1. **Цифровые подписи и сертификаты в GNU Privacy Guard. Система управления ключей Kleopatra.**

**1. Цель работы.**

Целью лабораторной работы является изучение основных функций программного средства шифрования информации, создание цифровых подписей GnuPG, получение навыков работы с данным программным средством.

**2. Теоретическая часть.**

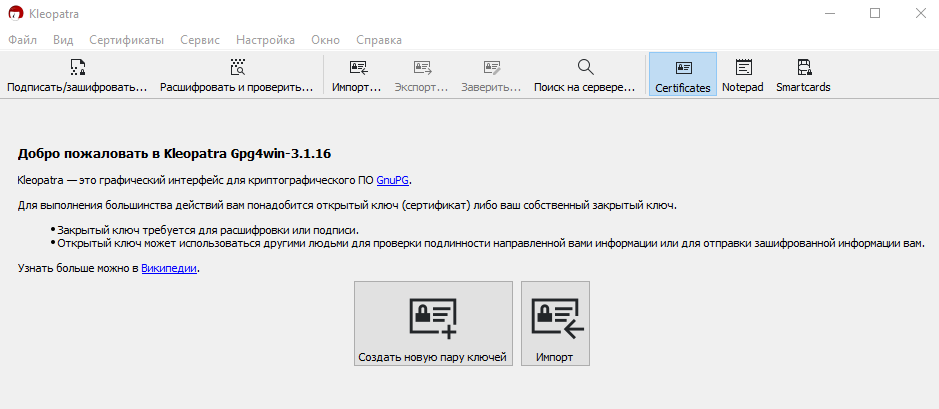
**2.1. Установка GnuPG.**

Ссылка для скачивания установочных файлов GnuPG для Windows: http://gpg4win.org/download.html

При установке программного средства GnuPG рекомендуется установить Менеджер ключей Kleopatra, поскольку дальнейшее руководство в данной лабораторной работе будет приведено для связки Kleopatra+GnuPG.

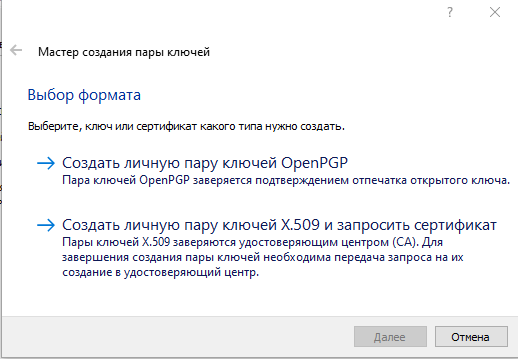
**2.2. Процедура генерации ключей.**

Запустите Менеджер ключей Kleopatra:

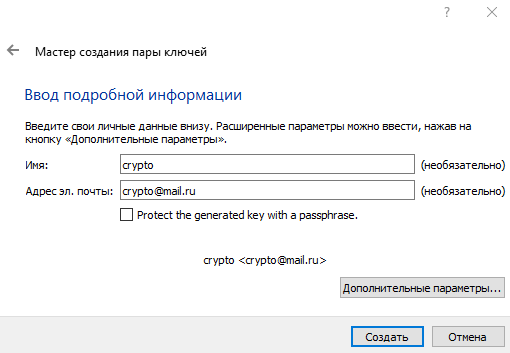


В главном окне программы, которое представлено на вышеприведённом скриншоте, отображаются известные программе ключи (свои пары ключей или открытые чужие ключи). Открытые ключи в программе включаются в сертификаты.

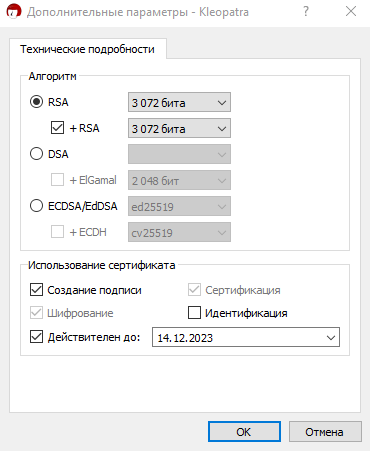
Чтобы создать новую пару ключей, необходимо выбрать пункт меню ***File → New Certificate***, в результате появится окно, показанное на следующемскриншоте:



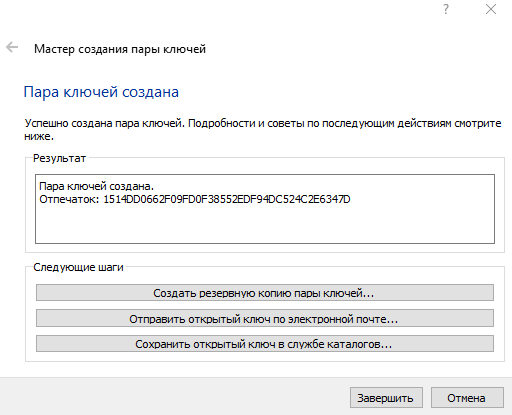
В данной лабораторной работе следует продемонстрировать работу программы по стандарту OpenPGP, поэтому необходимо нажать верхнюю кнопку и перейти в окно, где потребуется заполнить информацию о владельце ключа:



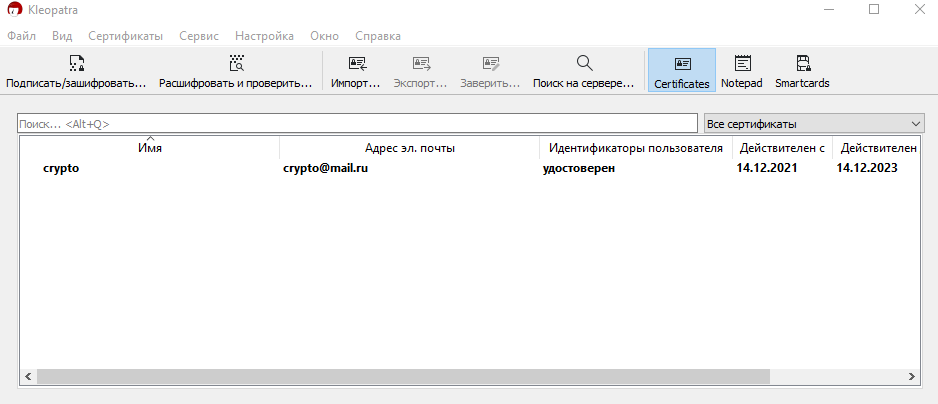
Настройки сертификата можно оставить по умолчанию:



Проверяем правильность введенных данных в следующем окне:



На этом процедура генерации ключей завершена.



**2.3. Процедура экспорта и импорта ключей.**

Для обмена открытыми частями ключевых пар необходимо иметь возможность экспортировать и импортировать открытые части ключей. Для экспорта открытого ключа необходимо выбрать нужный сертификат из списка главного окна программы Kleopatra и выбрать пункт меню ***File → Export Certificates***.

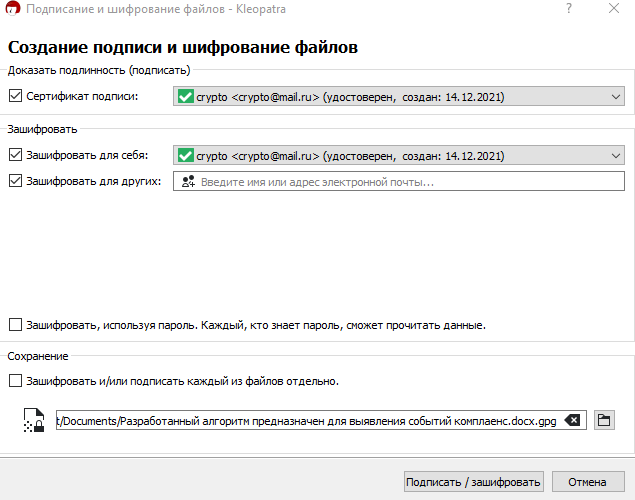
Сохраняем файл с расширением ***.asc***

Для импорта чужого открытого ключа необходимо выбрать пункт меню File →Import Certificates и выбрать файл сертификата (в данной лабораторной работе операции экспорта и импорта производятся с файлами формата ***.asc***).

**2.4. Шифрование и цифровая подпись файлов.**

Процедуры шифрования и цифровой подписи файлов в менеджере ключей

Kleopatra проходят схожим образом. В Kleopatra выбирается пункт меню ***File → Sign/Encrypt Files*** и выбирается целевой файл, после чего открывается окно:



В данном окне можно сделать выбор, какую процедуру осуществить с файлом:

- Encrypt (зашифровать);

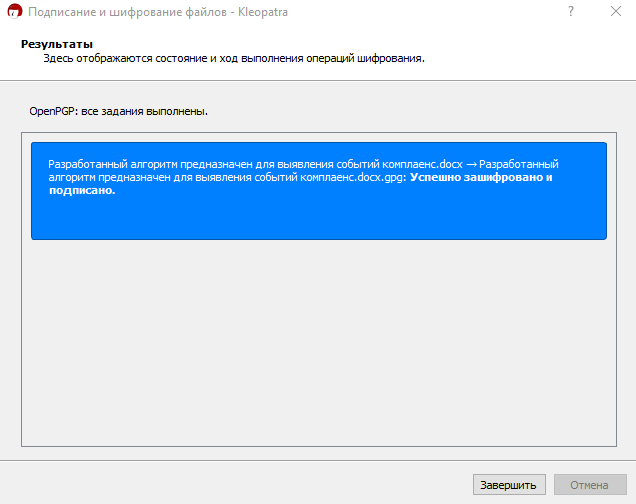
- Sign (подписать).

В данном окне необходимо выбрать сертификаты тех, для кого предназначено сообщение. Здесь можно задать процесс шифрования таким образом, чтобы сообщение могли расшифровать несколько человек.

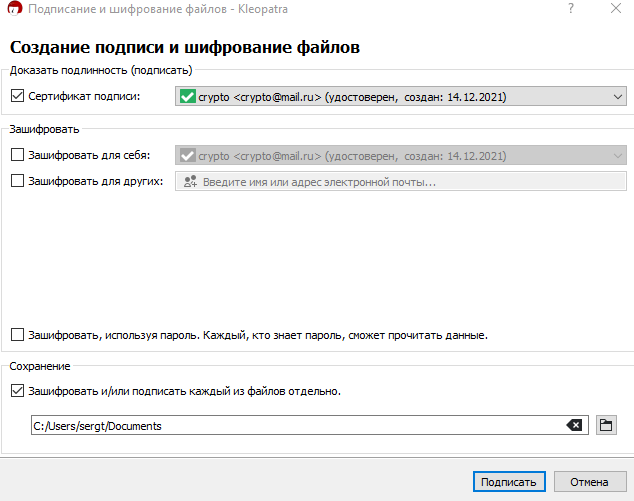
После нажатия кнопки ***Encrypt*** происходит процесс шифрования.

В результате будет создан файл формата ***.gpg***, который является зашифрованным файлом.

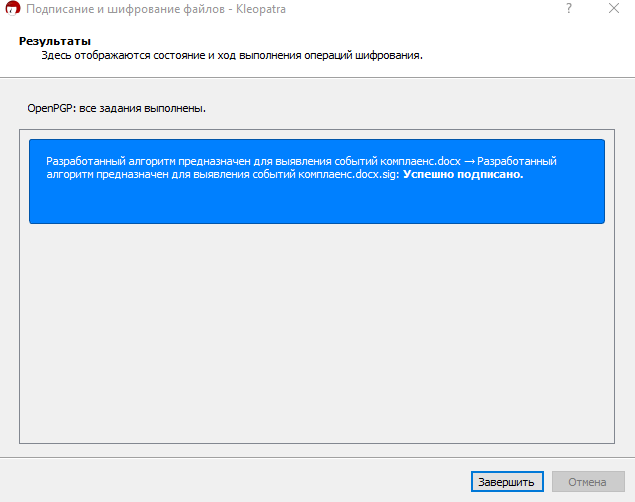
В случае, если был выбран пункт цифровой подписи, откроется окно:



В данном окне необходимо подтвердить использование стандарта OpenPGP. Далее ввести пароль для закрытой части ключевой пары, если он указывался при ее создании.



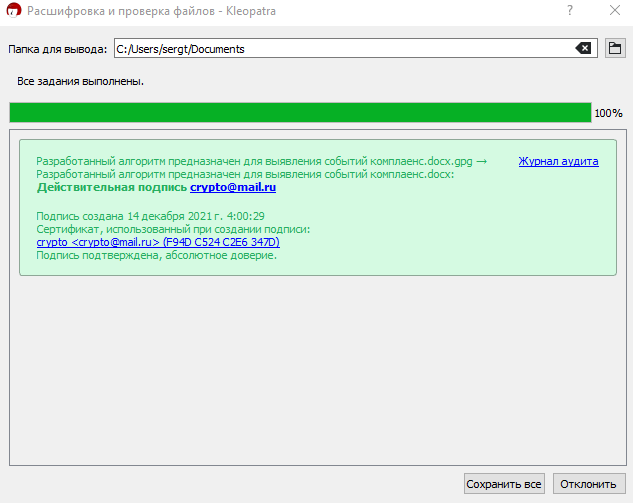
В результате будет создан файл формата ***.sig***, который будет являться цифровой подписью файла.

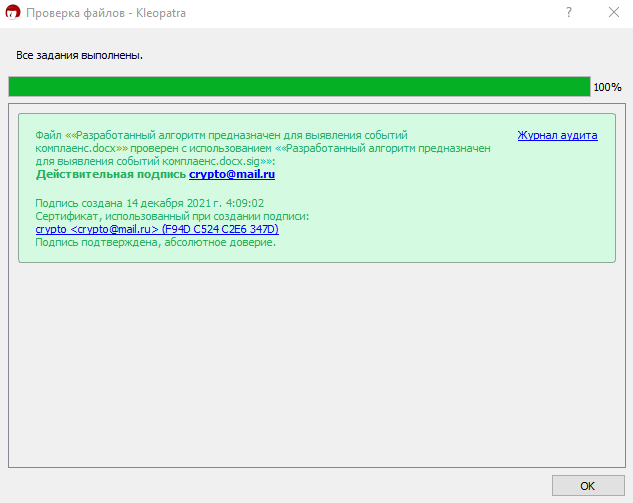


**2.5. Процедура дешифрования и проверки цифровой подписи.**

Процедуры дешифрования и проверки цифровой подписи файлов в менеджере ключей Kleopatra проходят схожим образом. В Kleopatra выбирается пункт меню ***File → Decrypt/Verify Files*** и выбирается зашифрованный файл (.gpg) или цифровая подпись (.sig), после чего открывается окно.

В результате будет получен дешифрованный файл или сообщение об успешной проверке цифровой подписи (в зависимости от того, что было выбрано):





**3. Порядок выполнения работы.**

1 Установите GnuPG и менеджер ключей Kleopatra на свою операционную систему.

2. Сгенерируйте новую пару ключей (создайте новый сертификат), следуя инструкциям, данным в Теоретической части данной лабораторной работы.

3. Экспортируйте открытую часть сгенерированной пары ключей в файл ***key.asc*** и приложите к отчету.

4. Составьте небольшой файл с названием ***notion.doc***, содержащий краткое определение термина (3-4 предложения), в зависимости от выбранного Вами варианта из таблицы ниже:

| **Вариант** | **Термин** |
| --- | --- |
| 1 | Симметричная система шифрования |
| 2 | Асимметричная система шифрования |
| 3 | Поточный шифр |
| 4 | Криптографический протокол |
| 5 | Цифровая подпись |
| 6 | Хэш |
| 7 | Криптостойкость шифра |
| 8 | Brute-force |
| 9 | Имитозащита |
| 10 | Имитовставка |
| 11 | Криптоанализ |
| 12 | Side channel attack |
| 13 | Ключ |
| 14 | Блочный шифр |
| 15 | Цифровой сертификат |
| 16 | Факторизация целых чисел |
| 17 | Дискретное логарифмирование |

5. Создайте цифровую подпись для файла ***notion.doc***, используя сгенерованную Вами пару ключей, и приложите файл цифровой подписи ***notion.doc.sig*** к отчету.

6. Осуществите проверку созданной Вами цифровой подписи и отразите результат в отчете.

7. Зашифруйте файл ***notion.doc***, используя импортированный открытый ключ (файл ***crypto.asc***) и приложите к отчету результат шифрования ***notion.doc.gpg.*** Импортированным ключом может являться вторая пара ключей или может использоваться открытый ключ, созданный одногруппником.

Кроме обязательных элементов отчета (титульный лист, цель, выводы, ход работы со скриншотами, подтверждающими выполнение задач практической работы) необходимо прикрепить в приложение три следующих файла:

* key.asc (экспортированная открытая часть ключа);
* notion.doc.sig (цифровая подпись файла, сделанная с помощью сгенерированной пары ключей);
* notion.doc.gpg (зашифрованный с помощью некоторого импортированного ключа).

**Вопросы для защиты**

1. Подписи DSA (ECDSA), подпись Эль-Гамаль. Подробное описание одного алгоритма подписи на выбор
2. Структура сертификата. Поля сертификата X.509. Корневые и промежуточные центры сертификации (CA)
3. Одноразовые, групповые и пороговые подписи
4. Системы управления и хранения криптографических ключей
5. Протоколы установления и распределения ключей. Транспортные протоколы и протоколы согласования. Модели злоумышленника. Атаки на протоколы установления и распределения ключей (MITM, replay, reflection атаки).
6. Дополнение (padding) и маскировка в цифровых подписях.
7. Повторное использование эфемерных ключей в цифровых подписях.