Санкт-Петербургский Политехнический Университет Петра Великого

Кафедра компьютерных систем и программных технологий

Отчёт по лабораторной работе №3

Курс: «Защита информации»

Тема: «Ознакомление с PGP системами на основе программы Kleopatra»

Выполнил студент:

Бояркин Никита Сергеевич
Группа: 43501/3

Проверил:

Новопашенный Андрей Гелиевич

Санкт-Петербург
2017 г.

Содержание

Лабораторная работа №3

1.1 Цель работы

Ознакомиться с PGP системами на основе программы Kleopatra.

1.2 Программа работы

1. Ознакомиться с программой Kleopatra.
2. Создать новый сертификат.
3. Зашифровать произвольный файл открытым ключем.
4. Расшифровать произвольный файл закрытым ключем.

1.3 Программное окружение

Первый компьютер

```
1 nikita@nikita-VirtualBox:~$ cat /proc/version
2 Linux version 4.4.0-72-generic (buildd@lcy01-17) (gcc version 5.4.0 20160609 (Ubuntu
    5.4.0-6ubuntu1~16.04.4) ) #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017
3 nikita@nikita-VirtualBox:~$ kleopatra --version
4 kleopatra 2.2.0
```

Второй компьютер

```
1 nikita@nikita-pc:~$ cat /proc/version
2 Linux version 4.4.0-59-generic (buildd@lgw01-11) (gcc version 5.4.0 20160609 (Ubuntu
    5.4.0-6ubuntu1~16.04.4) ) #80-Ubuntu SMP Fri Jan 6 17:47:47 UTC 2017
3 nikita@nikita-pc:~$ kleopatra --version
4 kleopatra 2.2.0
```

1.4 Ход работы

1.4.1 Pretty Good Privacy

Pretty Good Privacy (PGP) — компьютерная программа, также библиотека функций, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске. Первоначально разработана Филиппом Циммерманном в 1991 году.

В 1999 году силами Фонда свободного программного обеспечения была создана свободная реализация OpenPGP под названием GNU Privacy Guard (GnuPG).

В рамках данной лабораторной работы ограничимся изучением менеджера сертификатов Kleopatra, который включается в OpenPGP реализацию.

1.4.2 Принцип работы

Первым этапом является создание нового сертификата. Генерируется пара ключей: открытый ключ и закрытый ключ. Ключи являются парными, и файлы зашифрованные одним ключем можно расшифровать только парным ключем. Открытый ключ распространяется открыто, в то время как закрытый ключ должен сохраняться в секрете. Стоит отметить, что в программе Kleopatra доступ к расшифровке закрытым ключем защищается специальным паролем.

Таким образом, сторона создающая сертификат распространяет открытый ключ среди пользователей, от которых ожидается прием сообщений. Сообщения шифруются этим открытым ключем на стороне пользователя и пересылаются стороне, создавшей сертификат. После этого, сторона создавшая сертификат расшифровывает сообщение закрытым ключем.

1.4.3 Создание сертификата

Проиллюстрируем этап создания нового сертификата (File -> New Certificate...). Первый этап - выбор стандарта для пары ключей. Kleopatra поддерживает помимо OpenPGP также и X.509:

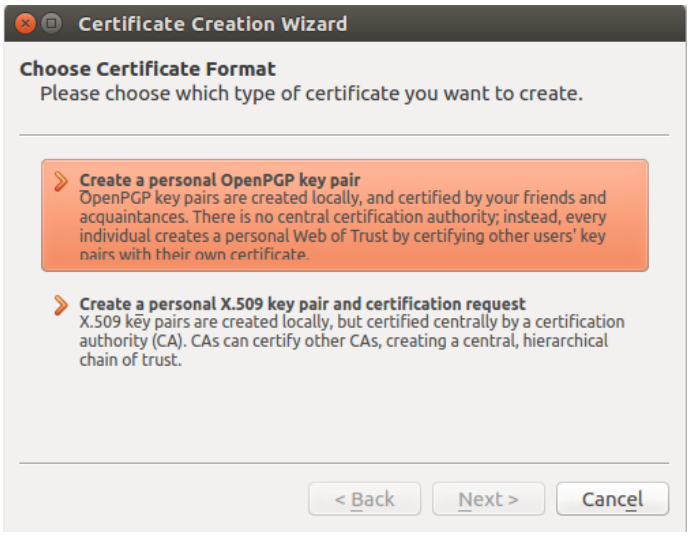

Рис. 1.1: Выбор стандарта для пары ключей

После этого происходит процесс конфигурирования сертификата (выбор алгоритма шифрования, длины ключа, названия сертификата и др.):

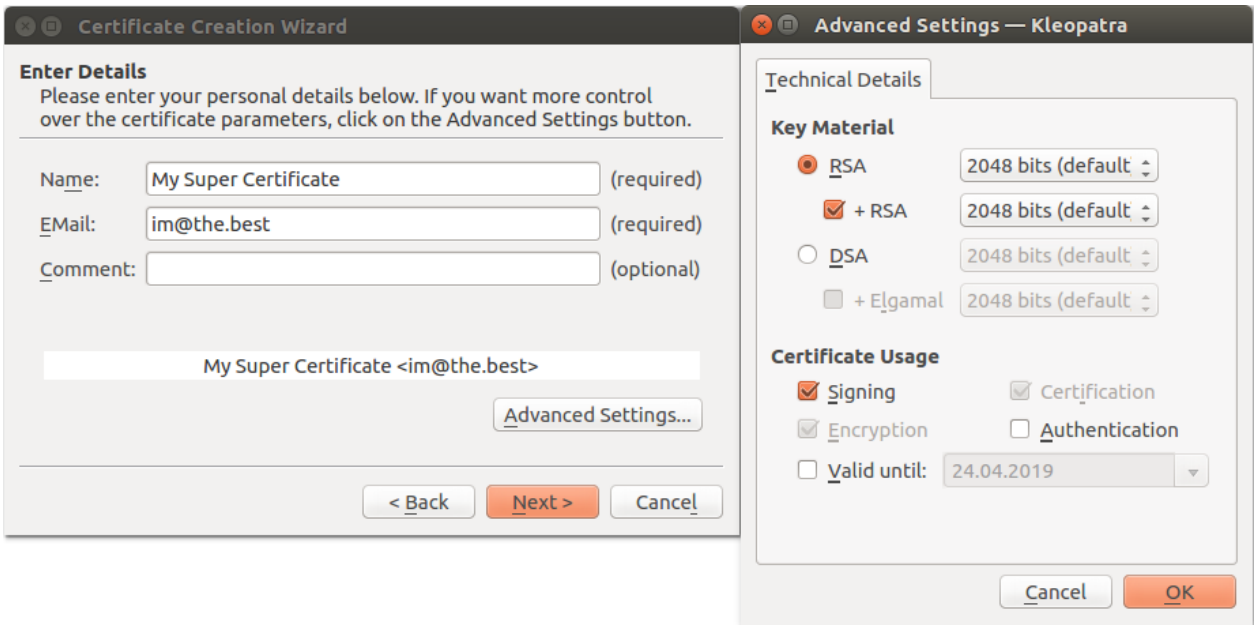

Рис. 1.2: Конфигурирование сертификата и выбор алгоритма шифрования

Затем, происходит процесс генерирования пары ключей (на основе случайных символов и движения окна), а также устанавливается пароль на доступ к закрытому ключу:

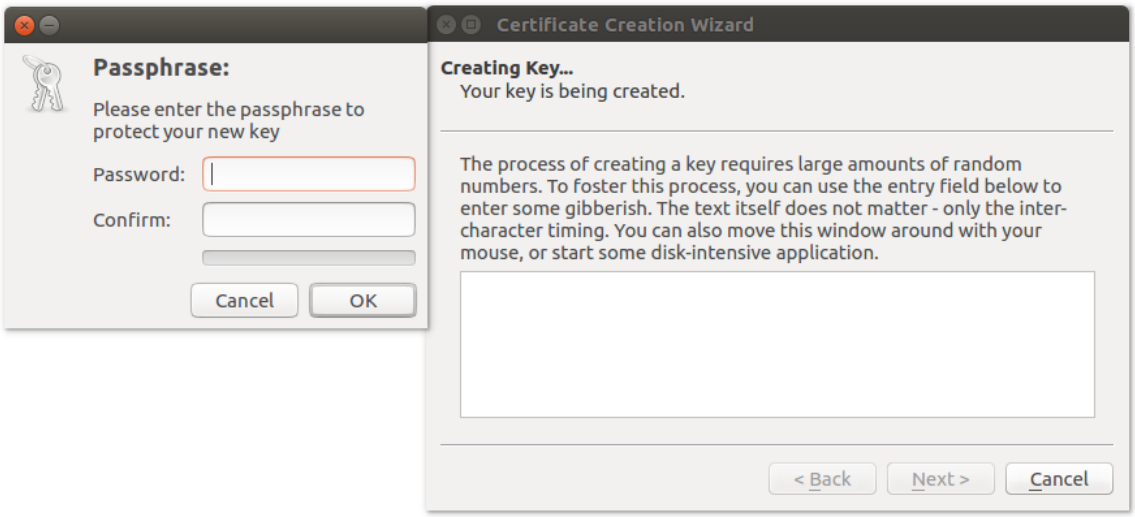

Рис. 1.3: Процесс генерирования пары ключей и установление пароля на доступ к закрытому ключу

Созданный сертификат появляется в списке сертификатов:

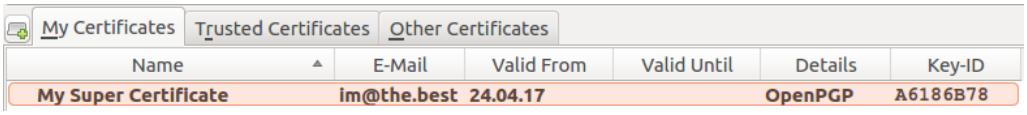

Рис. 1.4: Результат создания сертификата

Для получения открытого ключа воспользуемся командой ПКМ -> Export Certificates... Отрытый ключ сохраняется в файле с собственным расширением:

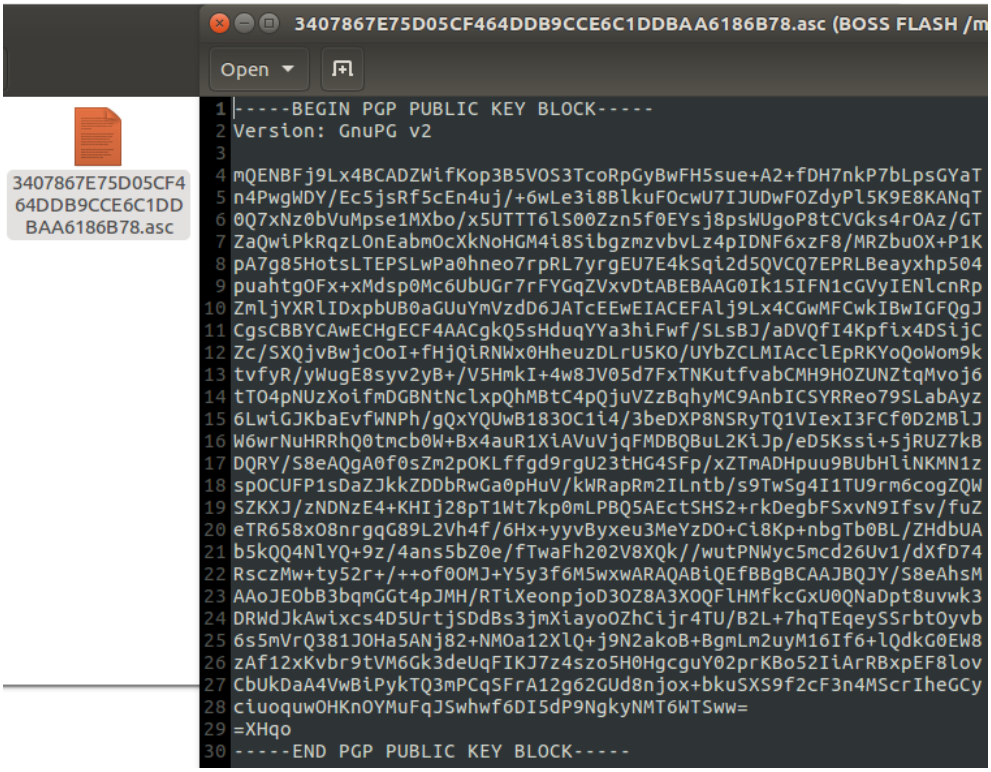

Рис. 1.5: Открытый ключ RSA 2048 бит

Этот файл можно распространять среди пользователей, от которых ожидается прием сообщений.

1.4.4 Шифрование файлов открытым ключем

На втором компьютере импортируем сертификат (File -> Import Certificates...), указав в качестве параметра созданный открытый ключ (см. п. 1.4.3):

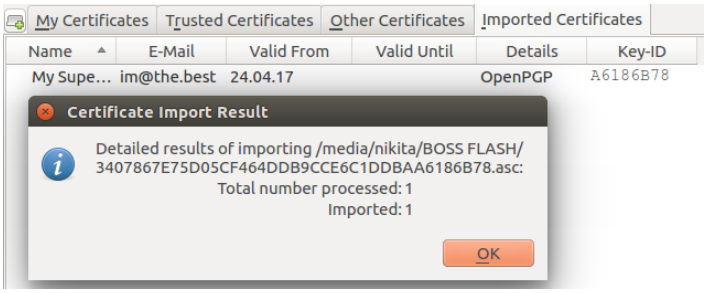

Рис. 1.6: Результат импортирования сертификата

Для шифрования файлов воспользуемся командой File -> Sign/Encrypt files... Появляется окно с выбором параметров шифрования:

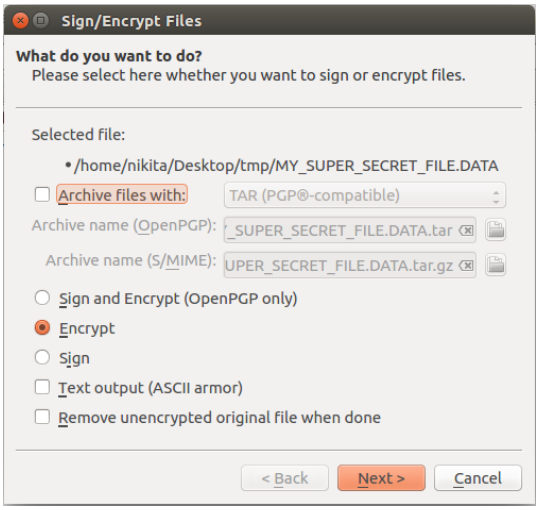

Рис. 1.7: Выбор параметров шифрования

Далее указывается сертификат для шифрования файла:

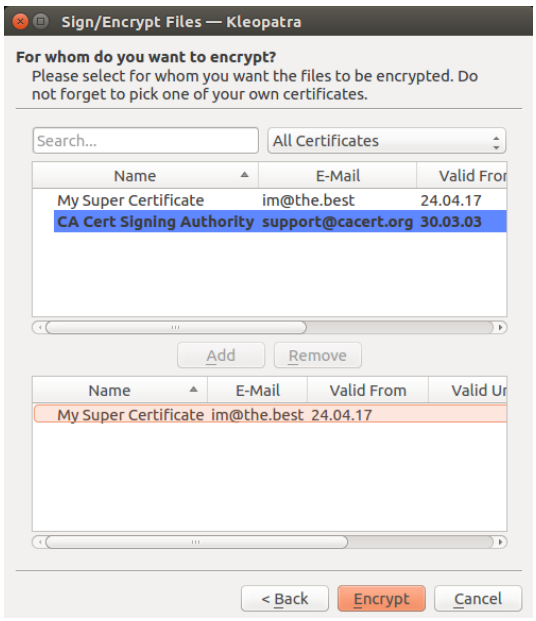

Рис. 1.8: Выбор сертификата для шифрования

Результат шифрования файла:

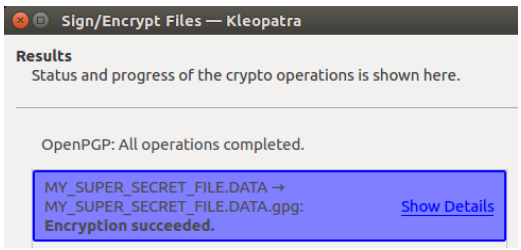

Рис. 1.9: Результат шифрования файла

Файл был зашифрован в формате .gpg, расшифровка этого файла возможна только закрытым ключем, поэтому расшифровать его на этом компьютере нельзя, даже учитывая что мы его и зашифровали.

1.4.5 Расшифровка файлов закрытым ключем

Для расшифровки файлов воспользуемся командой File -> Decrypt/Verify files... Появляется окно с выбором параметров расшифровки:

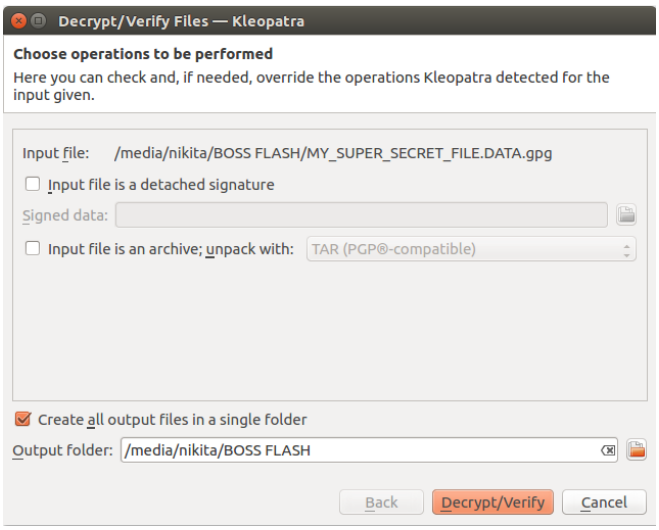

Рис. 1.10: Выбор параметров расшифровки

Для доступа к расшифровке закрытым ключем необходимо ввести пароль, который был создан вместе с сертификатом (см. п. 1.4.3):

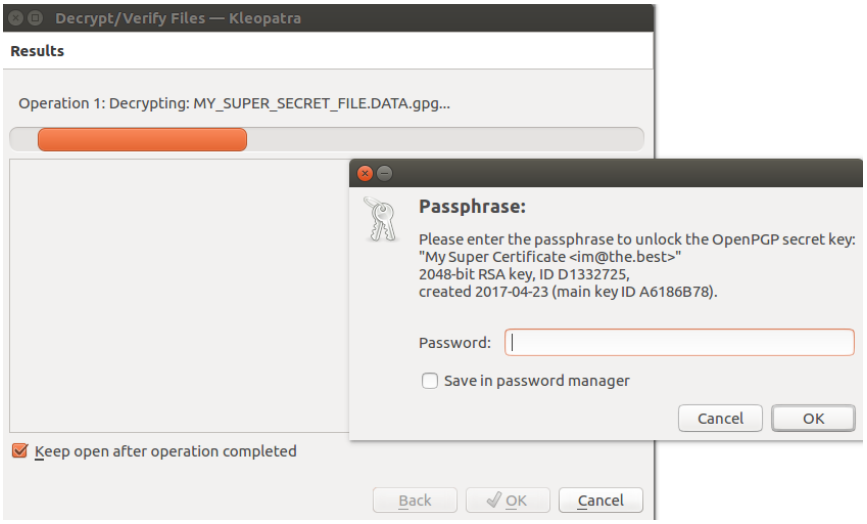

Рис. 1.11: Расшифровка закрытым ключем

Результат расшифровки файла:

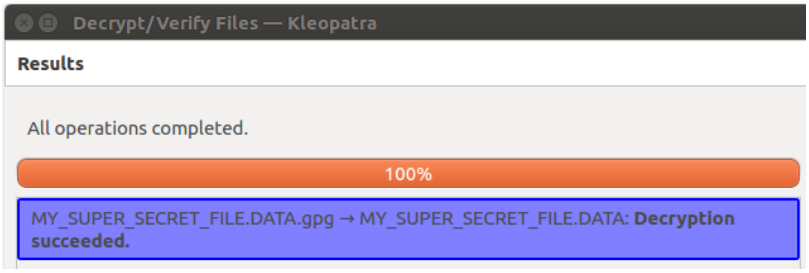

Рис. 1.12: Результат расшифровки файла

Файл был успешно расшифрован: название и содержимое файла совпадает с оригиналом.

1.5 Вывод

В данной работе было рассмотрено ассиметричное шифрование на примере программы Kleopatra семейства OpenPGP. Ассиметричное шифрование имеет преимущество перед симметричным в простоте обмена ключами, однако проигрывает в скорости шифрования. Рассмотренное в работе шифрование одностороннее. Для того, чтобы осуществить двустороннюю передачу используются два канала. В современных криптосистемах ассиметричное шифрование используется для обмена ключами, а одновременно с этим симметричное шифрование для обмена данными.