

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*

# 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:

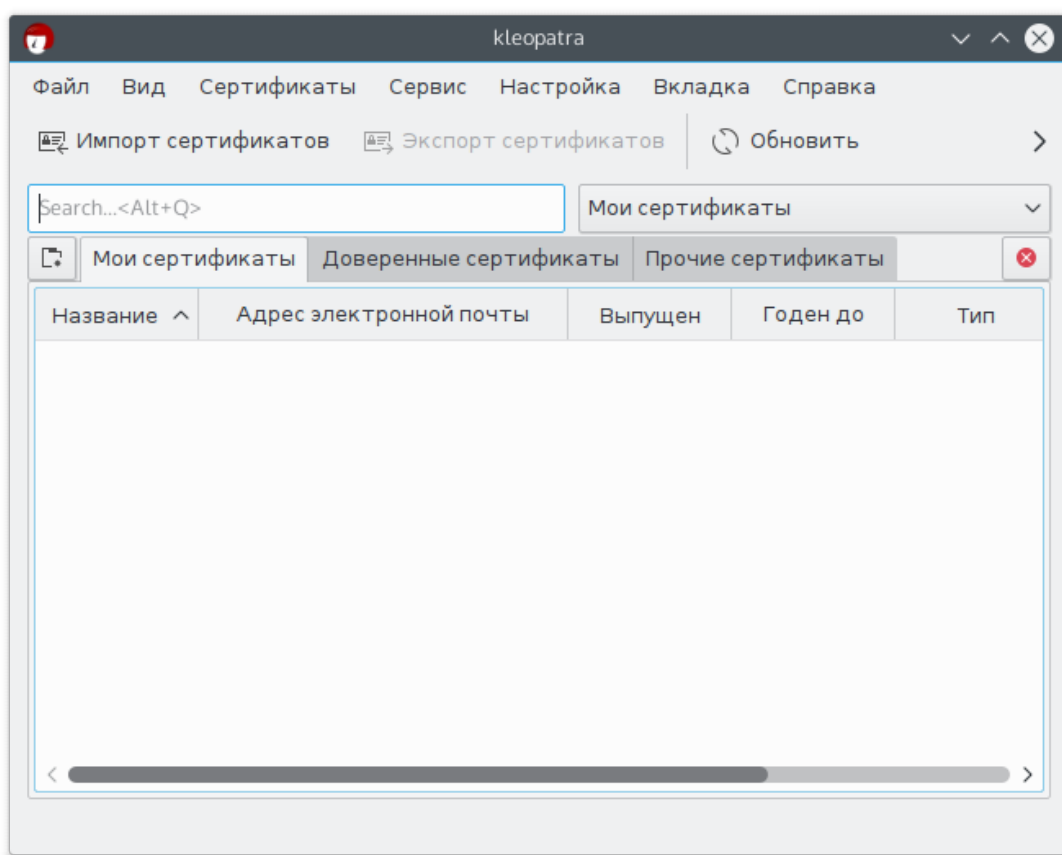


Рис. 1: Главное окно программы Kleopatra

Через меню «Файл» запустим мастер создания ключа

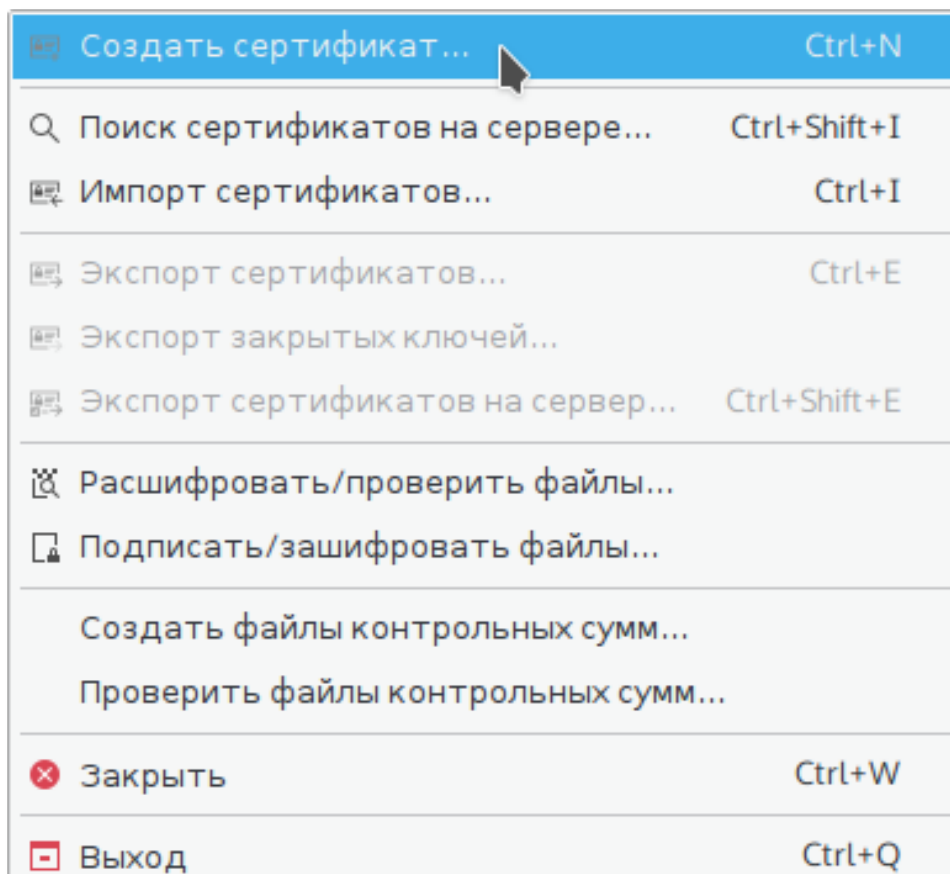


Рис. 2: Меню «Файл»

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

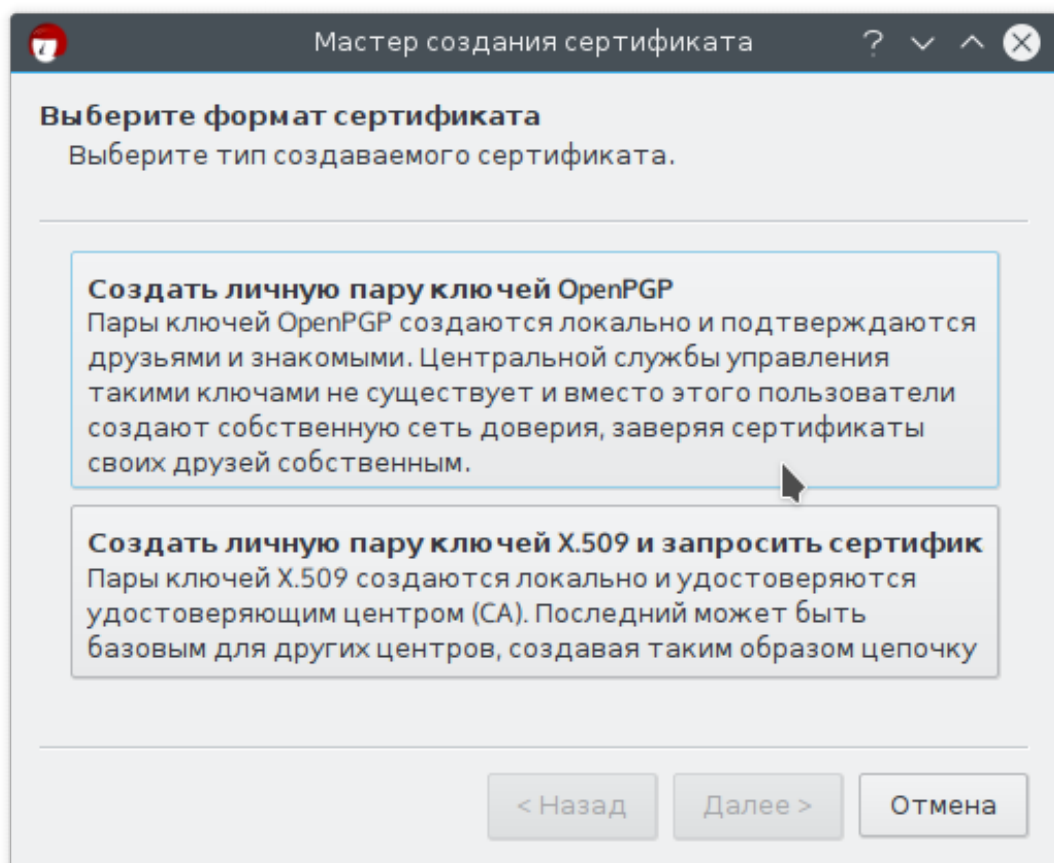


Рис. 3: Создание ключа

Укажем свои реквизиты

The screenshot shows a window titled "Мастер создания сертификата" (Certificate Creation Wizard). The current step is "Введите подробности" (Enter details). The instructions say: "Введите свои личные данные внизу. Расширенные параметры можно ввести, нажав на кнопку «Дополнительные параметры»." (Enter your personal data below. Advanced parameters can be entered by clicking the "Advanced parameters" button). The form contains three input fields: "Название:" (Name) with the value "Artyom Aleksyuk" and a "(обязательно)" (required) label; "E-Mail:" with the value "artyom.h31@gmail.com" and a "(обязательно)" (required) label; and "Примечания:" (Comments) which is empty and labeled "(необязательно)" (optional). Below these fields is a summary line: "Artyom Aleksyuk <artyom.h31@gmail.com>". To the right of this line is a button labeled "Дополнительные параметры..." (Advanced parameters...). At the bottom of the window are three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel).

Рис. 4: Создание ключа

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

The screenshot shows a window titled "Дополнительные параметры" (Advanced parameters). The "Подписи" (Signatures) tab is selected. It contains two main sections. The first section, "Алгоритм" (Algorithm), has four radio button options: "RSA" (selected), "+ RSA", "DSA", and "+ ElGamal". Each option has a corresponding dropdown menu showing "2048 бит (по умолчанию)" (2048 bits (default)). The second section, "Использование сертификата" (Certificate usage), has four checkboxes: "Подписание" (Signing, checked), "Шифрование" (Encryption, unchecked), "Сертификация" (Certification, unchecked), and "Идентификация" (Identification, unchecked). Below these is a "Годен до:" (Valid until:) label, a text box with the date "28.03.2018", and a dropdown arrow. At the bottom of the window are two buttons: "✓ OK" and "Отмена" (Cancel).

Рис. 5: Создание ключа

Введем пароль

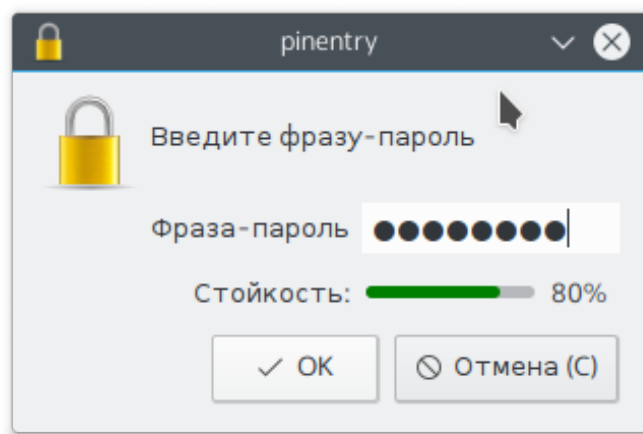


Рис. 6: Создание ключа

Voilà!

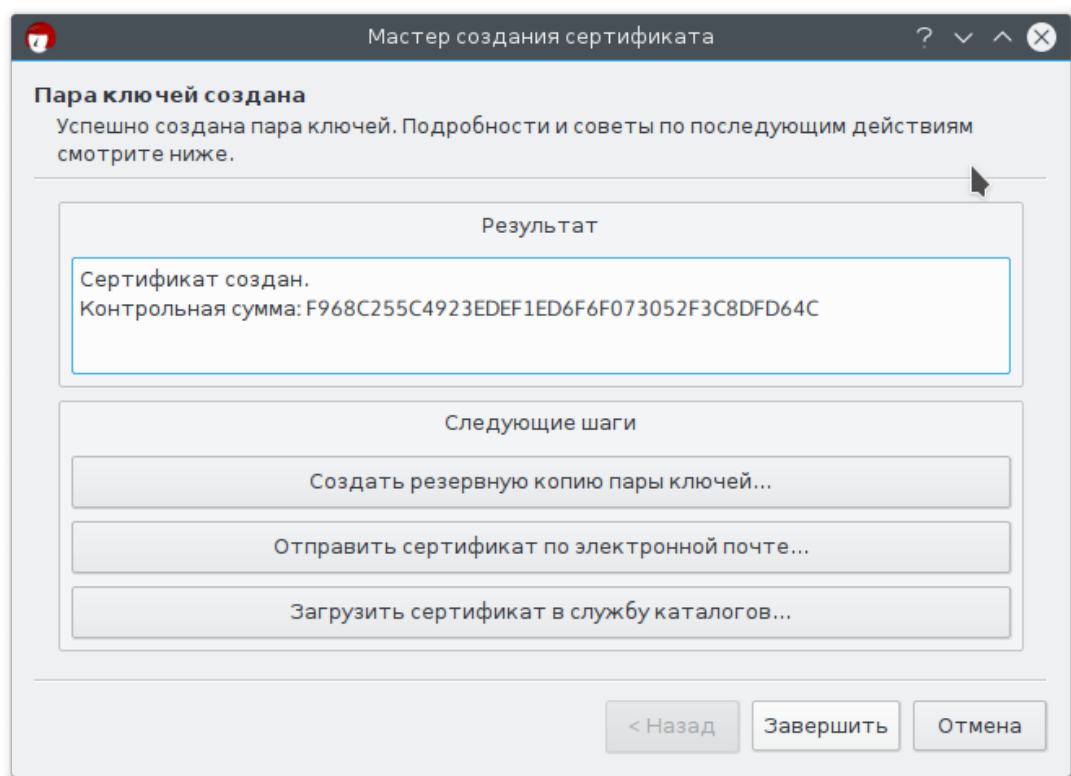


Рис. 7: Создание ключа

Наш ключ появился в списке

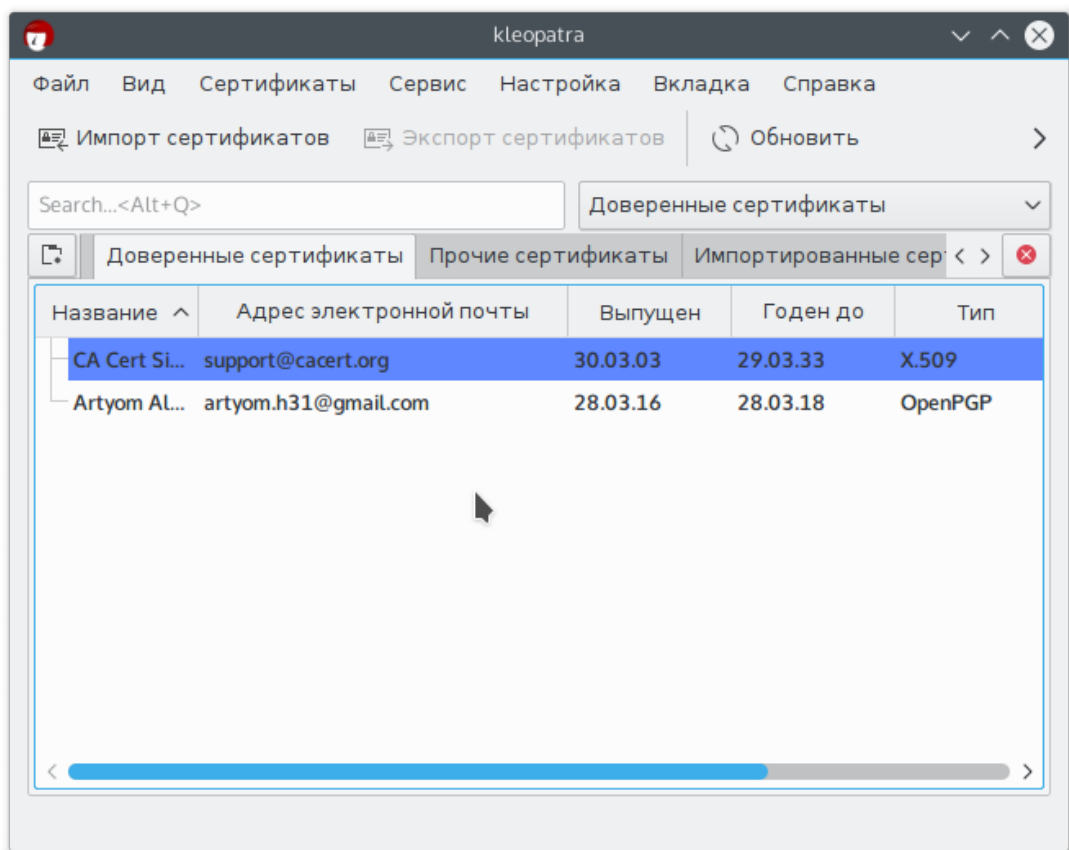


Рис. 8: Ключи

Получим сертификат от другого участника эксперимента, импортируем его.

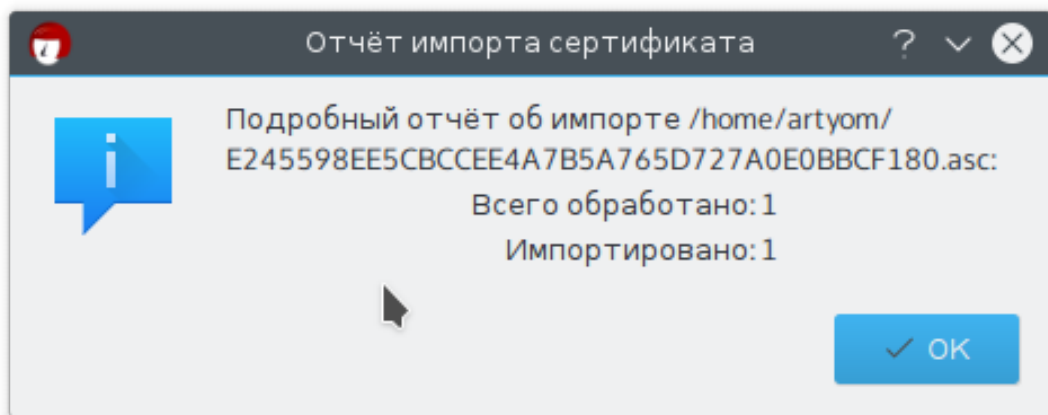


Рис. 9: Импорт сертификата

Видим его в списке

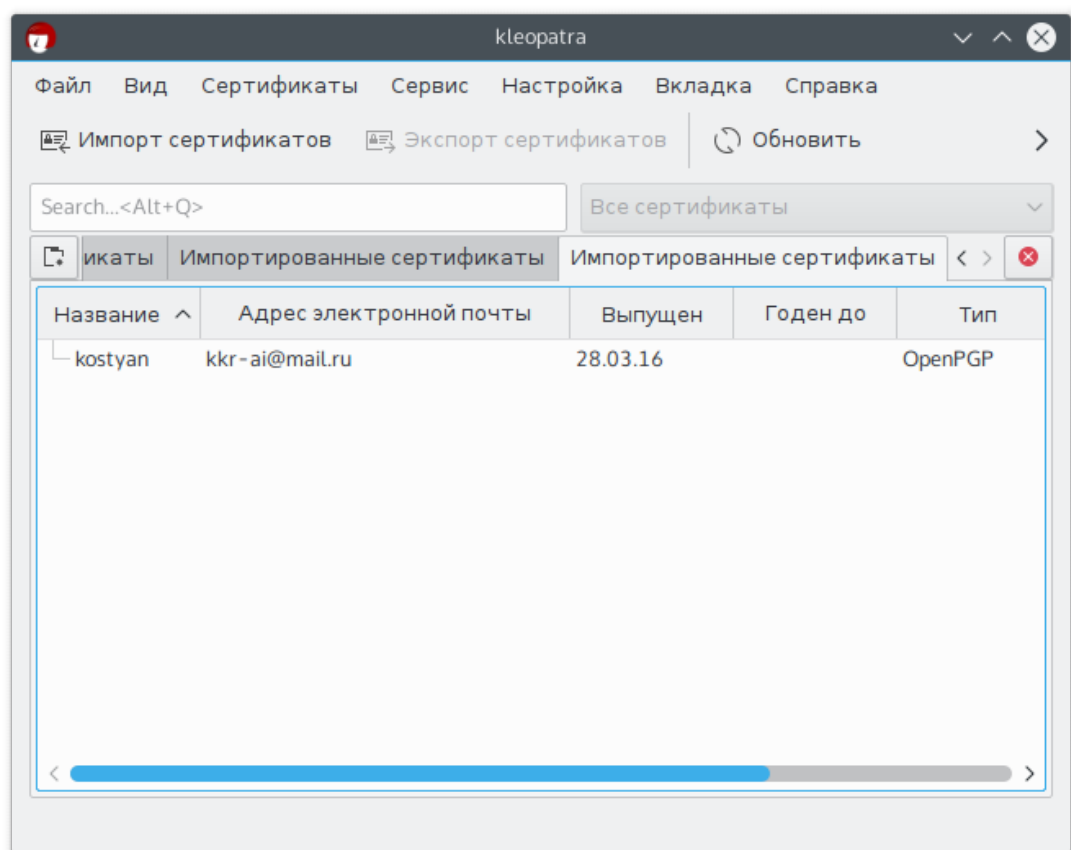


Рис. 10: Сертификаты

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

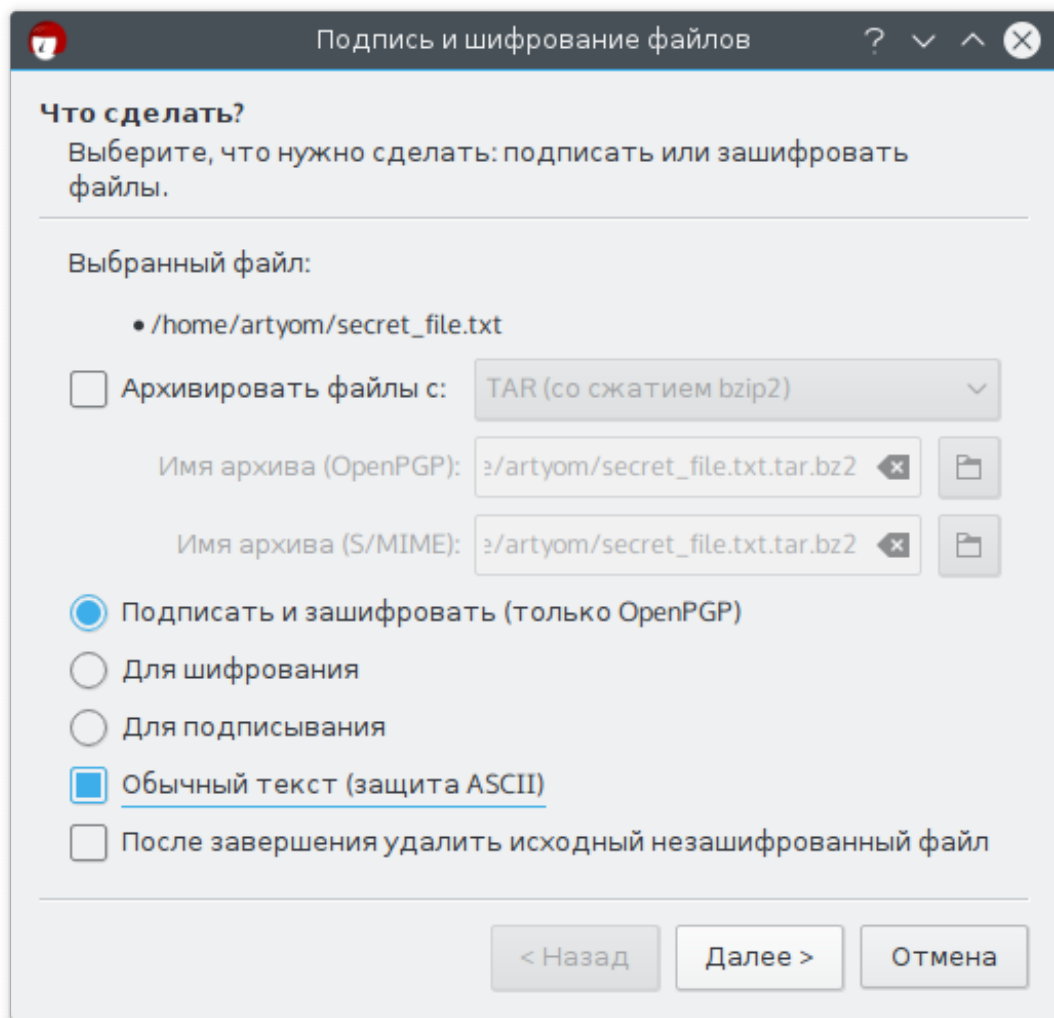


Рис. 11: Шифрование

Выберем свой и чужой ключ



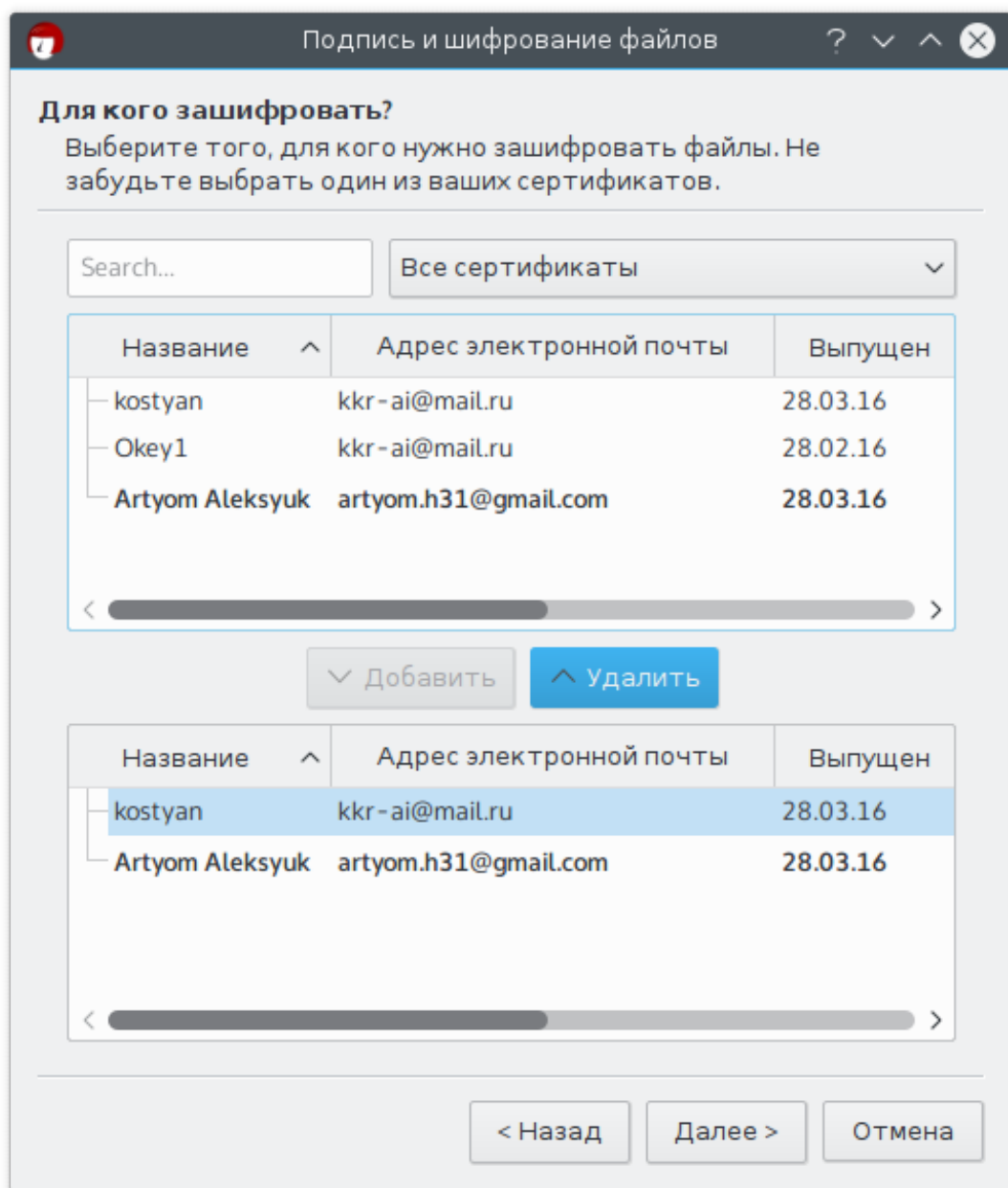


Рис. 12: Шифрование

Выберем открытый ключ, с помощью которого будем шифровать

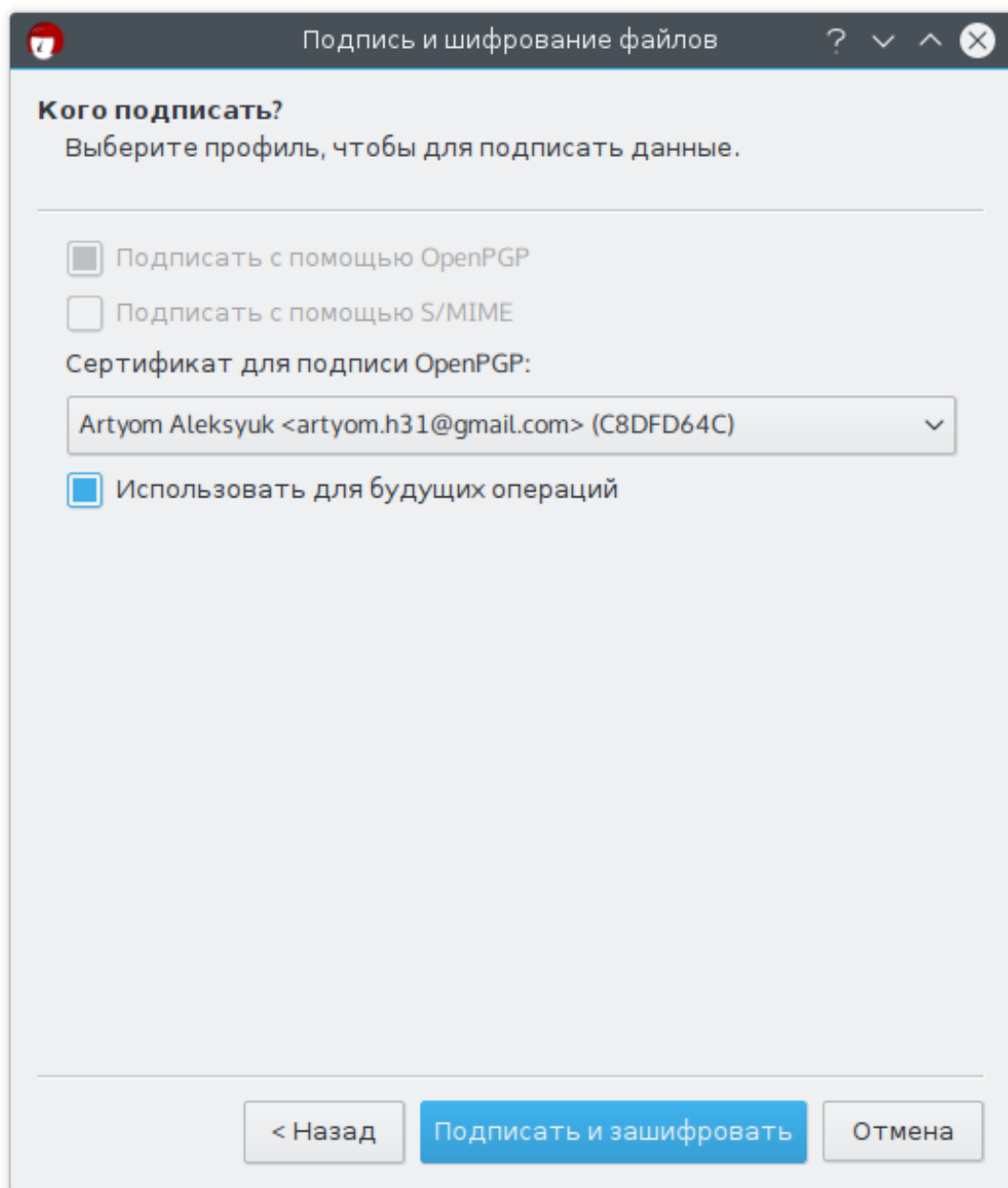


Рис. 13: Шифрование

Сообщение об успехе

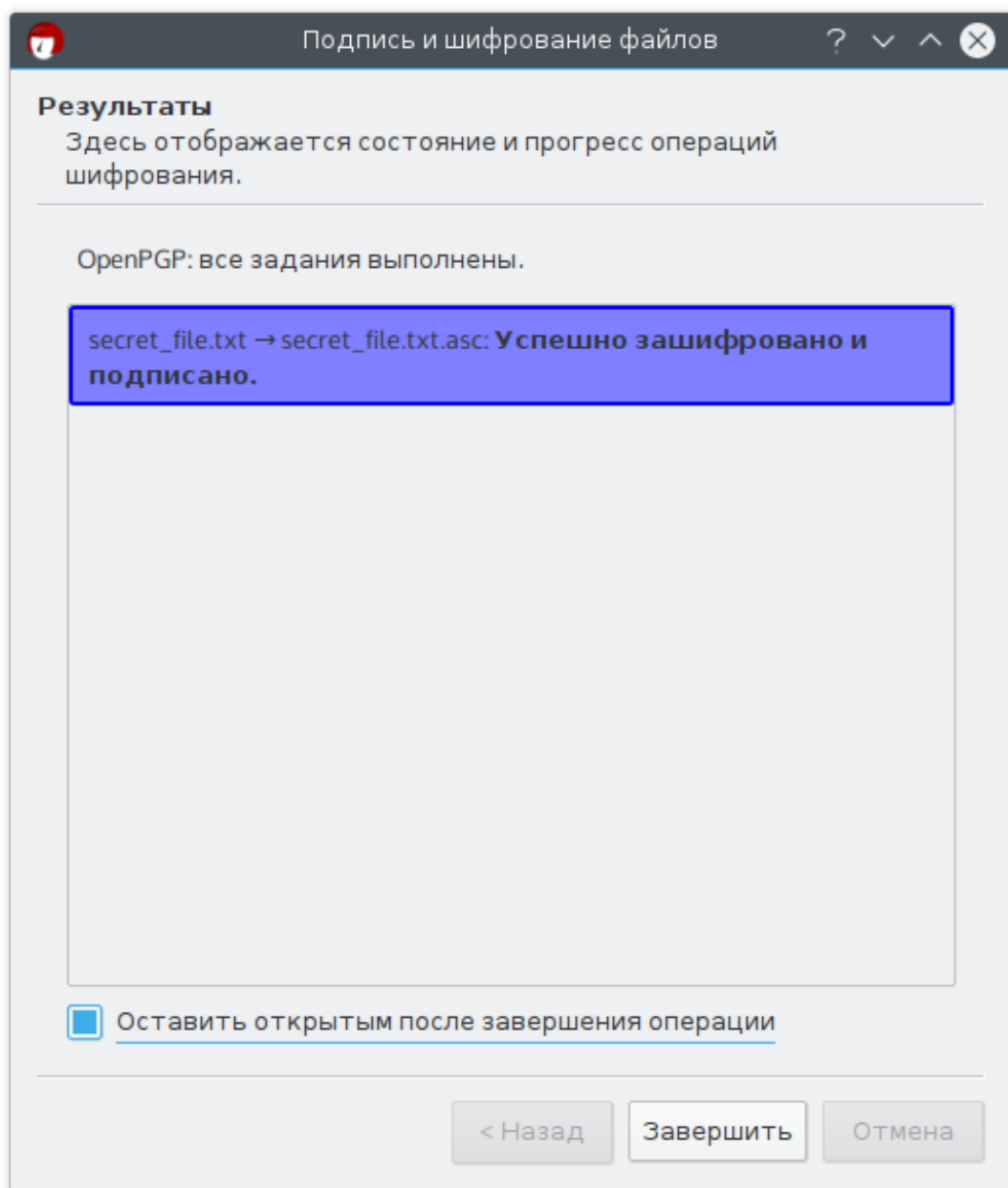


Рис. 14: Шифрование

Так выглядит зашифрованный файл

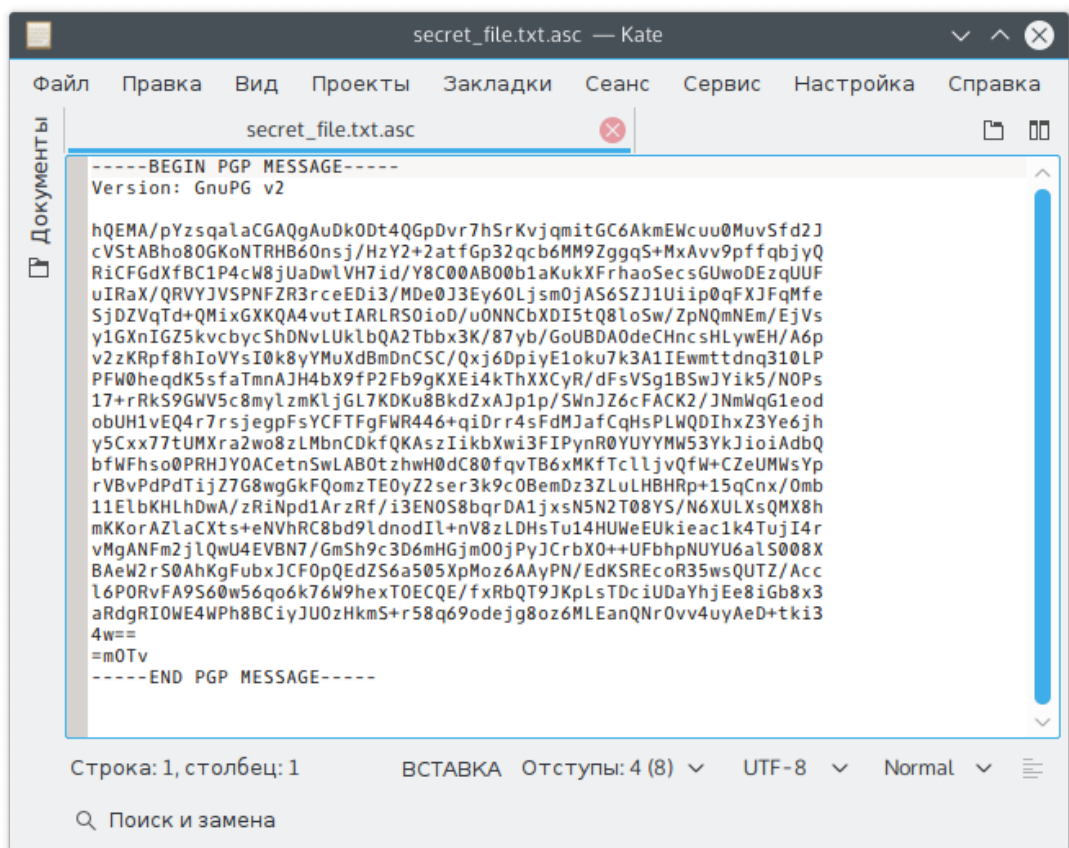


Рис. 15: Зашифрованный файл

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

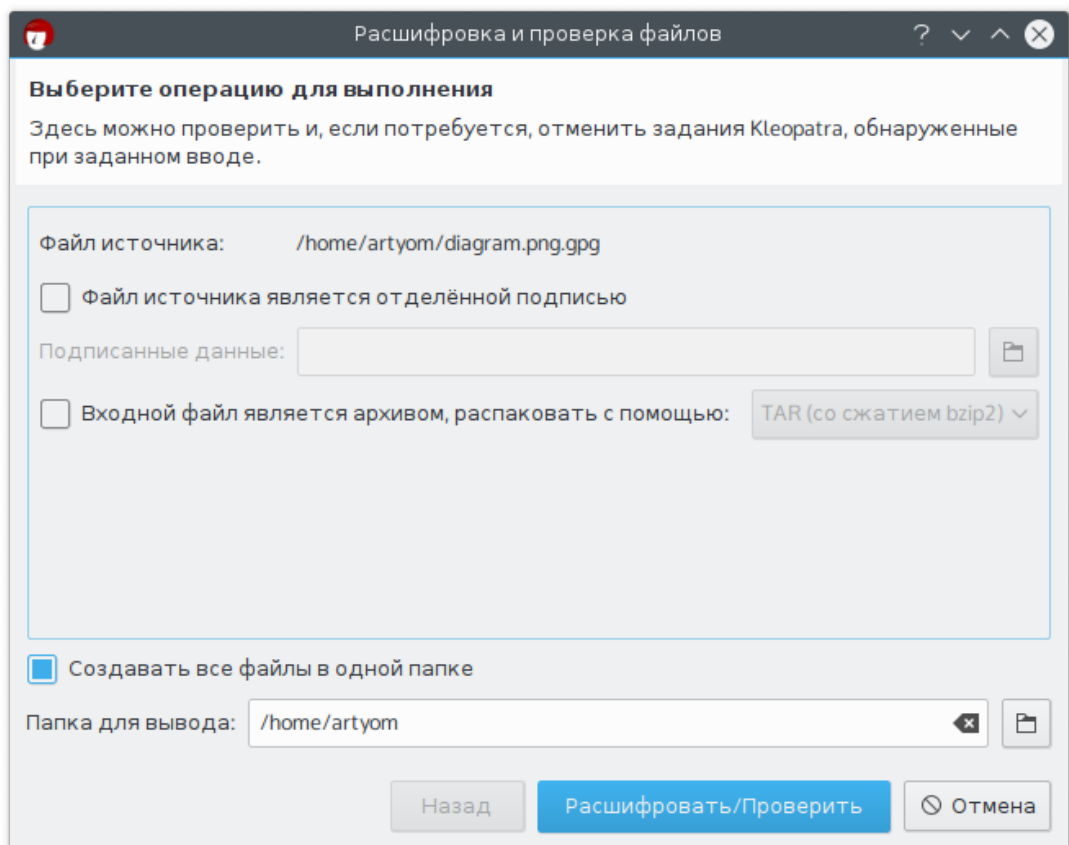


Рис. 16: Расшифровка

Так быстро?

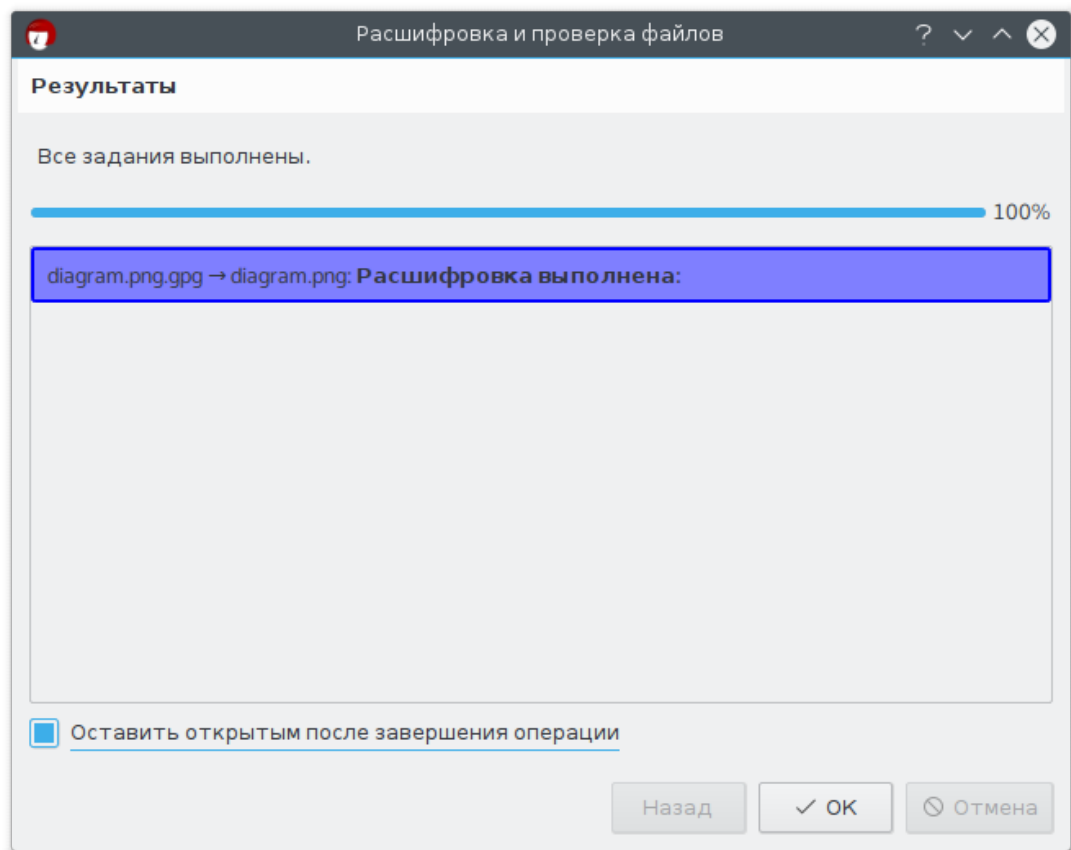


Рис. 17: Расшифровка

Ниже представлено расшифрованное изображение

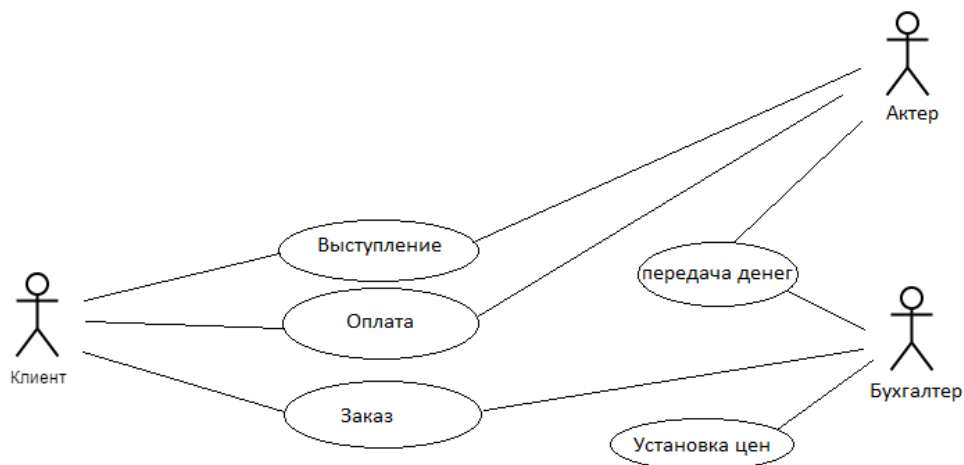


Рис. 18: Расшифрованное изображение

## 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.

```
1 artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --gen-key
2 gpg (GnuPG) 2.0.28; Copyright (C) 2015 Free Software Foundation, Inc.
3 This is free software: you are free to change and redistribute it.
4 There is NO WARRANTY, to the extent permitted by law.Выберитетипключа
5
6 :
7 (1) RSA и RSA по( умолчанию)
8 (2) DSA и Elgamal
9 (3) DSA только( дляподписи )
10 (4) RSA только( дляподписи )Вашвыбор
11 ? 1длинаключей
12 RSA можетбытьот 1024 до 4096 бит.КакойразмерключаВамнеобходим
13 ? (2048)Запрошенныйразмерключа
14 - 2048 битВыберитесрокдействияключа
15 .
16 0 = безограничениясрокадействия
17 <n> = срокдействияключа - n дней
18 <n>w = срокдействияключа - n недель
19 <n>m = срокдействияключа - n месяцев
20 <n>y = срокдействияключа - n летСрокдействияключа
21 ? (0) 2уКлючдействителендоСр
22 . 28 марта 2018 00:55:57 MSKBсеверно
23 ? (y/N) y
24
25 GnuPG необходимосоставить ID пользователякакчествоидентификатораключа .
26
27 : Artyom AleksyukАдресэлектроннойпочты
28 : artyom.h31@gmail.comКомментарий
29 :Вывыбралиследующий
30 ID пользователя:
31 "Artyom Aleksyuk <artyom.h31@gmail.com>"Сменить
32
33 (N)Имя, (C)Комментарий, (E)Адрес или (O)Принять/(Q)Выход? O
34 Длязащитызакрытогоключаанеобходимафразапароль
35 -.
36
37 (process:22404): GLib-WARNING **: /build/glib2.0-MuyBSS/glib2
38 .0-2.46.2/./glib/gmem.c:482: custom memory allocation vtable not
39 supported
40
41 (process:22412): GLib-WARNING **: /build/glib2.0-MuyBSS/glib2
42 .0-2.46.2/./glib/gmem.c:482: custom memory allocation vtable not
43 supportedНеобходимополучитьмногослучайныхчисел
44 . Желательно, чтобыВывпроцессегенерациивыполняликакието
45 - другиедействияпечать (наклавиатуре
46 , движениямышы , обращениякдискам );
47 этодастгенераторуслучайныхчиселбольшевозможностейполучитьдостаточноколичествоэнтроп
48 .Необходимополучитьмногослучайныхчисел
49 . Желательно, чтобыВывпроцессегенерациивыполняликакието
50 - другиедействияпечать (наклавиатуре
51 , движениямышы , обращениякдискам );
52 этодастгенераторуслучайныхчиселбольшевозможностейполучитьдостаточноколичествоэнтроп
```

```

47 .
48 gpg: ключ 92682E10 помечен как абсолютно доверенный .
   открытый/закрытый ключ/создан/и подписан
49 .
50
51 gpg: проверка таблицы доверия
52 gpg: требуется 3 сограниченными доверием , 1 полным , модель доверия PGP
53 gpg: глубина: 0 верных : 1 подписанных : 0 доверие : 0-, 0q, 0n, 0m, 0f
   , 1u
54 gpg: срок следующей проверки таблицы доверия 2018-03-27
55 pub 2048R/92682E10 2016-03-27 годен[ до: 2018-03-27] Отпечаток ключа
56 = 3642 F44F 0375 4B21 A4A1 F188 2704 20BB 9268 2E10
57 uid абсолютное [] Artyom Alekseyuk <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 Alekseyuk <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 Alekseyuk <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: импортирован открытый ключ "Artyom Alekseyuk <artyom.
   h31@gmail.com>"
3 gpg: Всего обработано : 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 Alekseyuk <artyom.h31@gmail.com>
10 sub 2048R/9AAC34E0 2016-03-27 годен[ до: 2018-03-27]
11

```

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

Запустим шифрование:

```
1 artyom@artyom-H97-D3H:~/Projects/InfoSecCourse/gpg$ gpg2 --armor --
  encrypt secret.txtНезадан
2   ID пользователяможно ( использовать "-r").Текущиеполучатели
3
4   :Введите
5
6   ID пользователя. Пустаястрокадлязавершения      : C8DFD64C
7 gpg: 72C1CBCB: Нетсвидетельствтого      ,
   чтоданныйключпринадлежитназванномупользователю
8
9 pub  2048R/72C1CBCB 2016-03-27 Artyom Aleksyuk <artyom.h31@gmail.com>
   Отпечатокглавногоключа
10   : F968 C255 C492 3EDE F1ED  6F6F 0730 52F3 C8DF D64CОтпечатокподключа
11   : 93B0 41C2 D4F3 17DC 0E25  3252 9D78 21E7 72C1 CBCBНетуверенностивтом
12
13   , чтоключпринадлежитчеловеку      , указанномув
14   ID пользователяключа . ЕслиВыТОЧНОзнаете      , чтоделаете ,
   можетеответитьнаследующийвопросутвердительно
15   .Всеравноиспользоватьданныйключ
16
17   ? (y/N) уТекущиеполучатели
18
19   :
20 2048R/72C1CBCB 2016-03-27 "Artyom Aleksyuk <artyom.h31@gmail.com>"
   Введите
21
22   ID пользователя. Пустаястрокадлязавершения      :
```

В директории появился новый файл

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

Импортируем открытый ключ на другой машине



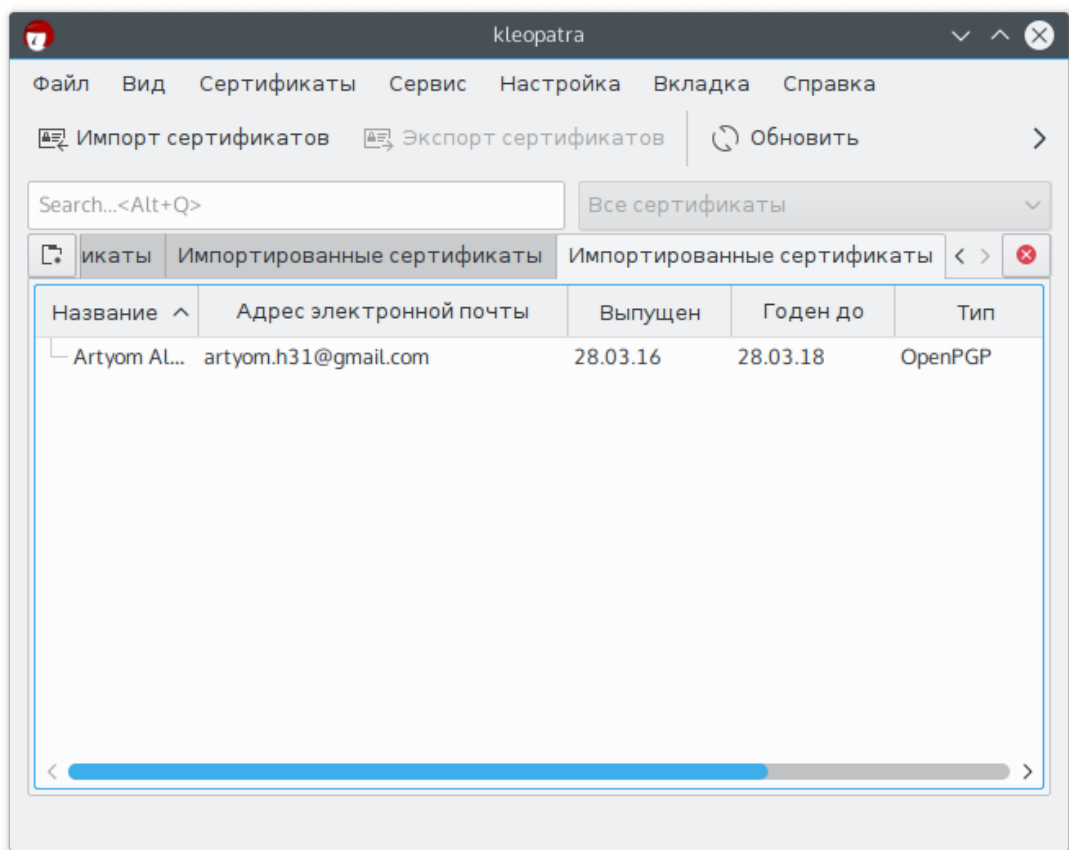


Рис. 19: Импорт ключа

Запустим расшифровку

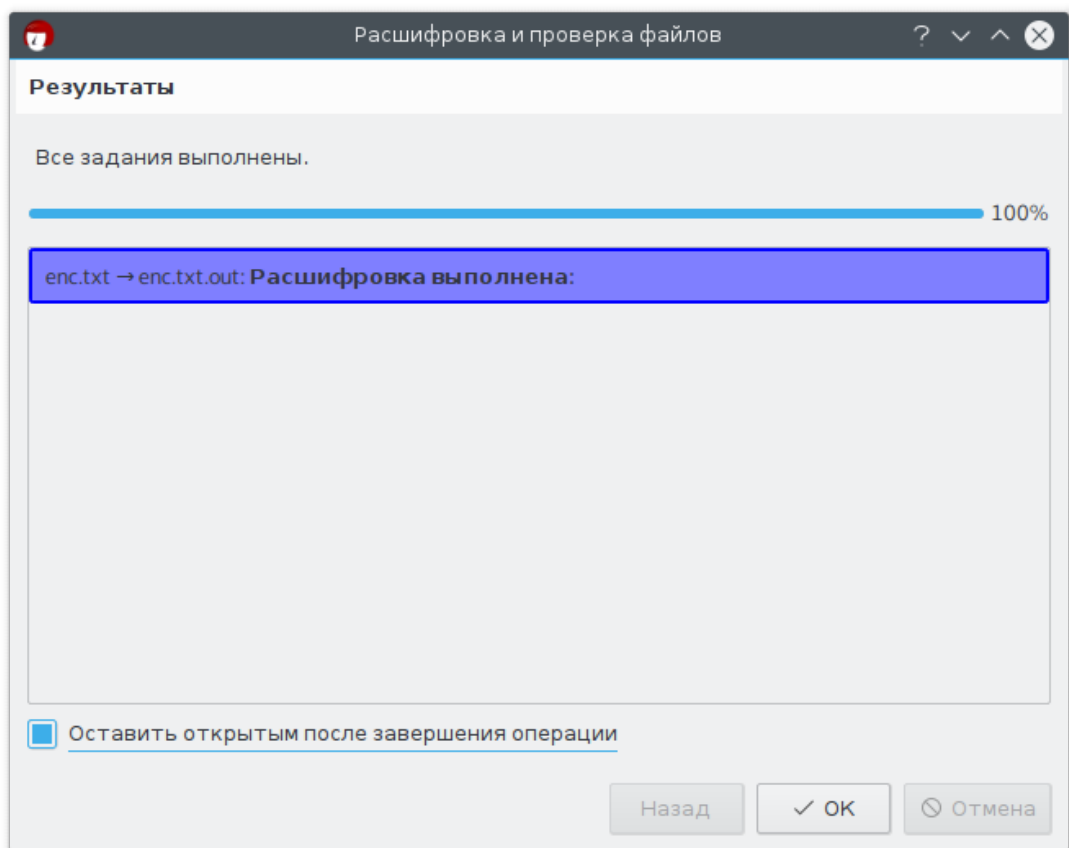


Рис. 20: Расшифровка

Проверим, что файл успешно расшифрован:

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