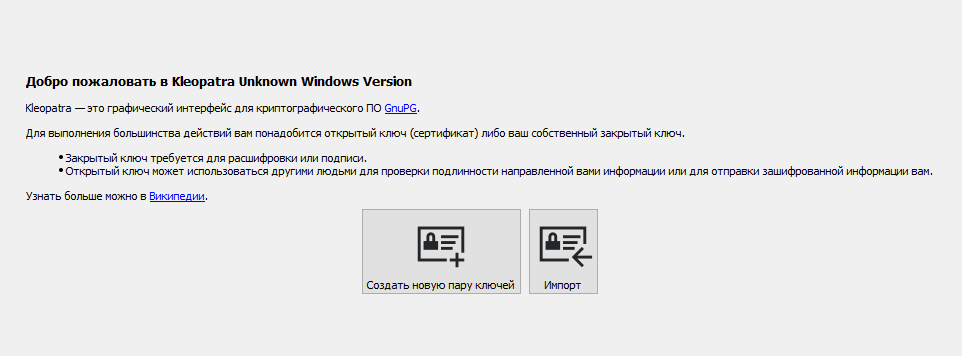
Безопасная переписка в почте с использованием ключей шифрования PGP (OpenPGP).

Использовать PGP шифрования для обеспечения безопасности переписки можно разными способами, но мы рассмотрим лишь пару из них - шифрование файлов и программа, интегрированная в электронную почту, которая зашифровывает сообщения автоматически.

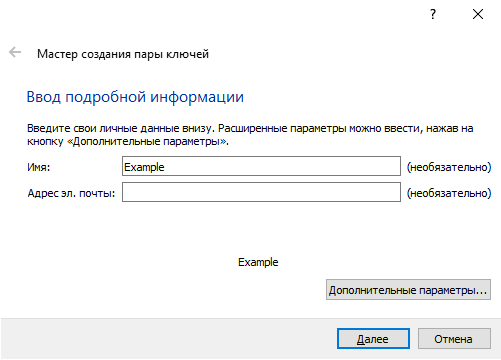
Во-первых - скачаем GnuPG с их официального сайта: https://gnupg.org/download/index.html.

GNU Privacy Guard (GnuPG, GPG) — свободная программа для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) информации и создания электронных цифровых подписей. Разработана как альтернатива [PGP](https://ru.wikipedia.org/wiki/Pretty_Good_Privacy) и выпущена под свободной лицензией [GNU General Public License](https://ru.wikipedia.org/wiki/GNU_General_Public_License). GnuPG полностью совместима со стандартом [IETF](https://ru.wikipedia.org/wiki/Internet_Engineering_Task_Force) [OpenPGP](https://ru.wikipedia.org/wiki/OpenPGP). Текущие версии GnuPG могут взаимодействовать с [PGP](https://ru.wikipedia.org/wiki/PGP) и другими OpenPGP-совместимыми системами.

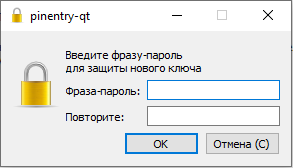
Во время установки укажите необходимость установить все дополнения. По окончанию установки запустите программу Kleopatra и, скорее всего, вы увидите следующее:



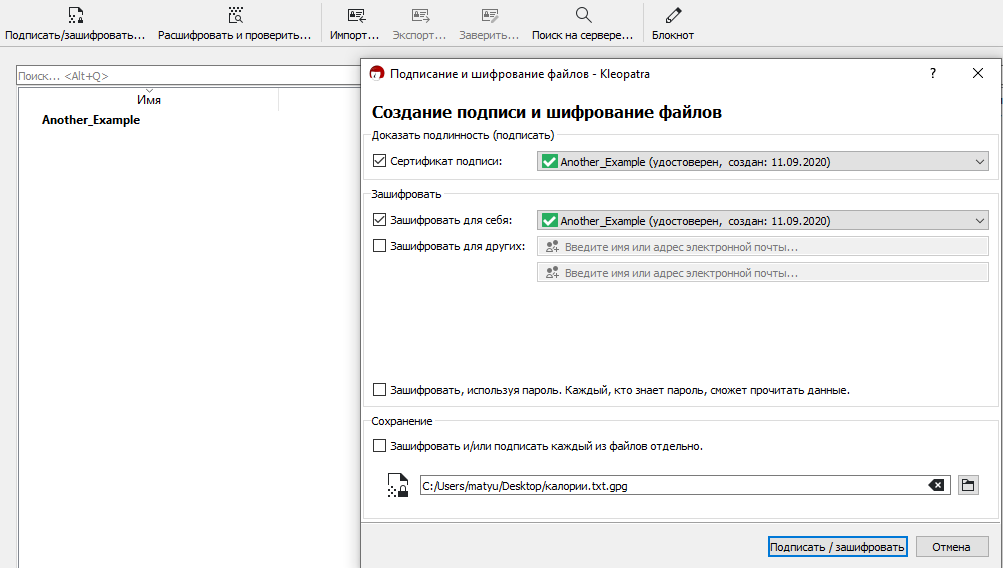
Создайте новую пару ключей, для этого достаточно указать имя либо же адрес электронной почты. Также на этом шаге вы можете настроить дополнительные параметры: алгоритмы шифрования, срок действия ключа и т.д.



Затем вас попросят указать секретную фразу, по которой вы будете получать доступ к закрытому ключу и подождать несколько секунд.



Теперь у вас есть рабочий ключ и вы можете зашифровывать файлы. Для этого достаточно нажать на соответствующую кнопку в левом верхнем углу. В появившемся окне выберите необходимые настройки. Если всё пройдёт хорошо, программа уведомит вас об этом.



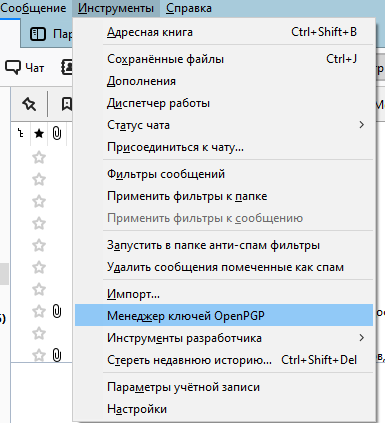
Теперь вы можете проверить работу ключей:  
1) Зашифруйте файл, а также экспортируйте закрытый ключ после чего удалите его. Вы можете удостовериться, что расшифровать файл более не удастся. Импортируйте закрытый ключ и проверьте, сможете ли расшифровать файл теперь.

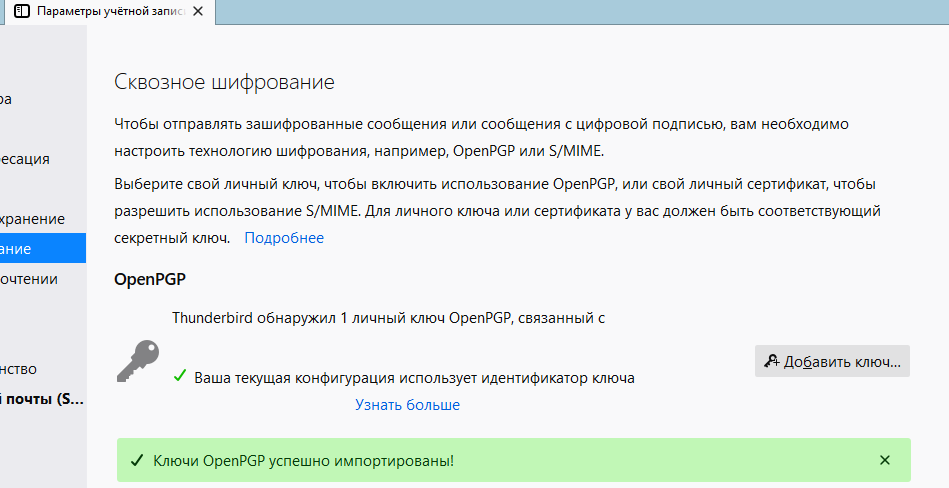
2) Экспортируйте свой открытый ключ одногруппнику и получите от него зашифрованный файл - расшифруйте его с помощью своего ключа. Удостоверьтесь, что ваш одногруппник, имеющий открытый ключ - не может расшифровать созданный вами файл. Для удобства вы так же можете использовать внутренний блокнот Kleopatra, и зашифровывать текст, который потом удобно отправить сообщением.

Другой метод: установка Thunderbird - программы для работы с электронной почтой <https://www.thunderbird.net/ru/>

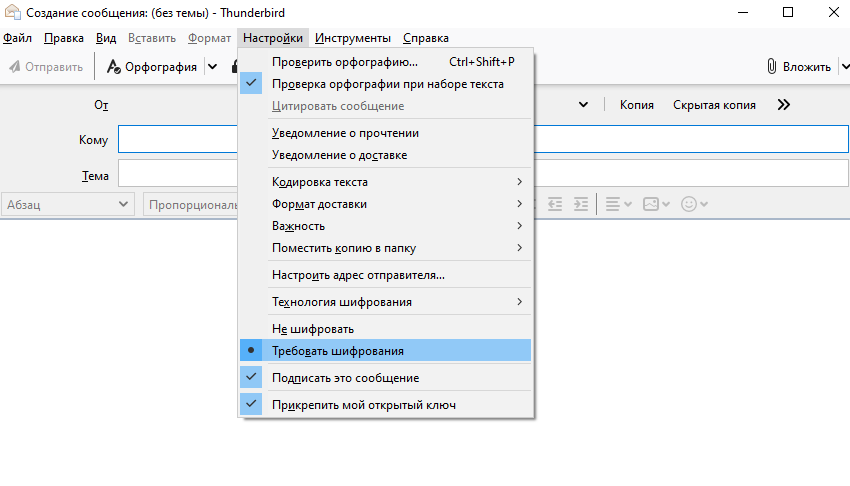
После установки интегрируйте свою почту с Thunderbird.

Во вкладке “Инструменты” (если у вас её нет, добавьте панель меню, щёлкнув правой кнопкой мыши по верхней рамке Thunderbird) выберите уже существующий ключ, импортируйте его, либо же создайте новый, после чего привяжите его к своему аккаунту. Вместе с этим импортируйте ключи людей, которым вы собираетесь посылать сообщения.





После этого вы можете отправлять зашифрованные сообщения. Перейдите во вкладку с почтой и создайте новое послание. Во вкладке “Настройки” выберите “Требовать шифрование”, а также остальные параметры по вкусу.



Готово. Можете отправлять сообщение. Возможно вас попросят подтвердить правильность ключа. Сделайте это и снова отправьте сообщение. Удостоверьтесь в том, что всё прошло хорошо, попросив у получателя его письмо.