Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение   
высшего образования   
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

Институт радиоэлектроники и информационных технологий - РТФ

**УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ**

Дисциплина: Криптографические методы защиты информации  
Тема: **Создание ключей с помощью Kleopatra. Создание корневого и заверенного сертификата. Обмен зашифрованными данными**

Екатеринбург 2020

**Оглавление**

[Введение 3](#_Toc40350618)

[Цель работы 4](#_Toc40350619)

[Теоретические положения 5](#_Toc40350620)

[Общие сведения 5](#_Toc40350621)

[Механизм работы PGP 5](#_Toc40350622)

[GPG4Win 5](#_Toc40350623)

[Особенности 6](#_Toc40350624)

[Kleopatra 6](#_Toc40350625)

[Криптографическая система с открытым ключом 8](#_Toc40350626)

[Схема шифрования с открытым ключом 9](#_Toc40350627)

[Лабораторный практикум 10](#_Toc40350628)

[Подготовка к лабораторной работе 10](#_Toc40350629)

[Создание ключей 13](#_Toc40350630)

[Шифрование файлов 18](#_Toc40350631)

[Обмен ключами 21](#_Toc40350632)

[Обмен зашифрованными данными 23](#_Toc40350633)

[Контрольные вопросы 27](#_Toc40350634)

# Введение

В современном мире очень важно соблюдать принципы и аспекты информационной безопасности (далее – ИБ). Ключевыми задачами ИБ в нынешних реалиях является обеспечение конфиденциальности и целостности данных. Важно понимать, что выполнять надежные процессы хранения, обработки и передачи информации может не только дорогостоящая техника на государственном уровне, но и любой компьютер у обычного гражданина.

Один из способов – использование компьютерных программ, позволяющих выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде. Данная лабораторная работа предлагает познакомиться студенту с принципами подобного шифрования и дать практическое применение на примере системы Kleopatra.

**Цель работы**

1. Ознакомиться со сведениями о программе Kleopatra

2. Ознакомиться с составом программных средств, входящих в систему Kleopatra, изучить справку о системе.

3. Создать криптографические ключи с помощью программы. Изучить порядок создания ключей шифрования в системе Kleopatra. Создание корневого и заверенного сертификата.

4. Изучить способы шифрования и дешифрования файлов с помощью программы Kleopatra. Узнать, как происходит обмен ключами.

# Теоретические положения

**PGP** (англ. *Pretty Good Privacy*) — 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.

## Общие сведения

PGP имеет множество реализаций, совместимых между собой и рядом других программ (GnuPG, FileCrypt и др.) благодаря стандарту OpenPGP (RFC 4880), но имеющих разный набор функциональных возможностей. Существуют реализации PGP для всех наиболее распространённых операционных систем. Кроме свободно распространяемых реализаций есть еще и коммерческие.

## Механизм работы PGP

[Шифрование](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) PGP осуществляется последовательно хешированием, сжатием данных, шифрованием с симметричным ключом, и, наконец, шифрованием с открытым ключом, причём каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов. Симметричное шифрование производится с использованием одного из семи симметричных алгоритмов ([AES,](http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) [CAST5,](http://ru.wikipedia.org/wiki/CAST5) [3DES,](http://ru.wikipedia.org/wiki/Triple_DES) [IDEA,](http://ru.wikipedia.org/wiki/IDEA) [Twofish,](http://ru.wikipedia.org/wiki/Twofish) [Blowfish,](http://ru.wikipedia.org/wiki/Blowfish) [Camellia)](http://ru.wikipedia.org/wiki/Camellia_(%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC)) на сеансовом ключе. Сеансовый ключ генерируется с использованием криптографически стойкогогенератора псевдослучайных чисе[л.](http://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80_%D0%BF%D1%81%D0%B5%D0%B2%D0%B4%D0%BE%D1%81%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB) Сеансовый ключ зашифровывается открытым ключом получателя с использованием алгоритмов [RSA](http://ru.wikipedia.org/wiki/RSA) или [Elgamal](http://ru.wikipedia.org/wiki/Elgamal) (в зависимости от типа ключа получателя). Каждый открытый ключ соответствует имени пользователя или адресу электронной почты.

## GPG4Win

Для пользователей операционной системы Windows вторая ветка GnuPG поставляется сразу с графическим интерфейсом. Начиная с 2005 года разработчиками проекта GnuPG выпускается Gpg4win (GNU Privacy Guard for Windows) — инсталляционный пакет, который включает в себя версию GnuPG для Windows (ядро пакета,само средство шифрования), Kleopatra (менеджер сертификатов), GpgOL (плагин для Outlook), GpgEX( плагин для проводника Windows, используется при шифровании файлов), Claws Mail (полноценная почтовая программа с поддержкой функций GnuPG) и документацию на английском и немецком языке. По сути Gpg4win -это официальная версия GnuPG для платформы Windows и все включённый в этот пакет компоненты также свободны.

## Особенности

* Полная альтернатива PGP.
* Не использует патентованные алгоритмы.
* Распространяется под GNU General Public License. - Полная реализация OpenPGP (RFC2440).
* Расшифрование и аутентификация почтовых сообщений, созданных с помощью PGP 5, 6 и 7.
* Поддержка электронной подписи с помощью алгоритмов DSA, RSA и хеш-функций MD5, SHA-1, SHA-2, RIPE-MD160 и TIGER.
* Работа с асимметричным шифровани-

ем ElGamal и RSA (длина ключа от 1024 до 4096 бит)

* Поддержка блочных алгоритмов симметричного шифрования ElGamal, AES, CAST5, 3DES, Twofish, Blowfish, Camellia, а также IDEA с помощью плагина.
* Поддержка алгоритмов сжатия: ZIP, ZLIB, BZIP2.
* Лёгкая реализация новых алгоритмов с помощью дополнительных модулей.

Поддержка просроченных ключей и подписей. - Интегрированная поддержка HKP серверов ключей.

# Kleopatra

**Kleopatra** — многофункциональное C++ / QT / KDE (kcmutils / kmime) графическое приложение, позволяющее подписывать и шифровать файлы, а также обеспечивает создание, хранение и управление сертификатами и ключами шифрования.

Kleopatra разрабатывается как часть рабочего окружения KDE (KDE Applications / KDE Utilities), поддерживает управление сертификатами X.509 и OpenPGP в ключах шифрования GnuPG (GPG), основные возможности приложения реализованы на криптографической библиотеке libkleo (KDE PIM cryptographic library), использующей функционал GnuPG Made Easy (GPGME).

Kleopatra имеет традиционный для большинства KDE приложений пользовательский интерфейс и множество настроек, во многом приложение аналогично KGpg (KDE приложение для создания и централизованного хранения ключей шифрования и паролей), но имеет множество дополнительных возможностей. Приложение поставляется с параметрами "по умолчанию" обеспечивающих большинству пользователей приемлемый уровень безопасности и комфорта.

Для полноценной работы Kleopatra необходимо наличие хотя бы одной пары ключей, при первом запуске приложением автоматически сканируются каталоги в которых "по умолчанию" находятся ключи GPG (~/.gnupg и пр). Поддерживается импорт сертификатов из файлов множества наиболее распространённых форматов (\*.acs, \*.cer, \*.crt, \*.pem, \*.pfx и др).

Kleopatra с помощью "Мастера создания ключей" позволяет быстро создать пару ключей OpenPGP, просто введя имя и электронную почту (при желании можно изменить алгоритм шифрования), или пару ключей X.509 и запросить сертификат (заверяются удостоверяющим центром), в дальнейшем параметры ключей можно редактировать (из контекстного меню в списке ключей).

С помощью Kleopatra можно шифровать файл или каталог используя симметричное шифрование, данные будут зашифрованы паролем и расшифровать его можно на любом компьютере с GPG (при наличии пароля). Шифрование с ключом намного сложнее, но безопаснее, сначала нужно создать свою пару ключей и задать кодовую разу, приватный и открытый, приватный (секретный) необходим хранить в надёжном месте, а открытый использовать для обмена зашифрованными сообщениями.

Kleopatra поддерживает ASCII шифрование и шифрование с ненадёжными ключами, поддерживается подпись и публикация, а также получение (синхронизация) ключей с LDAP серверами, есть возможность поиска по сервера ключей. В окне менеджера ключей можно просмотреть имеющиеся ключи, отсортировав их по любому параметру, из контекстного меню можно выполнить любое действие с одним и/или несколькими ключами.

Kleopatra простой текст шифрует и расшифровывается в "Блокноте", поддерживается шифрование "на лету" текста из буфера обмена, при наличии клиента электронной почты KMail (разрабатываемый в рамках проекта KDE) зашифрованное письмо можно сразу отправить, а зашифрованное расшифровать. При шифровании к файлам и каталогам добавляется расширение (\*.gpg или \*.pgp), поддерживается создание или проверка контрольной суммы файла (группы файлов) и многое другое...

Kleopatra интегрируется в область уведомлений (системный трей), а также в контекстное меню файловых менеджеров Konqueror и Dolphin (при использовании в рабочем окружении KDE). Для управления большинством функций используется мышь, частично можно использовать клавиатурные сочетания (настраивается).

По сути, мы имеем дело с криптосистемой с открытым ключом.

## Криптографическая система с открытым ключом

**Криптографическая система с открытым ключом** — система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH.

Асимметричное шифрование с открытым ключом базируется на следующих ***принципах***:

* Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. При этом механизм генерации является общеизвестным.
* Имеются надёжные методы шифрования, позволяющие зашифровать сообщение открытым ключом так, чтобы расшифровать его можно было только закрытым ключом. Механизм шифрования является общеизвестным.
* Владелец двух ключей никому не сообщает закрытый ключ, но передает открытый ключ контрагентам или делает его общеизвестным.
* Если необходимо передать зашифрованное сообщение владельцу ключей, то отправитель должен получить открытый ключ. Отправитель шифрует свое сообщение открытым ключом получателя и передает его получателю (владельцу ключей) по открытым каналам. При этом расшифровать сообщение не может никто, кроме владельца закрытого ключа.

В результате можно обеспечить надёжное шифрование сообщений, сохраняя ключ расшифровки секретным для всех - даже для отправителей сообщений.

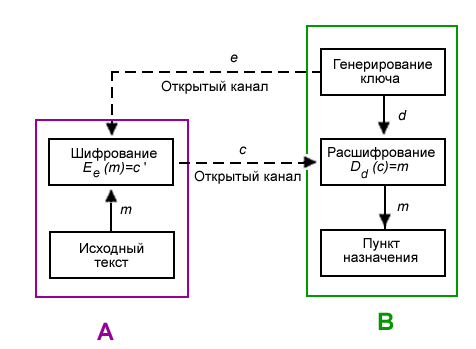
## Схема шифрования с открытым ключом

Пусть К — пространство ключей, а *e* e» и *d*d» — ключи шифрования и расшифрования соответственно Ее — функция шифрования для произвольного ключа*, такая что* Ее(m) = *с*

Здесь с принадлежит С, а m прин. М, где М – пространство сообщений.

Dd – функция расшифрования, с помощью которой можно найти исходное сообщение *m*, зная шифротекст *с*: Dd(с) = m

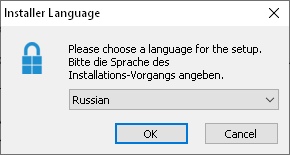
Ниже показана схема передачи информации лицом А лицу В. Они могут быть как физическими лицами, так и организациями и так далее. Но для более лёгкого восприятия принято участников передачи отождествлять с людьми, чаще всего именуемыми Алиса и Боб. Участника, который стремится перехватить и расшифровать сообщения Алисы и Боба, чаще всего называют Евой.

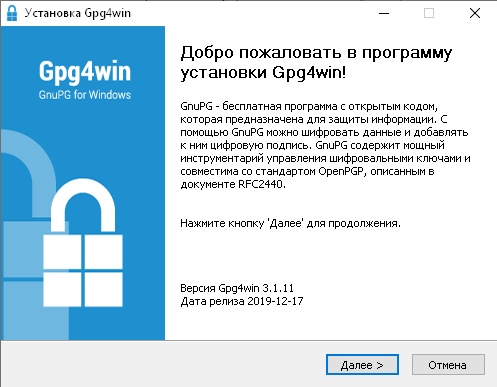


# Лабораторный практикум

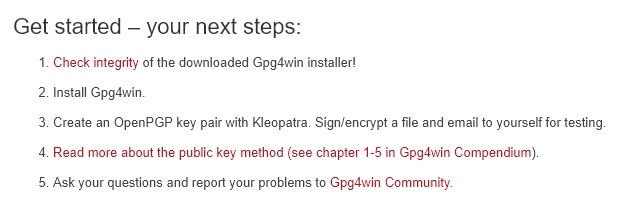
## Подготовка к лабораторной работе

1. Ознакомьтесь с теоретическим материалом
2. Для того, чтобы скачать и установить gpg4win с встроенным менеджером сертификатов, вам нужно перейти по данной ссылке: <http://www.gpg4win.org/download.html>
3. Для начала установки нажмите «Далее»

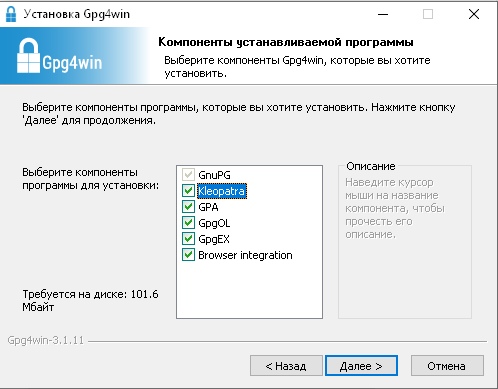




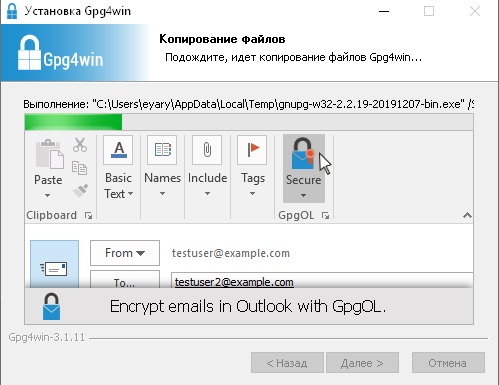
1. Ознакомьтесь с установочным пакетом и лицензией



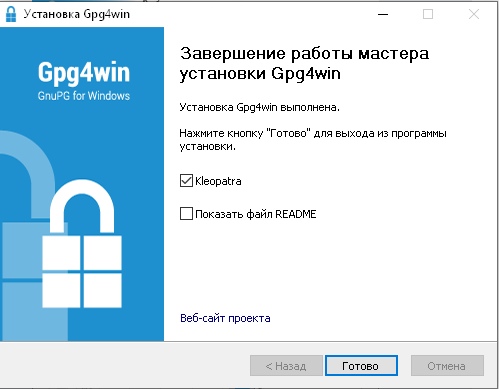
1. Отметьте те пункты, которые должны быть выбраны для выполнения лабораторной работы



1. На последнем шаге укажите каталог в меню «Пуск» и нажмите «Установить», после чего дождитесь установки



1. Выбираем необходимую нам «Клеопатру»

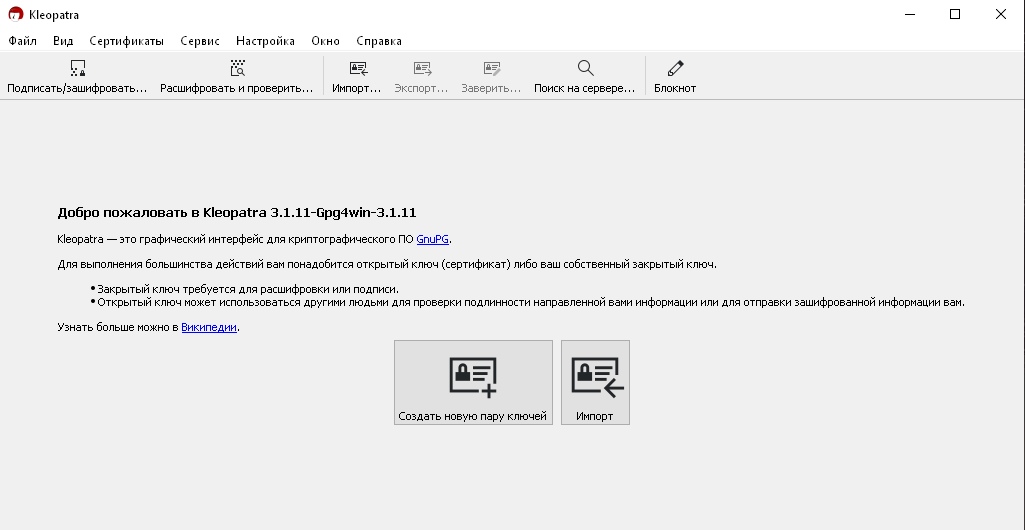


## Создание ключей

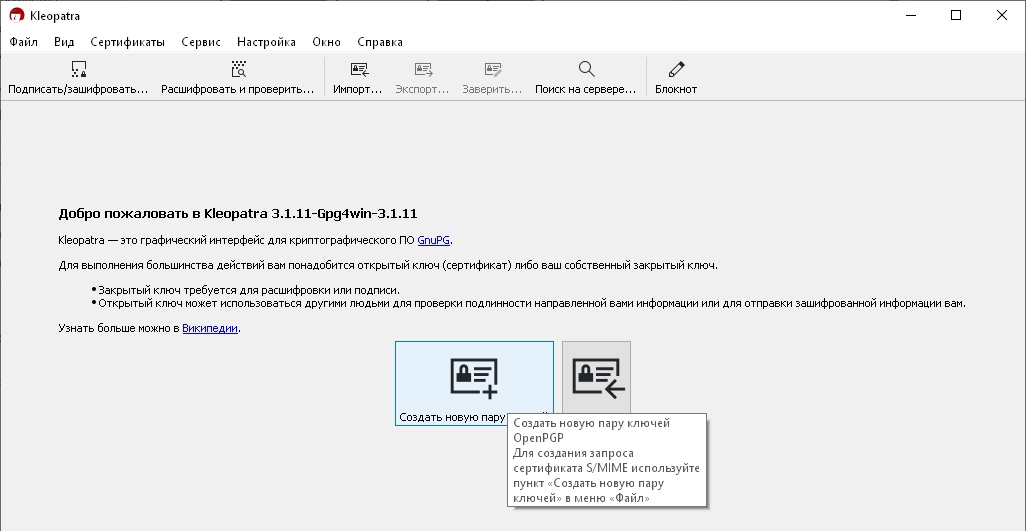
1. Для создания ключа вам необходимо запустить утилиту Kleopatra.ехе

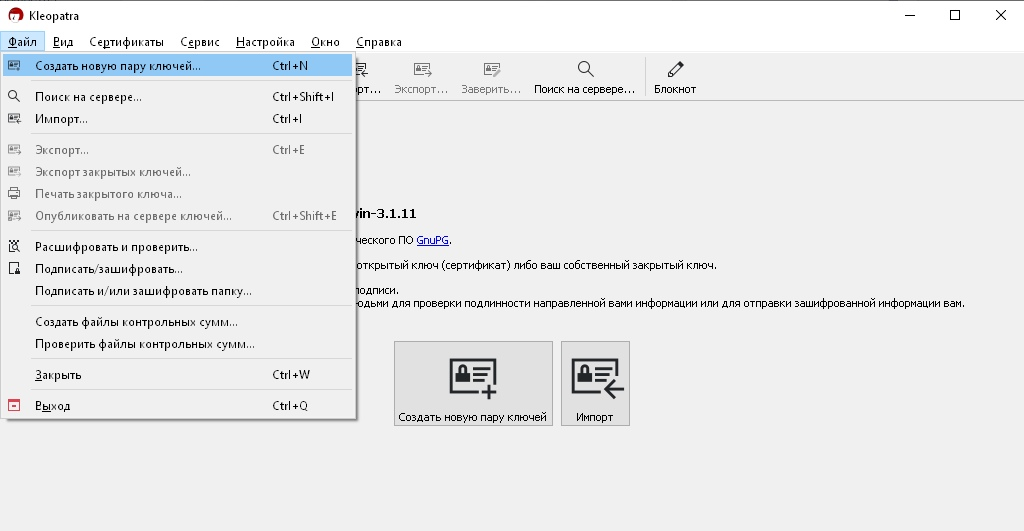


1. Убедитесь, что открылось окно управления ключами:

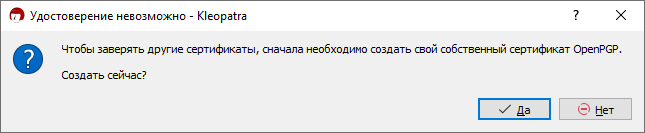


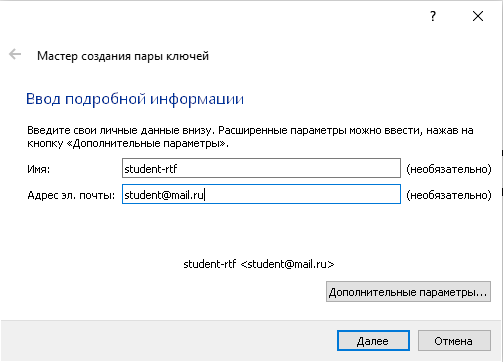
1. Для создания ключа вы можете воспользоваться кнопкой "создать новую пару ключей на главном экране утилиты. Или нажмите «Файл» -> «Создать новую пару ключей». Также создать новую пару ключей можно с помощью сочетания клавиш "Ctrl + N".



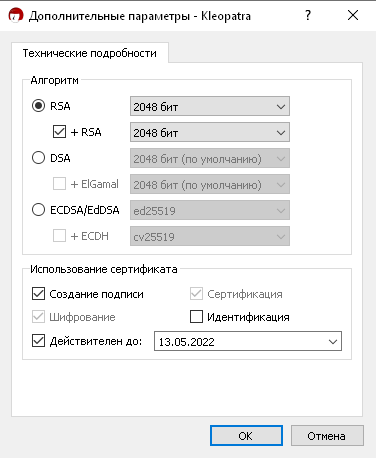


1. Выберете пункт создания обычной пары и нажмите “Далее”
2. Система предложит Вам заполнить свои персональные данные, нажмите “Да”.   
   Далее откроется Мастер создания пары ключей, и Вам нужно заполнить все требуемые данные.

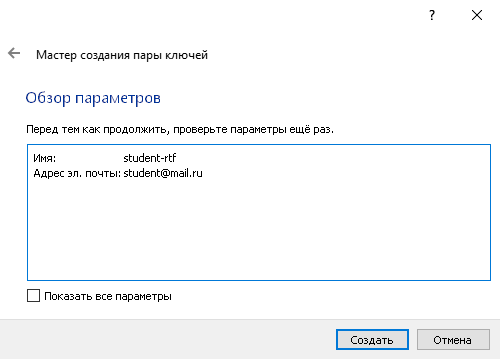


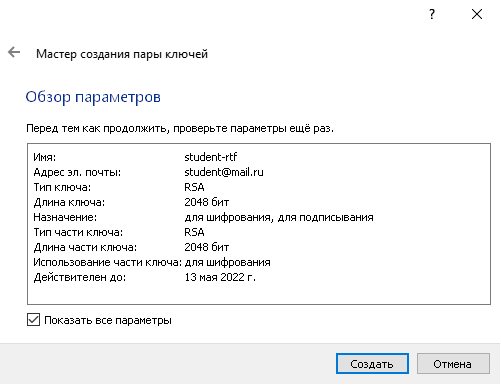


1. Также можно ознакомиться с настройками сертификата. Ознакомьтесь с заполнением Дополнительных параметров. Чем отличаются предложенные алгоритмы? Что еще можно изменить в предложенных параметрах?

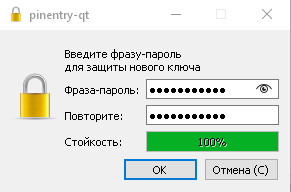


1. Подтвердите введенную ранее информацию, также если Вы меняли дополнительные параметры, можно убедиться в их правильности, нажав на “Показать все параметры”:

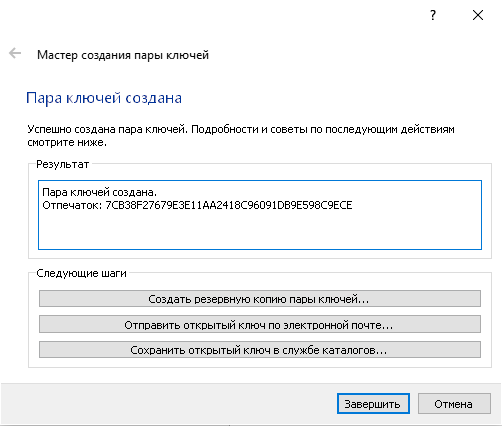




1. Создайте и введите стойкий пароль

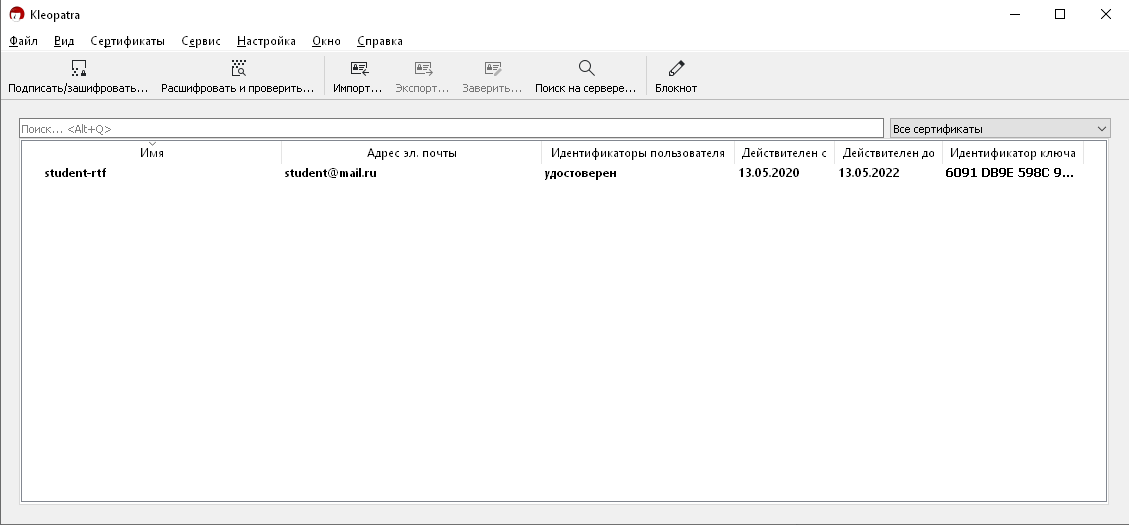


1. Убедитесь, что пара создана

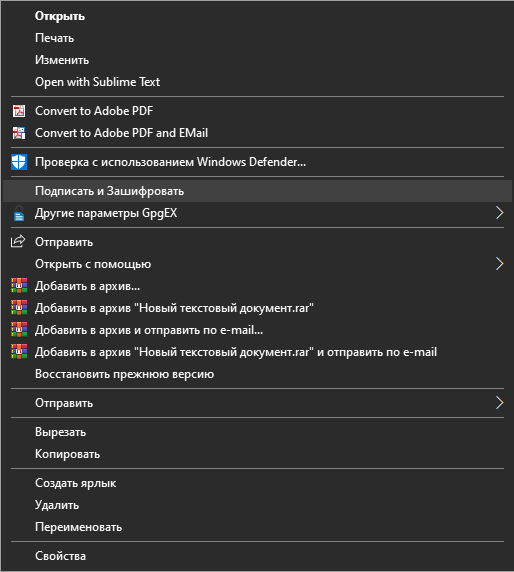


Здесь можно сохранить резервную копию ключей в файл. При этом будет создан бинарный файл с расширением *pgp*, например, *пример.pgp*.

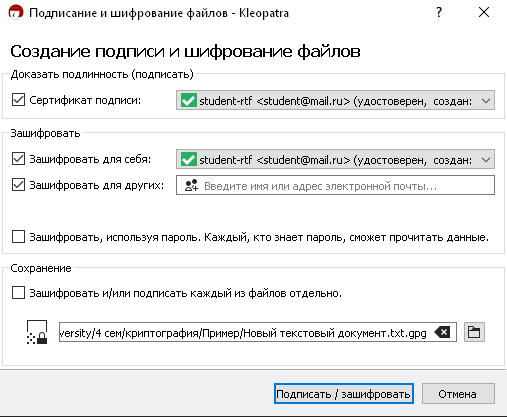
1. Убедитесь в создании сертификата



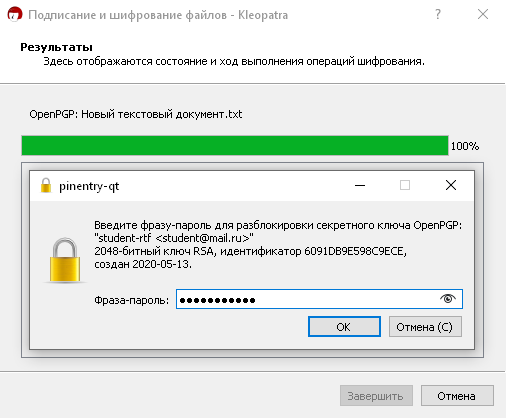
## Шифрование файлов

1. На своем рабочем компьютере выберете файл для зашифровки:

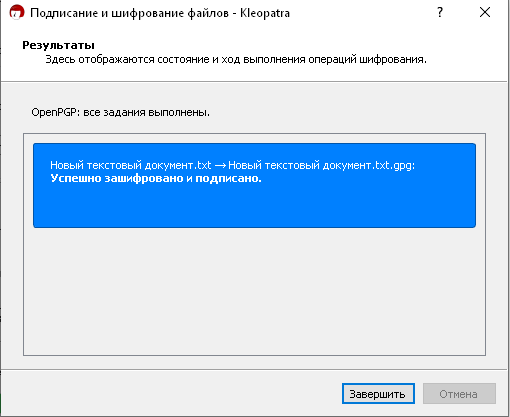
2. Изучите параметры шифрования. Что будет, если не выбрать пункт шифрования с паролем? Как это повлияет на безопасность?



3. Введите фразу пароль. Возможна ли подмена идентификатора?

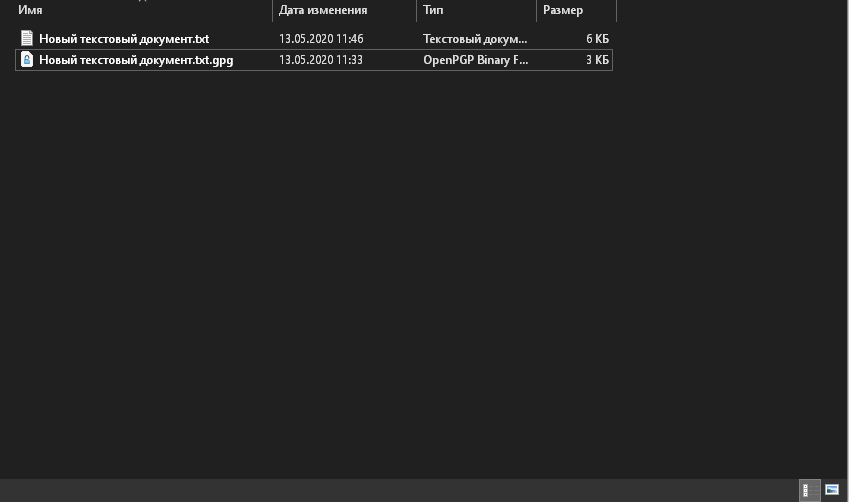


4. Нажмите кнопку Завершить.



Перед тем, как выполнять следующую часть лабораторной работы, вам необходимо объединиться со вторым студентом, который также проделал все предыдущие пункты.

5. Убедитесь, что на вашем компьютере присутствует зашифрованный ранее файл.

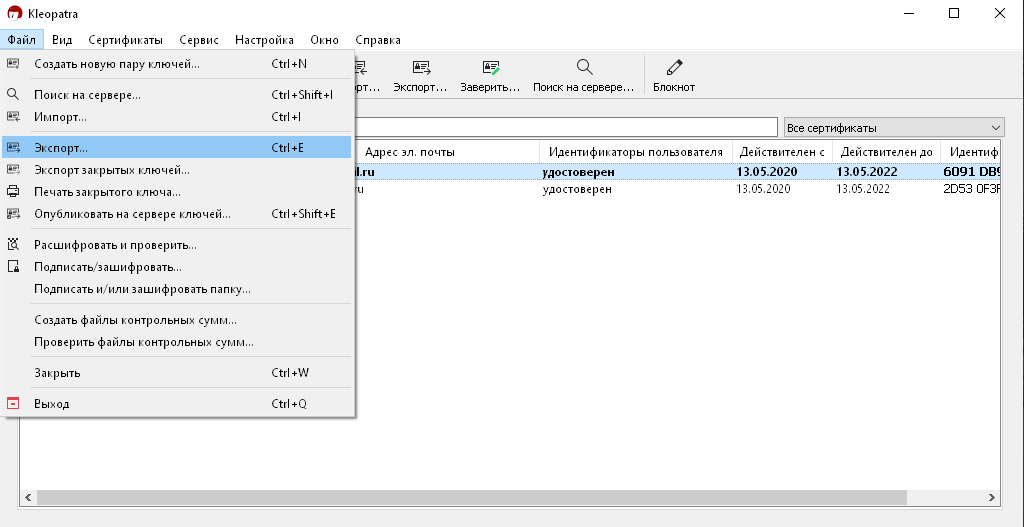


6. Обменяйтесь зашифрованными файлами со своим напарником.

7. Попробуйте расшифровать полученный от напарника файл, получилось ли? Объясните почему.

## Обмен ключами

1. Вы и ваш напарник имеете по паре ключей. Обменяйтесь ими. Выбираем нужный сертификат из списка и переходим “*файл*” -> “*экспорт*”, как показано ниже:



Также можно воспользоваться сочетанием клавиш Ctrl+E.

2. Программа предложит сохранить файл с расширением asc.

3. Сохраните файл.

4. В итоге вы должны получить файл (его можно открыть с помощью текстового редактора), который будет выглядеть примерно так:



5. Обменяйтесь данными файлами или просто передайте текст ключа, добавив его в текст электронной почты, или сообщения зашифрованного канала в телеграмме.

При этом не забывайте оставить *шапку* ——BEGIN PGP PUBLIC KEY BLOCK—— и *подвал* ——END PGP PUBLIC KEY BLOCK——

6.  Добавьте открытый ключ вашего напарника в список сертификатов. В программе Kleopatra выберите пункт меню “Файл” -> “Импорт…” и выберите файл .asс, который вам дал напарник.

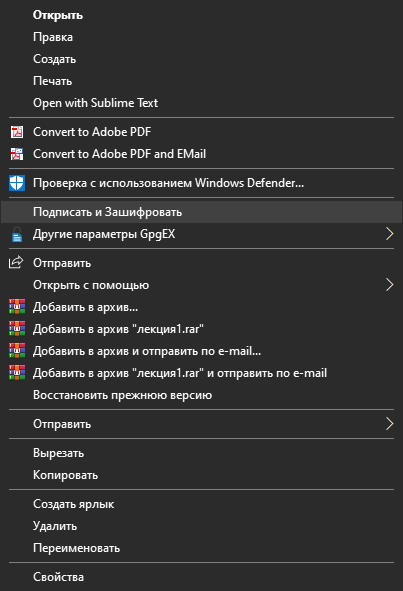
7. Если ваш напарник дал вам свой ключ в виде текста, а не файла, тогда вы должны перейти в пункт меню «*Файл» -> «Импорт сертификата»* и вставить текст ключа (включая шапку и подвал).

1. Появится сообщение о том, что ключ импортировался. Теперь в вашем списке сертификатов у вас появится ключ вашего напарника. Если он у вас не появился, объясните почему.
2. Двойным кликом откройте сертификат и изучите информацию. Прокомментируйте. Какой уровень доверия отмечен?
3. Перейдите в “Подробные сведения…”, также прокомментируйте.

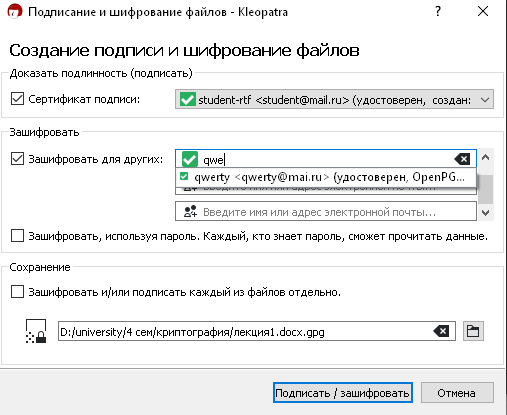
11. Найдите информацию о ключе. Какой тип идентификатора стоит? Что он обозначает? Прокомментируйте тип алгоритма RSA, каковы его преимущества?

## Обмен зашифрованными данными

1. Создайте новый текстовый файл с произвольным названием и произвольным содержанием.
2. Сохраните файл с кодировкой UTF-8 и закройте его. В конце можете проделать все то же, только с другой кодировкой. Что изменится?
3. Откройте контекстное меню созданного файла и выберите “Подписать и Зашифровать”, как показано ниже:

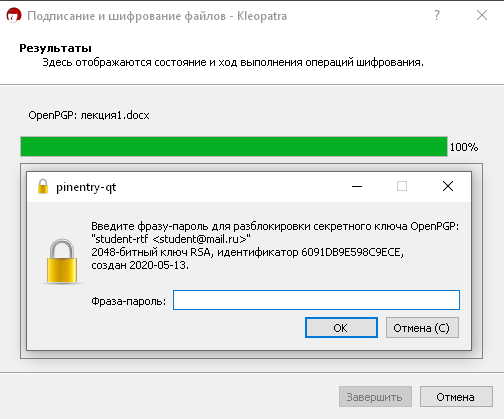


1. В появившемся окне снимите галочку с пункта “Зашифровать для себя” и начните заполнять поле “Зашифровать для других” ник/почту вашего напарника. Выберите его из выпадающего списка.

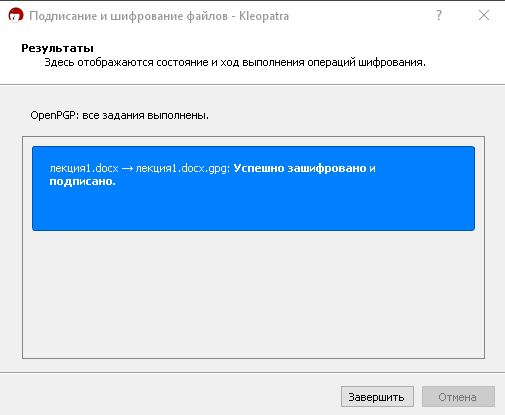


Примечание: как вы можете заметить, можно добавлять несколько человек, для которых будут шифроваться данные.

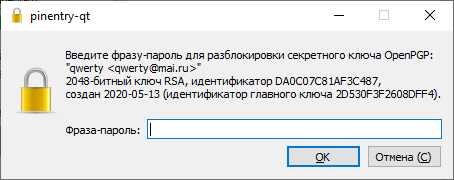
1. Нажмите кнопку “Подписать / зашифровать”.
2. Вам будет показано предупреждение о шифровании для себя. Далее будет сообщение о том, что вы не сможете расшифровать данные.
3. Введите фразу-пароль для окончания шифрования.



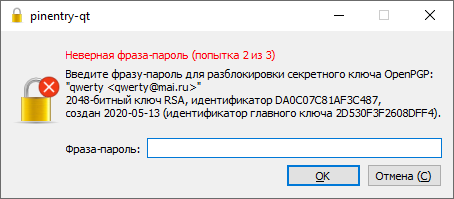
1. Проверьте, что файл успешно зашифрован.



1. Рядом с файлом *произвольное\_имя.txt* будет создан файл *произвольное\_имя.txt.gpg*. Это и есть зашифрованное сообщение.
2. Теперь вы можете переслать зашифрованный файл напарнику.
3. Когда вы получили зашифрованный файл от напарника, нажмите правой кнопкой мыши на полученный файл и нажмите “Расшифровать и проверить”.
4. Введите фразу-пароль, с помощью которой было зашифрован исходный файл

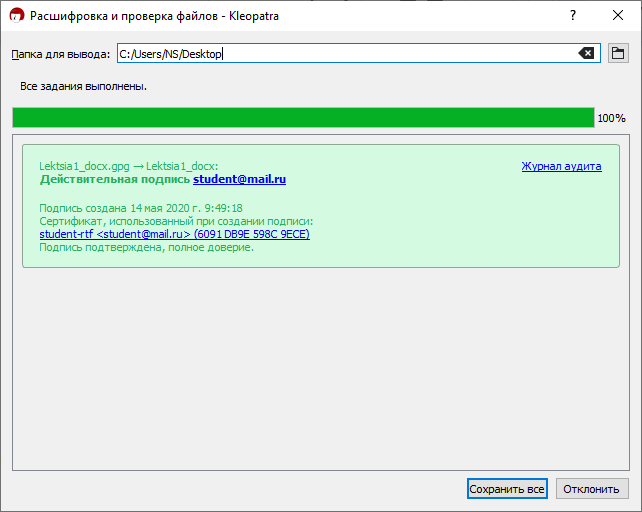


Примечание: если будет введен неверный пароль, то вы увидите такое уведомление об оставшихся попытках:



Если пароль не будет введен правильно 3 раза, возможно ли будет расшифровать далее файл?

1. Проверьте, удалось ли получить такое оповещение:



1. Проверьте журнал аудита. Какая информация содержится в нем? Как это повлияет на безопасность, если злоумышленник получит все коды идентификаторов ключа?

# Контрольные вопросы

1) Для чего предназначена программа Gpg4win и Kleopatra?

2) Как с помощью программы Kleopatra создать ключи?

3) Для чего применяются открытый (публичный) и закрытый (секретный) ключи?

4) Как и для чего осуществляется шифрование файлов?

5) Как изменить свой пароль? В каких случаях это необходимо?

6) Назовите способы шифрования текстовых файлов с помощью Gpg4win.

7) Как проверяется достоверность ключа?

8) Как удалить устаревшие ключи?

9) Как дешифровать закрытый файл?

10) Какова длина ключа, использованного в данной работе?

11) Перечислите способы обмена открытыми ключами.

12) Что такое идентификатор пользователя?

13) Какие компоненты включает программа Gpg4win?

14) Какие алгоритмы шифрования используются в программе Kleopatra?