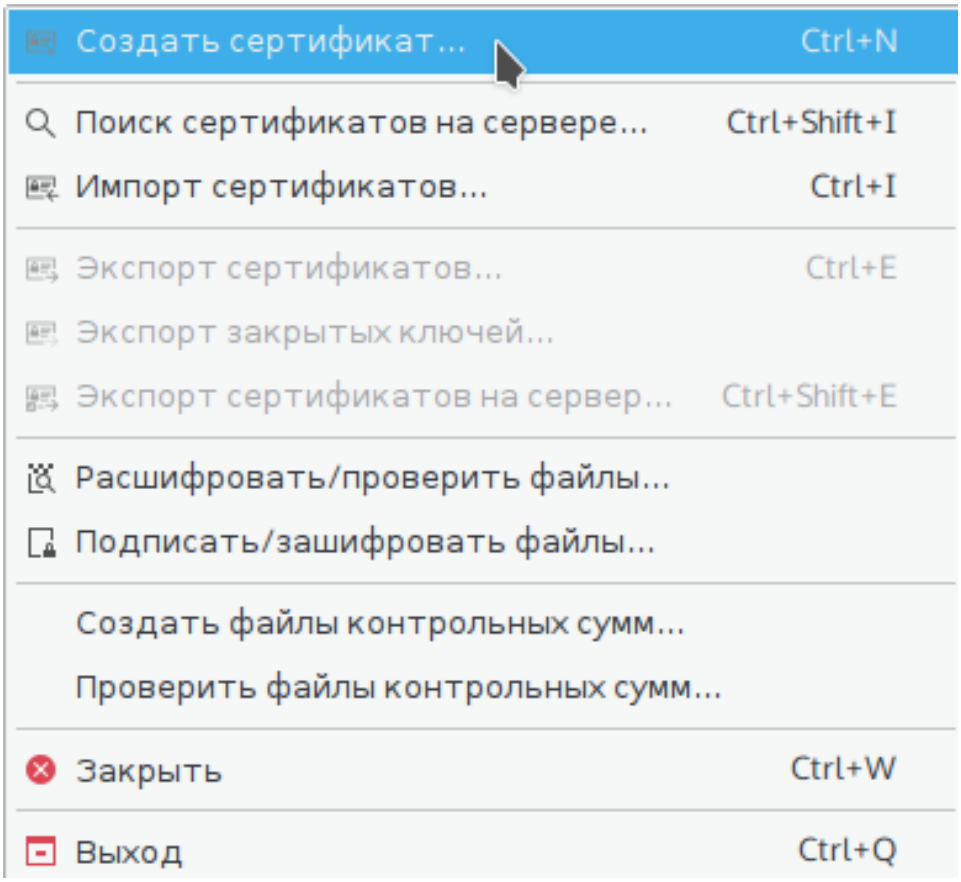

Рис. 2: Меню «Файл»

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

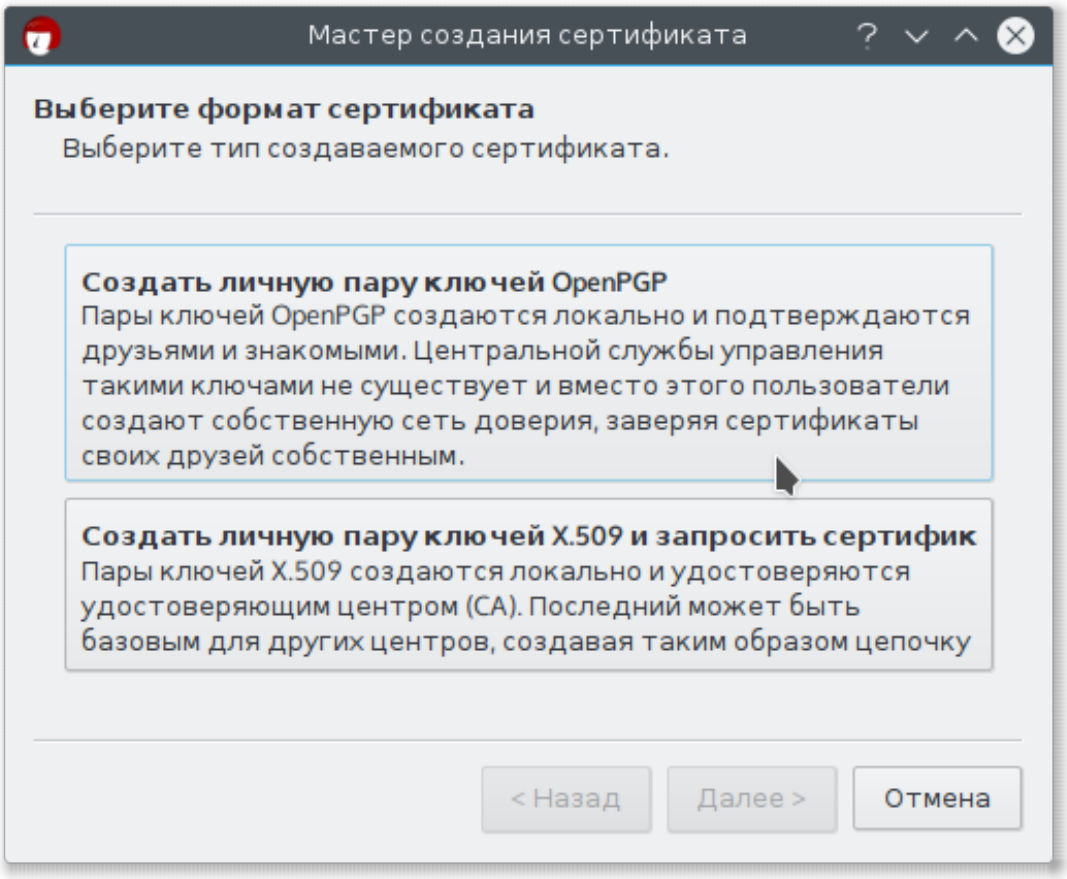

Рис. 3: Создание ключа

Укажем свои реквизиты

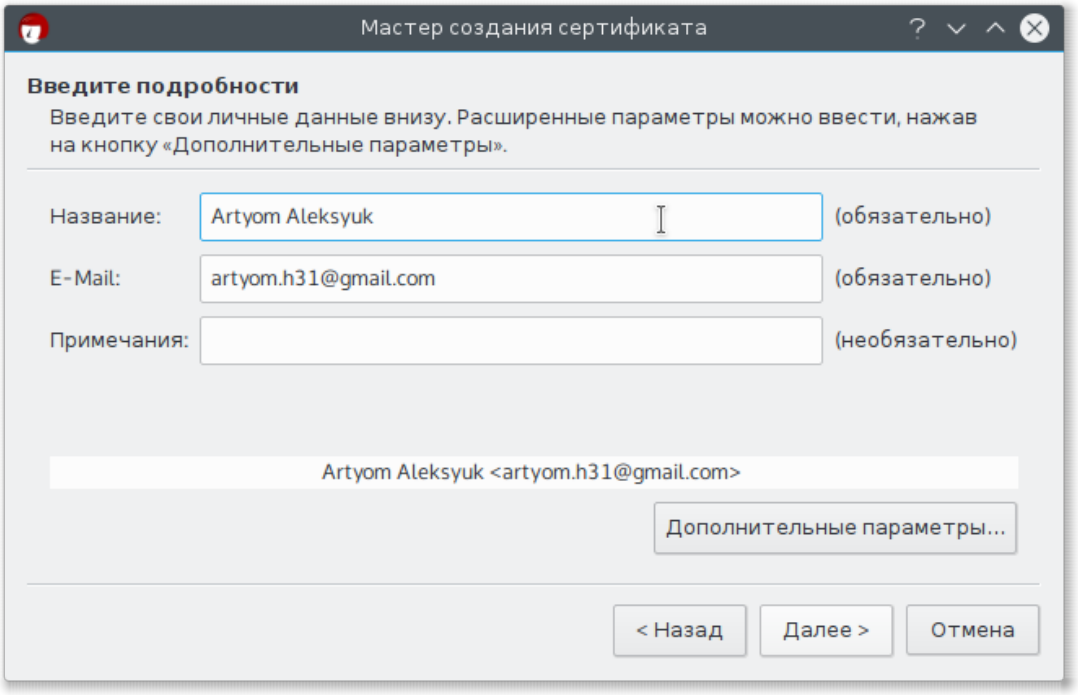

Рис. 4: Создание ключа

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

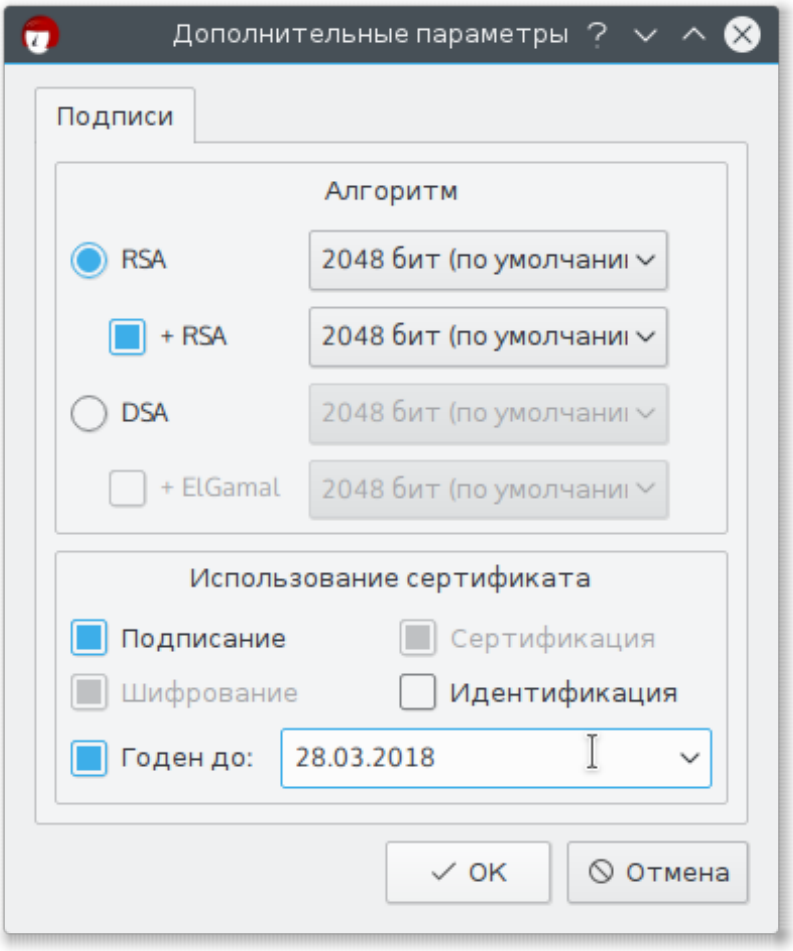

Рис. 5: Создание ключа

Введем пароль

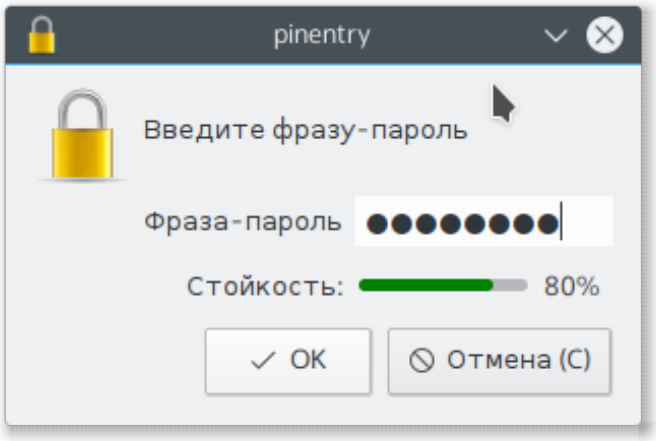

Рис. 6: Создание ключа

Voilà!

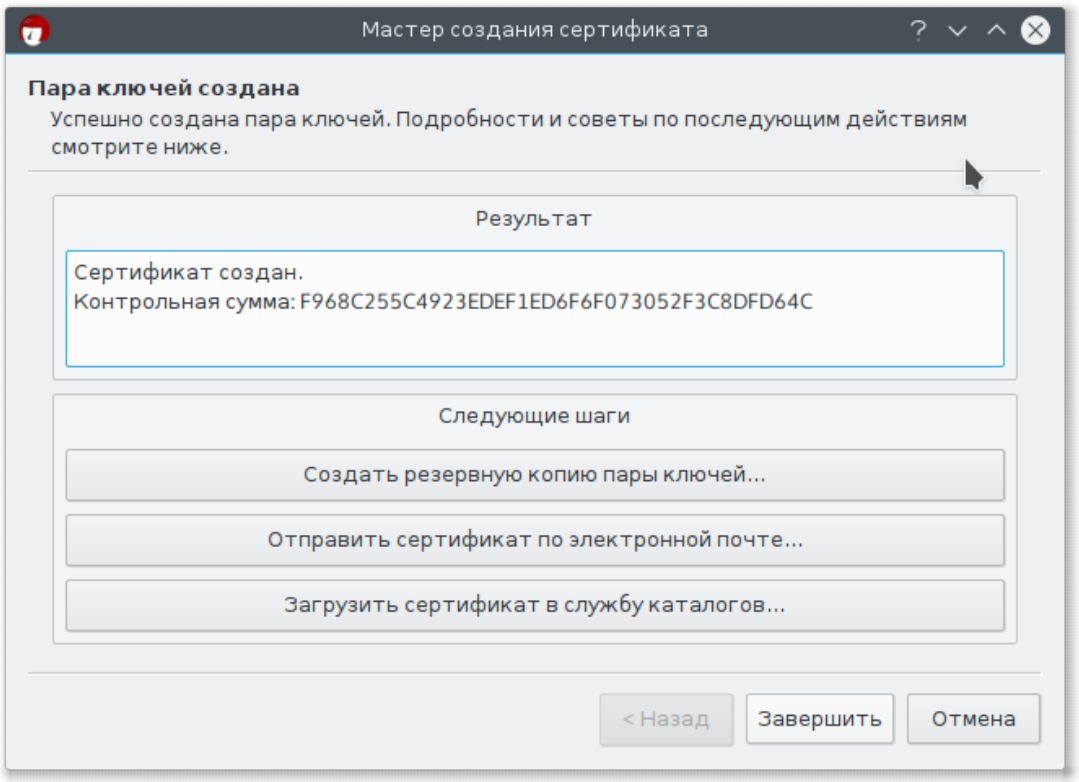

Рис. 7: Создание ключа

Наш ключ появился в списке

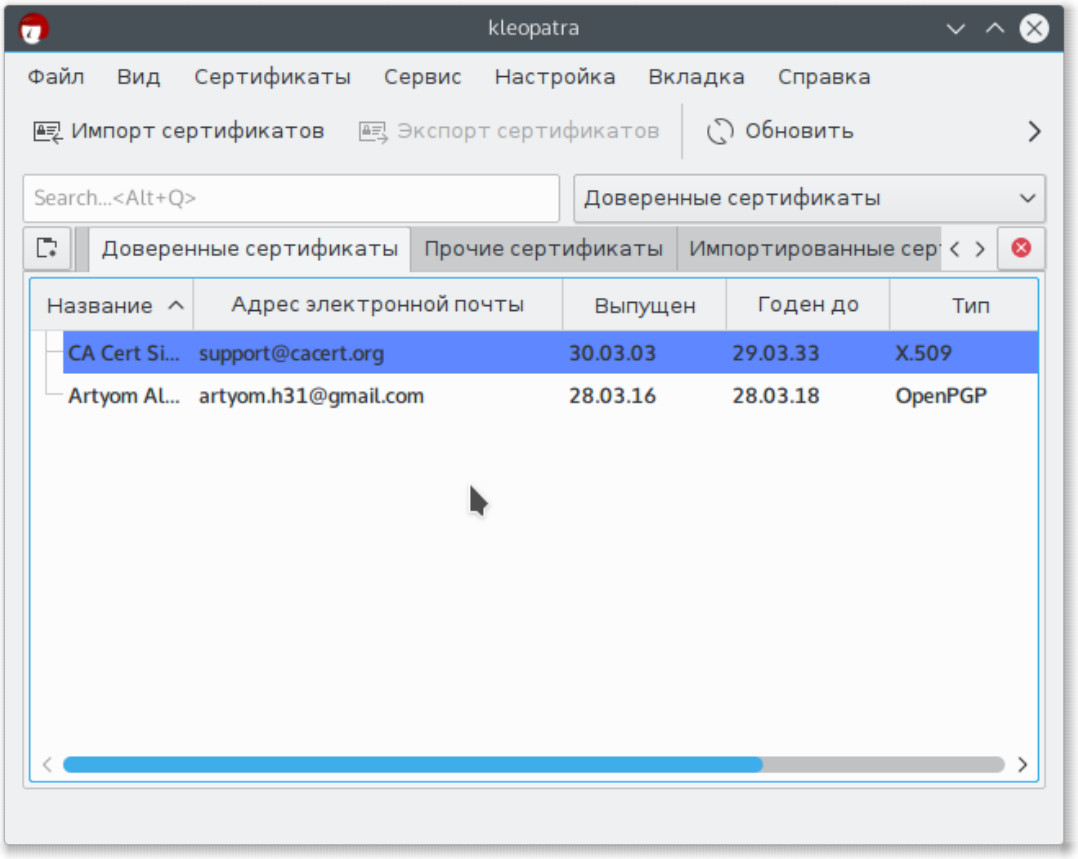

Рис. 8: Ключи

Получим сертификат от другого участника эксперимента, импортируем его.

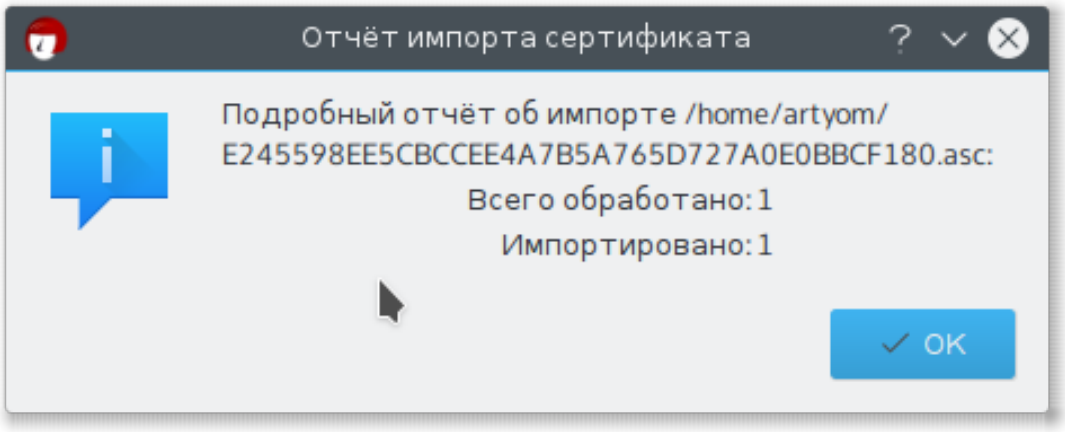

Рис. 9: Импорт сертификата

Видим его в списке

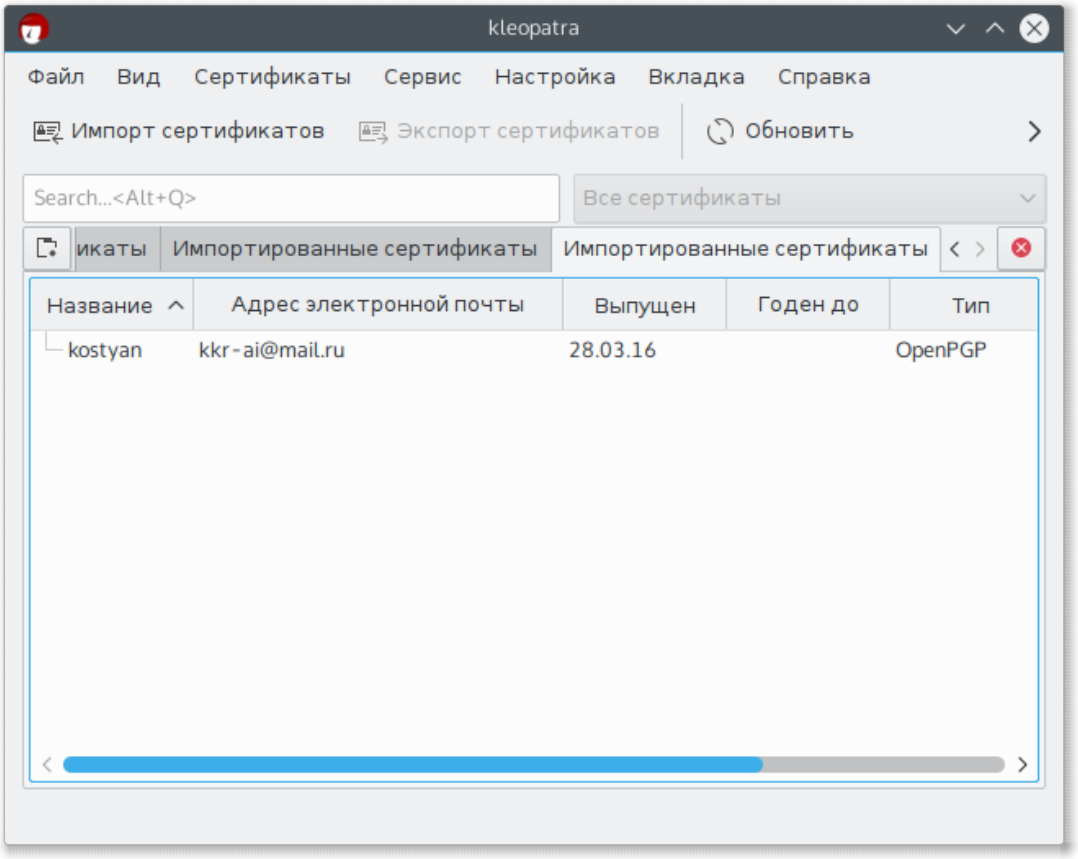

Рис. 10: Сертификаты

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

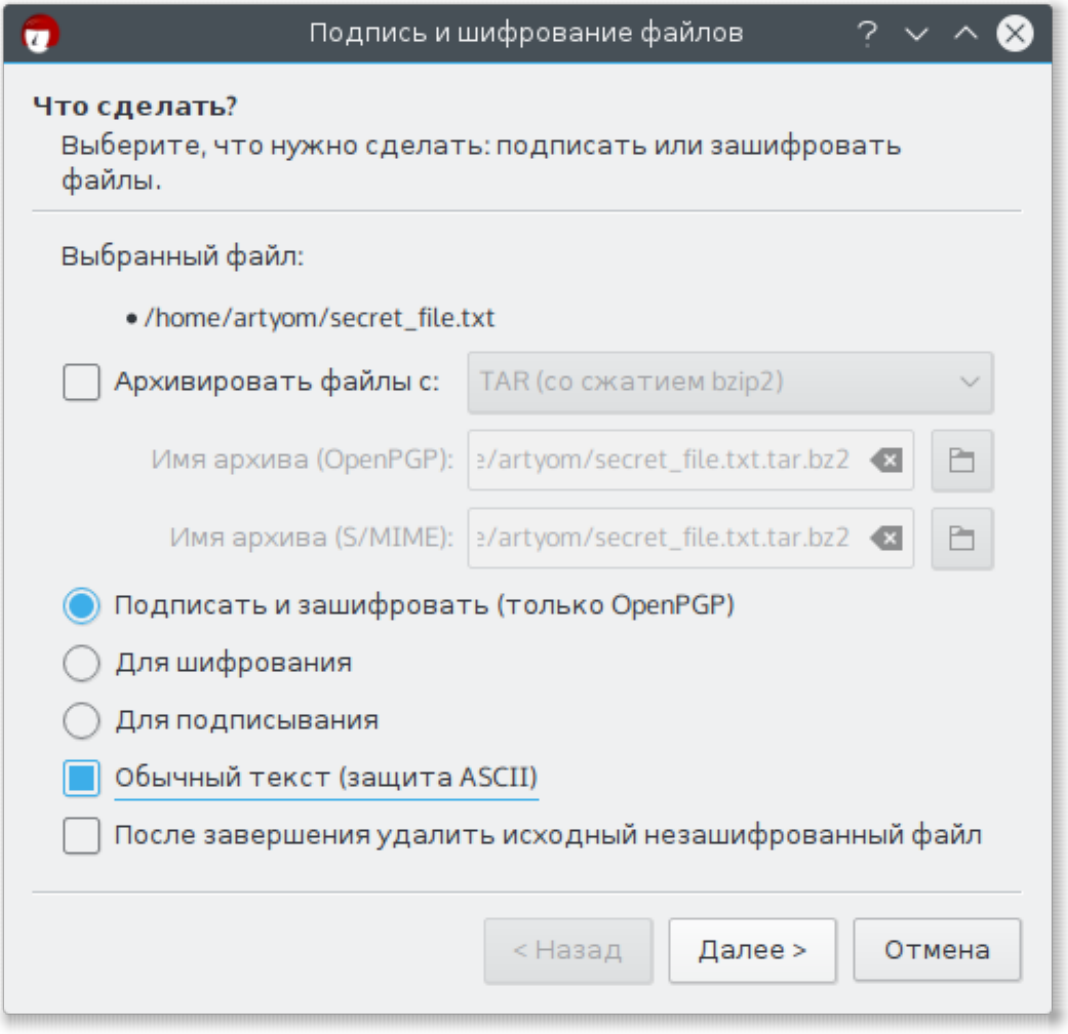

Рис. 11: Шифрование

Выберем свой и чужой ключ

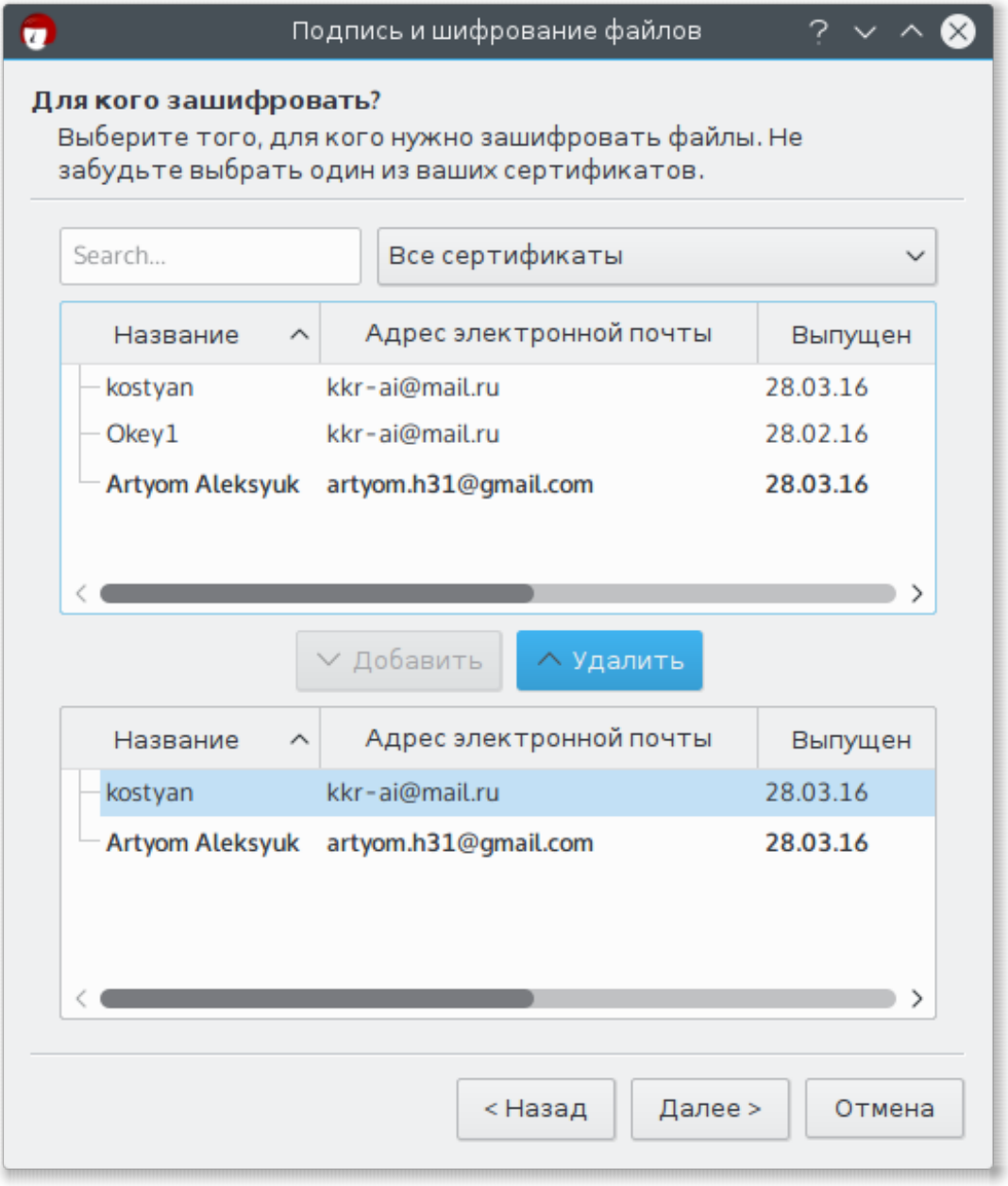

Рис. 12: Шифрование

Выберем открытый ключ, с помощью которого будем шифровать

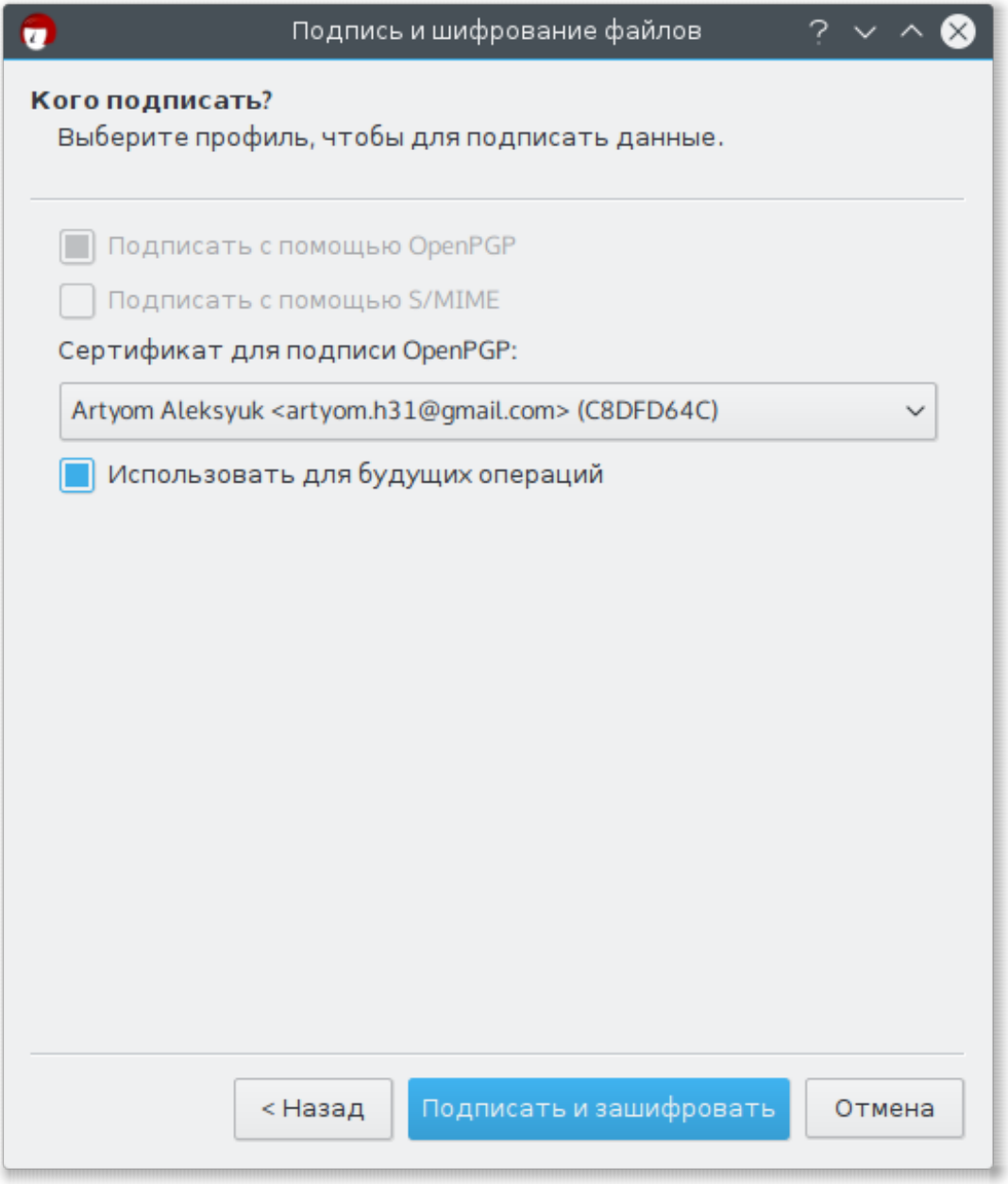

Рис. 13: Шифрование

Сообщение об успехе

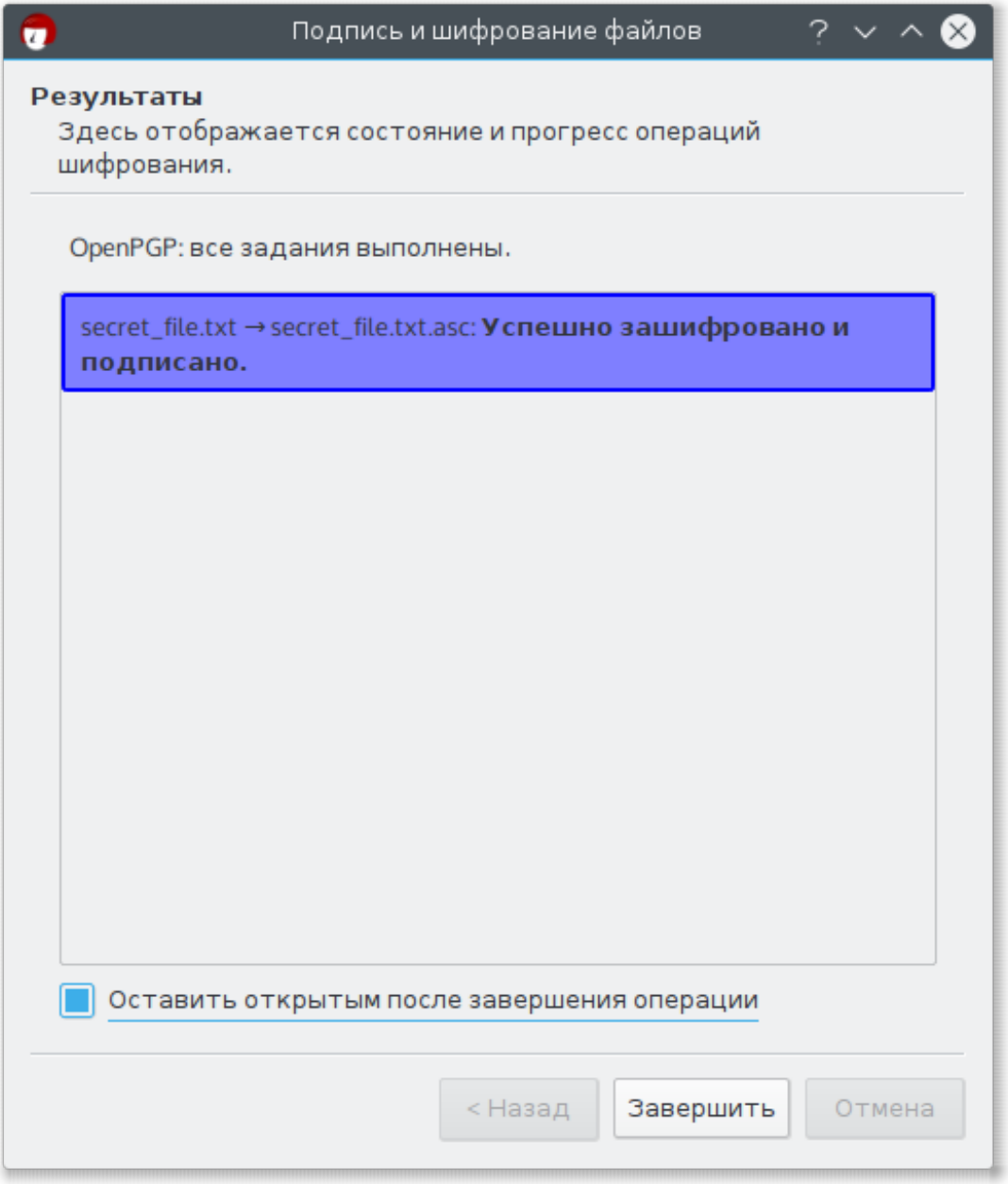

Рис. 14: Шифрование

Так выглядит зашифрованный файл

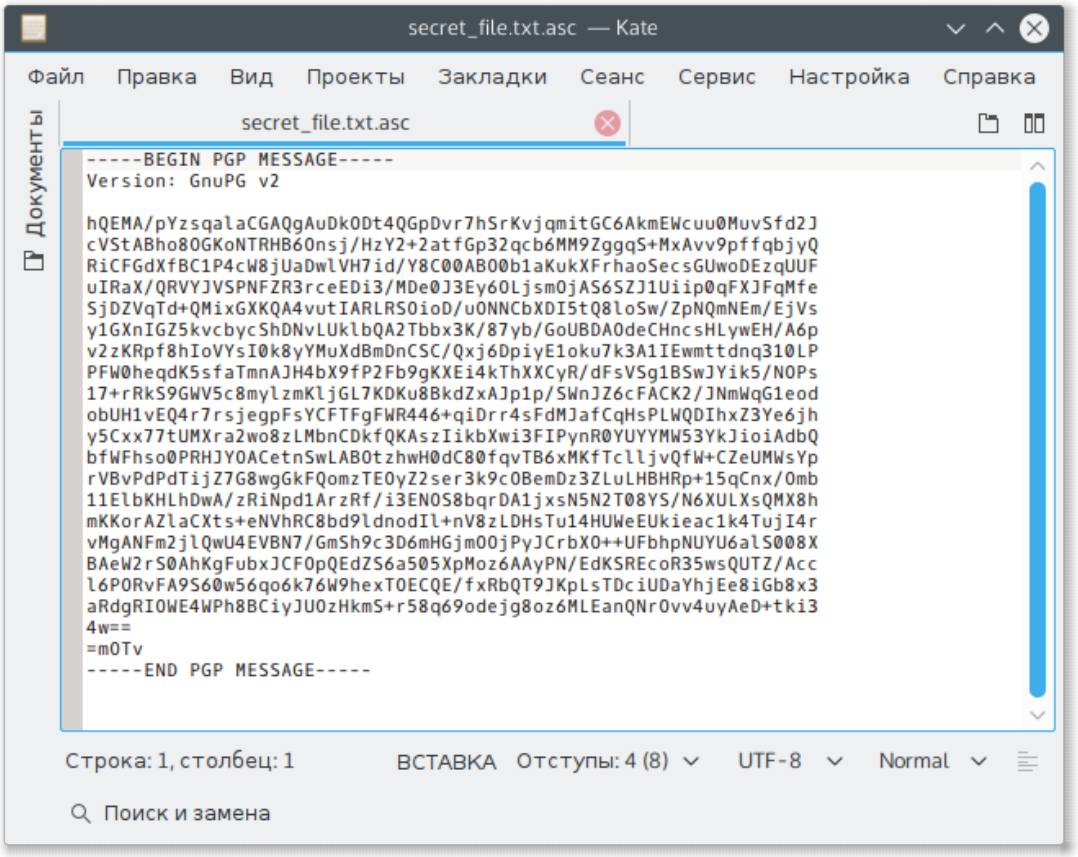

Рис. 15: Зашифрованный файл

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

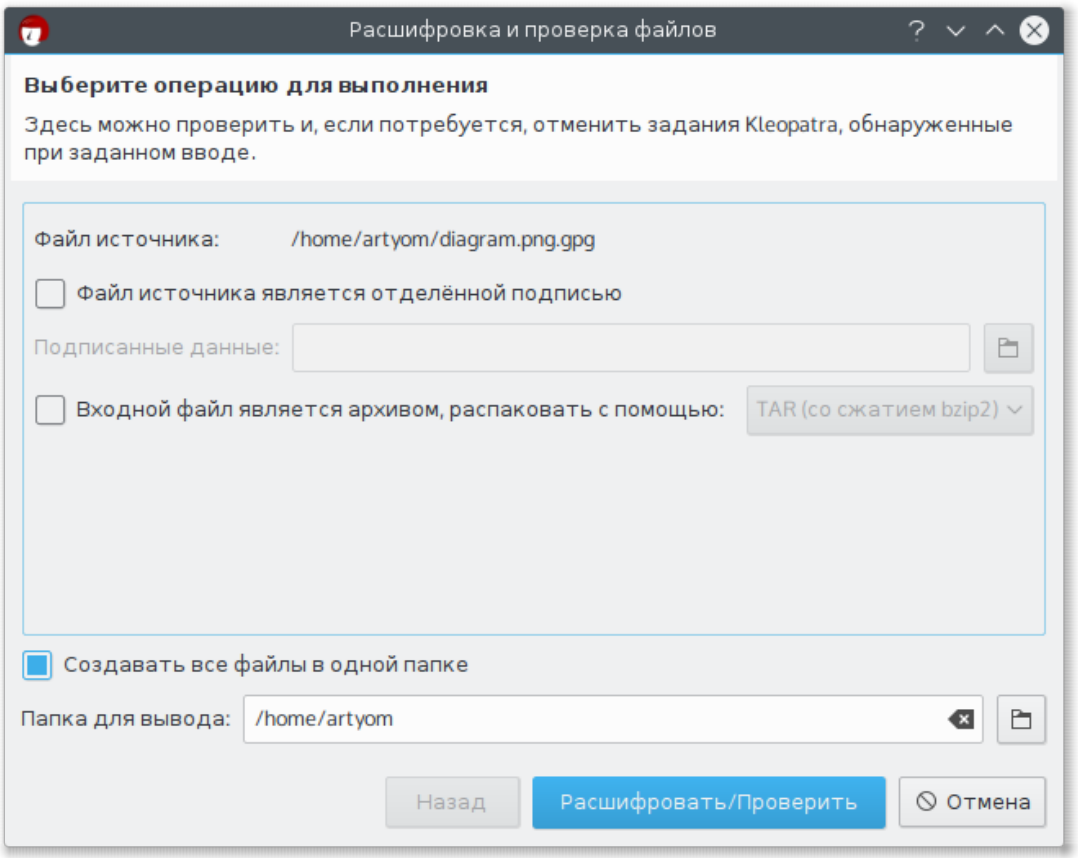

Рис. 16: Расшифровка

Так быстро?

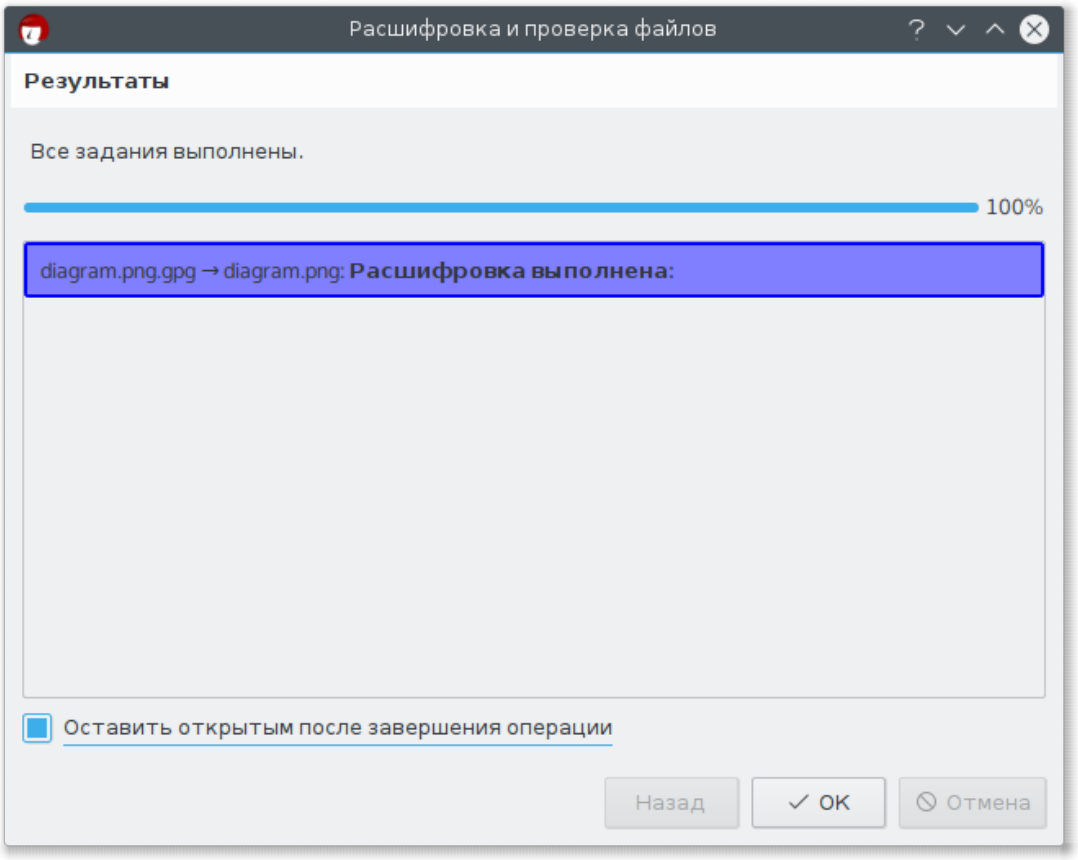

Рис. 17: Расшифровка

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.

```
1 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.Выберитетипключа

  :
(1) RSA и RSA по( умолчанию)
(2) DSA и Elgamal
(3) DSA только( дляподписи )
(4) RSA только( дляподписи )Вашвыбор
 ? 1длинаключей
  RSA можетбытьот   1024 до 4096 бит.КакойразмерключаВамнеобходим
    ? (2048)Запрошенныйразмерключа
   - 2048 битВыберитесрокдействияключа
   .
0 = безограниченияСрокадействия
<n>  = срокдействияключа    - n дней
<n>w = срокдействияключа    - n недель
<n>m = срокдействияключа    - n месяцев
<n>y = срокдействияключа    - n летСрокдействияключа
  ? (0) 2уКлючдействителендоСр
   . 28 марта 2018 00:55:57 MSKВсеверно
 ? (y/N) y

GnuPG необходимосоставить  ID пользователявкачествеидентификатораключа     .
   Вашенастоящееимя

  : Artyom AleksyukАдресэлектроннойпочты
  : artyom.h31@gmail.comКомментарий
:Вывыбралиследующий
   ID пользователя:
"Artyom Aleksyuk <artyom.h31@gmail.com>"Сменить

 (N)Имя, (C)Комментарий, (E)Адрес или (O)Принять/(Q)Выход? O
    Длязащитызакрытогоключанеобходимафразапароль
     -.


(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
   supportedНеобходимополучитьмногослучайныхчисел
    . Желательно, чтобыВывпроцессегенерацииивыполняликакието
    - другиедействияпечать  (наклавиатуре
 , движениямыши , обращениякдискам  );
    этодастгенераторуслучайныхчиселбольшевозможностейполучитьдостаточноеколичествоэнтроп
        .Необходимополучитьмногослучайныхчисел
    . Желательно, чтобыВывпроцессегенерацииивыполняликакието
    - другиедействияпечать  (наклавиатуре
 , движениямыши , обращениякдискам  );
    этодастгенераторуслучайныхчиселбольшевозможностейполучитьдостаточноеколичествоэнтроп
```

```
47          .
48 gpg: ключ 92682E10 помеченкакабсолютнодоверенный    .
      открытыйизакрытыйключисозданыиподписаны
49          .
50
51 gpg: проверкатаблицыдоверия
52 gpg: требуется 3 сограниченнымдоверием   , 1 сполным , модельдоверия  PGP
53 gpg: глубина: 0 верных :    1 подписанных :    0 доверие : 0-, 0q, 0n, 0m, 0f
      , 1u
54 gpg: срокследующейпроверкитаблицыдоверия      2018-03-27
55 pub    2048R/92682E10 2016-03-27 годен[ до: 2018-03-27]Отпечатокключа
56   = 3642 F44F 0375 4B21 A4A1  F188 2704 20BB 9268 2E10
57 uid абсолютное     [] Artyom Aleksyuk <artyom.h31@gmail.com>
58 sub    2048R/9AAC34E0 2016-03-27 годен[ до: 2018-03-27]
59 artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --list-keys
60 /home/artyom/.gnupg/pubring.gpg
61 ------------------------------
62 pub    2048R/92682E10 2016-03-27 годен[ до: 2018-03-27]
63 uid абсолютное     [] Artyom Aleksyuk <artyom.h31@gmail.com>
64 sub    2048R/9AAC34E0 2016-03-27 годен[ до: 2018-03-27]
```

В списке появился новый ключ:

```
1 artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --list-keys
2 /home/artyom/.gnupg/pubring.gpg
3 ------------------------------
4 pub    2048R/92682E10 2016-03-27 годен[ до: 2018-03-27]
5 uid абсолютное     [] Artyom Aleksyuk <artyom.h31@gmail.com>
6 sub    2048R/9AAC34E0 2016-03-27 годен[ до: 2018-03-27]
```

Экспортируем его.

```
1 artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --export --
     armor 92682E10
2 -----BEGIN PGP PUBLIC KEY BLOCK-----
3 Version: GnuPG v2
4 ...
```

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:

```
1 artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --import ~/
     Downloads/F968C255C4923EDEF1ED6F6F073052F3C8DFD64C.asc
2 gpg: ключ C8DFD64C: импортированоткрытыйключ   "Artyom Aleksyuk <artyom.
     h31@gmail.com>"
3 gpg: Всегообработано : 1
4 gpg: импортировано                : 1  (RSA: 1)
5 artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --list-keys
6 /home/artyom/.gnupg/pubring.gpg
7 ------------------------------
8 pub    2048R/92682E10 2016-03-27 годен[ до: 2018-03-27]
9 uid абсолютное     [] Artyom Aleksyuk <artyom.h31@gmail.com>
10 sub    2048R/9AAC34E0 2016-03-27 годен[ до: 2018-03-27]
11
```

```
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.txtНезадан
  ID пользователяможно ( использовать "-r").Текущиеполучатели

 :Введите

 ID пользователя. Пустаястрокадлязавершения    : C8DFD64C
gpg: 72C1CBCB: Нетсвидетельстватого  ,
   чтоданныйключпринадлежитназванномупользователю

pub  2048R/72C1CBCB 2016-03-27 Artyom Aleksyuk <artyom.h31@gmail.com>
   Отпечатокглавногоключа
  : F968 C255 C492 3EDE F1ED  6F6F 0730 52F3 C8DF D64COтпечатокподключа
 : 93B0 41C2 D4F3 17DC 0E25  3252 9D78 21E7 72C1 CBCBНетуверенностивтом

   , чтоключпринадлежитчеловеку   , указанномув
 ID пользователяключа . ЕслиВыТОЧНОзнаете   , чтоделаете ,
    можетеответитьнаследующийвопросутвердительно
      .Всеравноиспользоватьданныйключ

    ? (y/N) yТекущиеполучатели

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

 ID пользователя. Пустаястрокадлязавершения   :
```

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

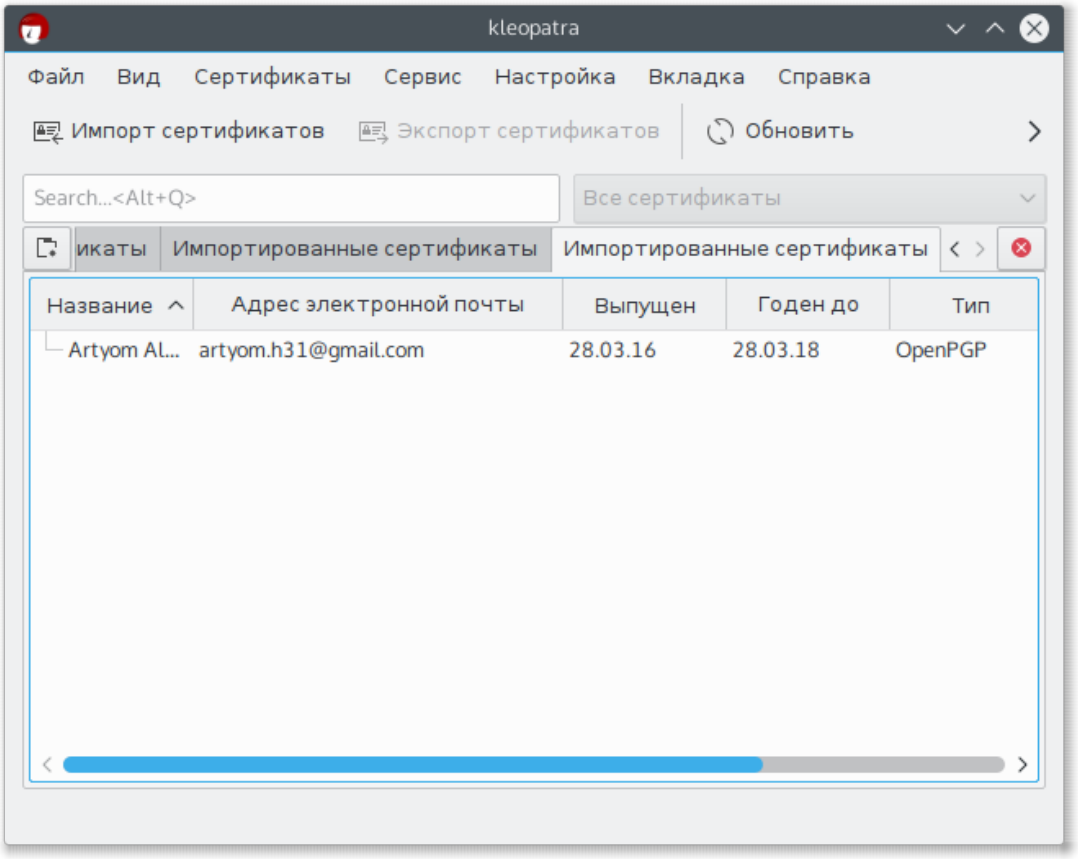

Рис. 19: Импорт ключа

Запустим расшифровку

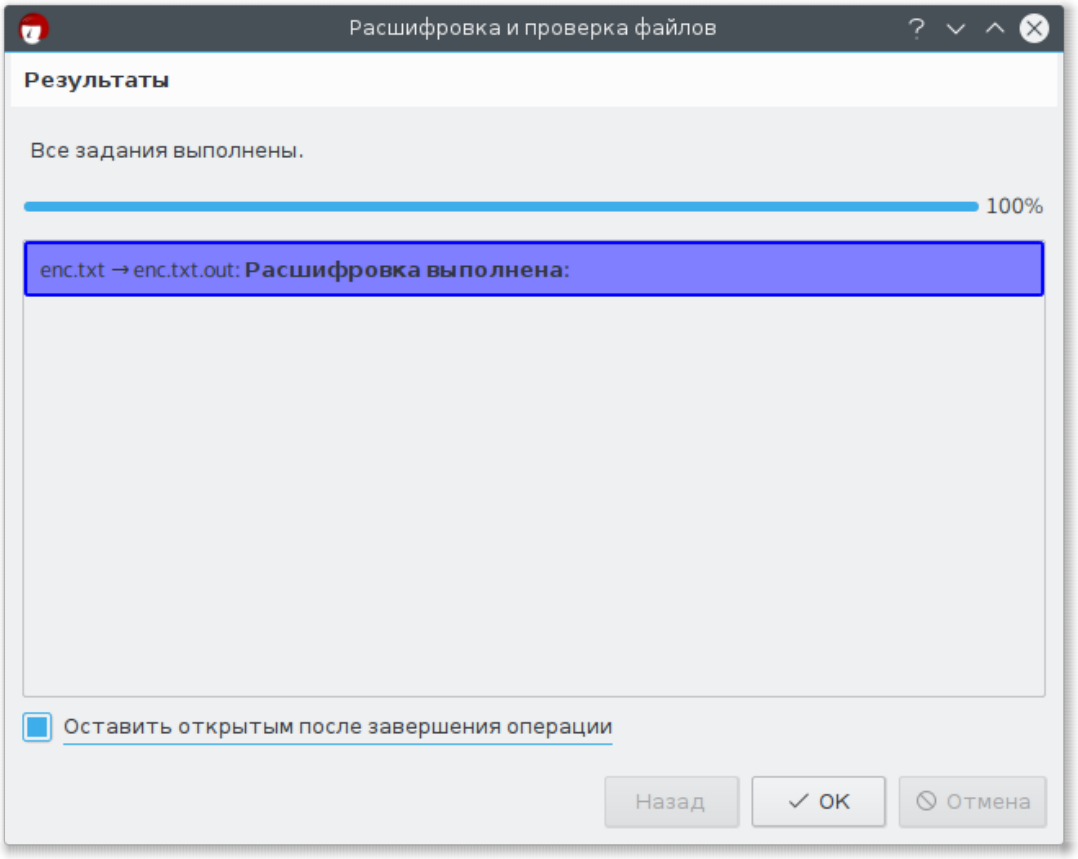

Рис. 20: Расшифровка

Проверим, что файл успешно расшифрован:

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