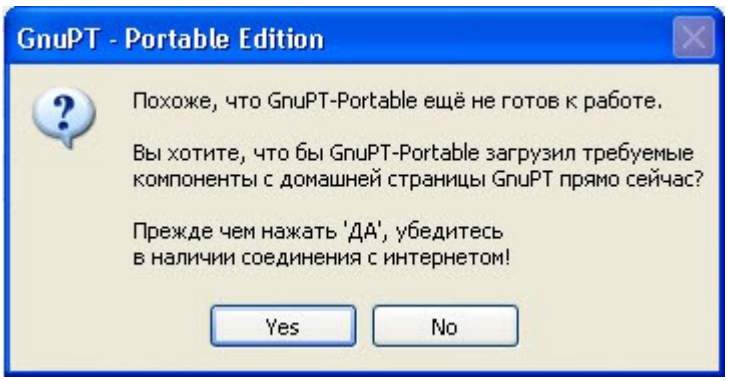
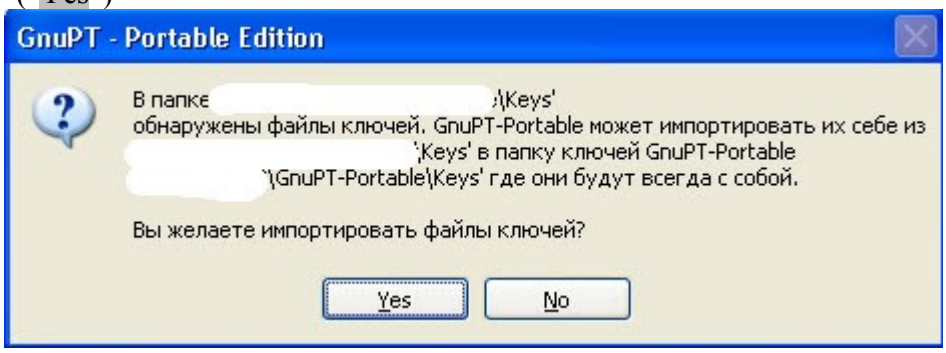
Поговорим о таком протоколе шифрования как GnuPG. Вобщем, если кратко, это протокол шифрования которому есть смысл доверять. Открытые исходники, асимметричное шифрование, огромная криптостойкость. За больше информацией можно взглянуть на вики: http://ru.wikipedia.org/wiki/GnuPG .
Я попытаюсь в скриншотах и пояснениях рассказать как настраивается и используется это чудо криптографии на Windows. Вначале нам нужен сам GnuPG - http://www.gnupg.org/download/ вот он. Смотрим в раздел Binaries – находим там ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.10b.exe (лучше посмотреть самим, тут дается ссылка на текущую версию, а алгоритм постоянно развивается). Качаем и устанавливаем — никаких особых настроек нам не понадобится — все по Default. Дальше есть два пути:
1.Вручную через командную строку создать ключ (для человека прежде этого не делавшего понадобится довольно много времени)
2.Найди GUI инструмент облегчающий работу с GnuPG (этот способ описывается в статье).
Так-с раз мы выбрали второй пункт то нужно найти этот самый инструмент. Я лично пользуюсь WinPT (http://winpt.gnupt.de/int/), хотя по правде говоря этот инструмент устарел и давно не обновляется. Так же есть Gpg4win(http://www.gpg4win.org/) идет сразу вместе с GnuPG и поэтому вам не придется скачивать GnuPG отдельно, GnuPT-Portable (http://portable.gnupt.de/). Рассмотрим интерфейс GnuPG-portable. Скачиваем архив - http://portable.gnupt.de/gnupt_portable.zip и распаковываем (желательно на какой нибудь зашифрованный TrueCrypt'ом USB носитель). Запускаем.
После первого запуска программы появится окошко с настройками. Выберите настройки, как на картинке и нажмите на кнопку “Save and go…”

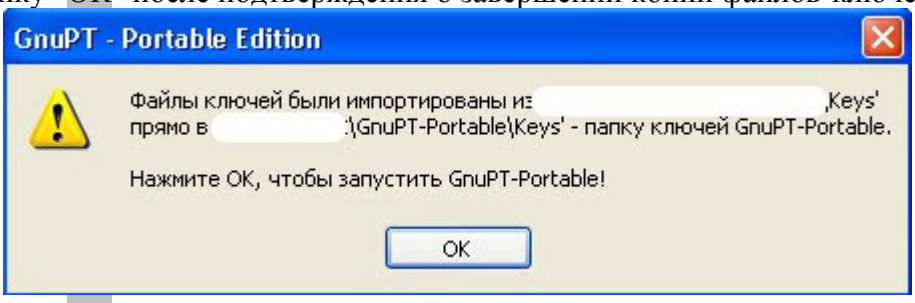
Если всплывёт окошко с вопросом о дозагрузке модулей GnuPT, нажмите на кнопку "ДА" ("Yes”)



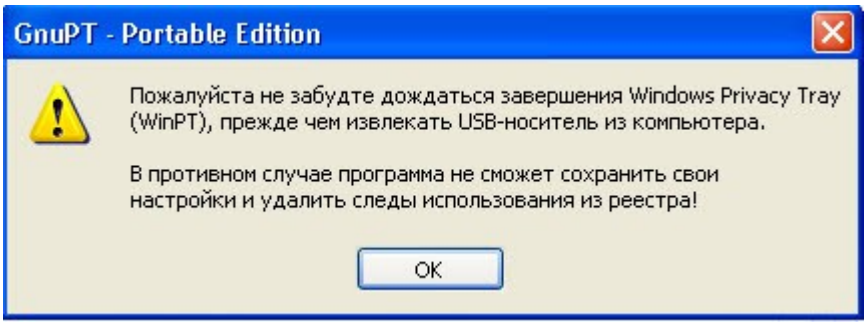
Если вы уже устанавливали какую либо версию или, то может появиться окно с копированием существующих файлов-ключей в место новой установки программы. Нажмите кнопку "ДА" ("Yes")



Нажмите кнопку "ОК" после подтверждения о завершении копии файлов-ключей.



Нажмите кнопку "ОК" для завершения установки программы.



В дальнейшем, для запуска программы с переносного носителя, просто щёлкните мышкой дважды по файлу **GnuPT-Portable.exe**. В правом углу панели задач Windows (Task Bar) найдите новую иконку GnuPT в виде ключа

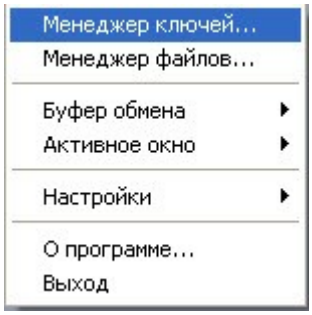
2. Генерация ключей

После установки ***GnuPT***, необходимо создать пару ключей (открытый и закрытый). В

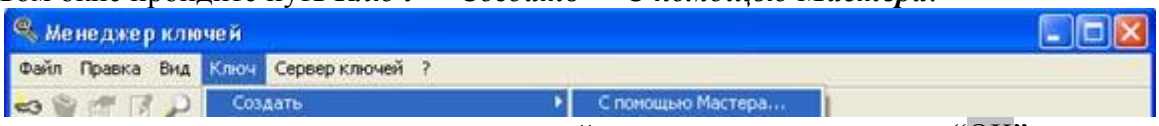
каждой паре ключей её открытый и закрытый ключ неразрывно связаны. Открытый ключ используется для шифрования сообщения, расшифровать которое может только владелец соответствующего закрытого ключа.

Например, пользователь А желает отправить зашифрованное сообщение пользователю Б. Для этого пользователь Б должен сообщить пользователю А свой открытый ключ. Далее, пользователь А при помощи полученного от пользователя Б открытого ключа шифрует сообщение. Зашифрованное сообщение пользователь А отправляется пользователю Б. Пользователь Б расшифровывает полученное сообщение своим закрытым ключом. Закрытый ключ всегда держится в секрете, поэтому никто кроме пользователя Б не сможет расшифровать адресованное ему зашифрованное сообщение. Для каждой задачи (как то: защищённая переписка по электронной почте, электронная цифровая подпись, защищённая переписка в сетях мгновенных сообщений вроде Jabber) настоятельно рекомендуется использовать отдельные ключи.

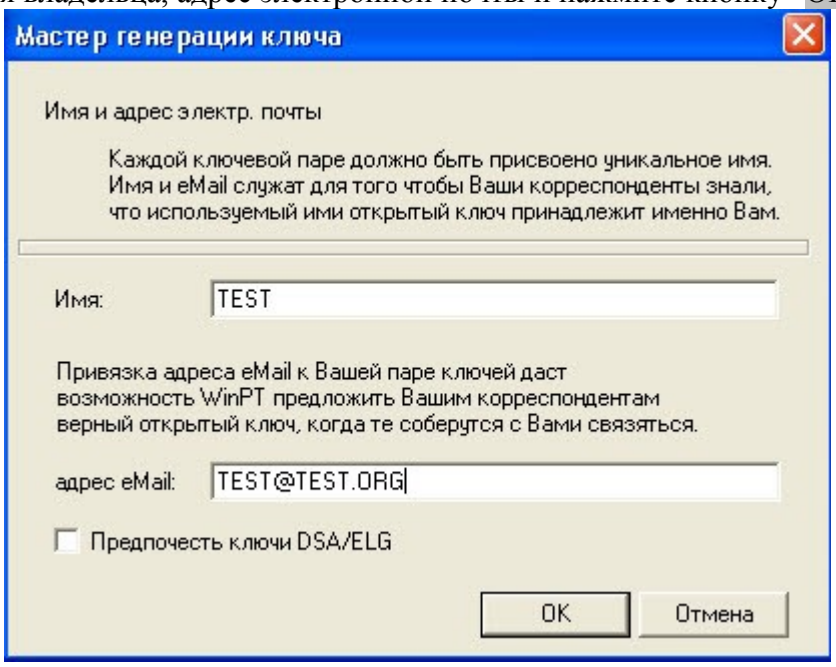
Для создания пары ключей щелкните правой клавишей мышки по иконке GnuPT на панели задач и выберите ***Менеджер ключей***.



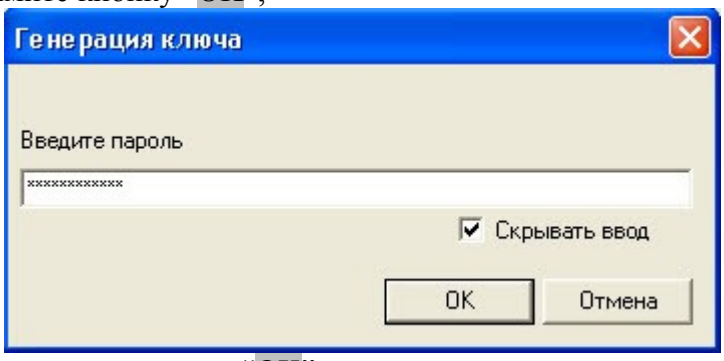
В новом окне пройдите путь ***Ключ -> Создать -> С помощью Мастера***.



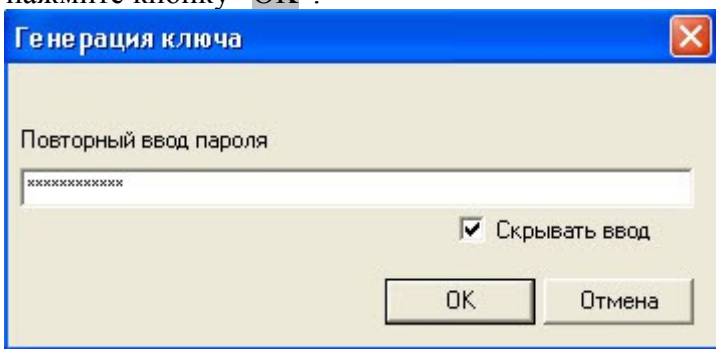
Введите свое имя владельца, адрес электронной почты и нажмите кнопку “OK”.



Введите пароль, нажмите кнопку “OK”,



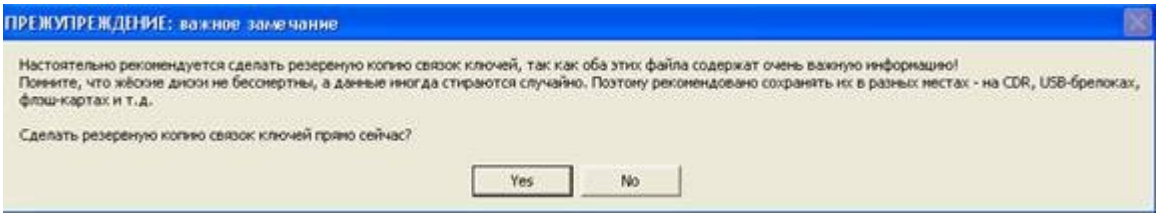
подтвердите пароль, нажмите кнопку “OK”.



Чем длиннее ваш пароль, тем он секретней. Попробуйте ввести по крайней мере 30 символов. Во вторых, нелишне отметить, что вы должны ввести пароль, который вы запомните наизусть. Не пишите его ни в какой файл, и не записывайте на бумаге! Вы будете его использовать каждый раз, когда соберетесь расшифровывать сообщение от своего партнера.

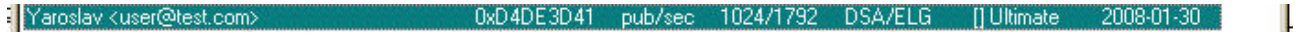
Поводите указателем мышки по экрану нового окна " Генерация ключа", пока не появится подтверждение " Генерация ключа завершена". Это рекомендуется для большей секретности генерируемого ключа. Нажмите кнопку “OK”.

В следующем окне нажмите кнопку “Yes” («Да») для сохранения копии базы данных своих ключей. Выберите, где вы хотите сохранить копию и имя файла (по умолчанию pubring_bak.gpg для открытых ключей) и нажмите кнопку “Save” («Сохранить») . После этого появится такое же окно с предложение сохранить личные ключи (secring_bak.gpg). Нажмите “Сохранить” еще раз. Сохраните на резервной флешке.



Копия пригодится вам в случае утери или порчи оригинала базы ключей.

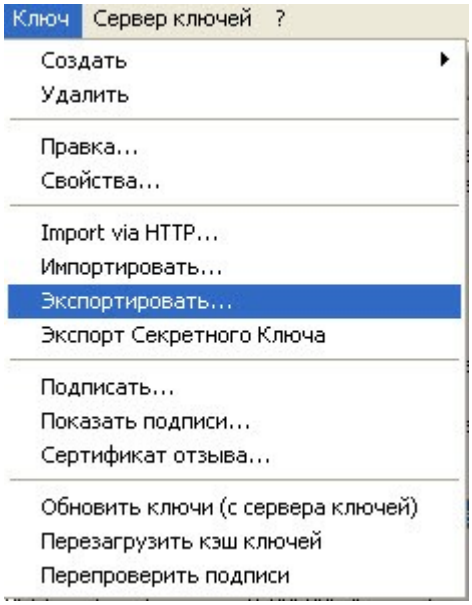
Если появится новое окно с предложением перезагрузить кэш ключей, нажмите кнопку «Yes» («Да»). Вы увидите свою новую пару ключей на экране Менеджера Ключей.



Обозначение типа **pub/sec** означает, что это именно пара открытого (public) и личного секретного (secret) ключей. При получении и импортирования открытого ключа от своего партнера, вы увидите только тип **pub** (public).

Экспорт открытого ключа

Теперь, после создания своей пары ключей, необходимо передать свой открытый ключ всем корреспондентам, с которыми предполагается вести защищённую переписку. Для этого надо экспортировать свой ключ в файл. Выделите свой ключ мышью и затем пройдите путь ***Ключ успешно сохранён*** в главном меню окна Менеджера Ключей.



В новом окне выберите место расположения файла и имя файла (по умолчанию в формате «<ИМЯ>.asc»). Нажмите кнопку «Сохранить». Появится подтверждение «*Ключ успешно сохранён»*... Нажмите кнопку «OK». Операция экспорта ключа выполнена и вы можете его передавать своим корреспондентам.
Еще, если нужно просто передать его в сообщении, можно выделить ключ в списке и нажать Ctrl+C.

Импорт открытого ключа

Перед использованием чужого открытого ключа, его сначала необходимо импортировать. Пройдите путь ***Ключ -> Импортировать***. В новом окне укажите папку где расположен файл для импорта и выделите присланный вам файл ключа, (он имеет расширение «.asc»), затем нажмите кнопку «Открыть» ("Open"). Должно появиться новое окошко " Импорт ключа". Нажмите клавишу "Import". Должно появиться новое окно " Статистика импорта ключей", где в случае удачного импорта значение поля " Кол-во открытых ключей" будет равно 1 и значение поля " Из них импортировано" также будет равно 1.

Для проверки, закройте окно Менеджера Ключей и откройте его снова – вы увидите что импорт ключа прошел успешно у вас появилась новая запись в окне Менеджера Ключей. Теперь импортированный ключ можно использовать для шифрования сообщений, предназначенных автору ключа.

После импорта ключа рекомендуем попросить своего партнера подтвердить так называемый отпечаток ключа «fingerprint». Пройдите путь ***Ключ -> Свойства*** и сличите fingerprint с тем, что вам сообщил ваш партнер. При совпадении fingerprint, вы можете изменить степень доверия к этому ключу. Если вы уверены, что это ключ, полученный от вашего партнера, то нажмите на кнопку “Изменить” и выберите «Доверяю безоговорочно» и нажмите кнопку “OK”. Нажмите кнопку “OK” дважды. Если вы не измените так называемый *Уровень доверия* после импорта ключа, вы будете получать предупреждающее сообщение каждый раз, когда

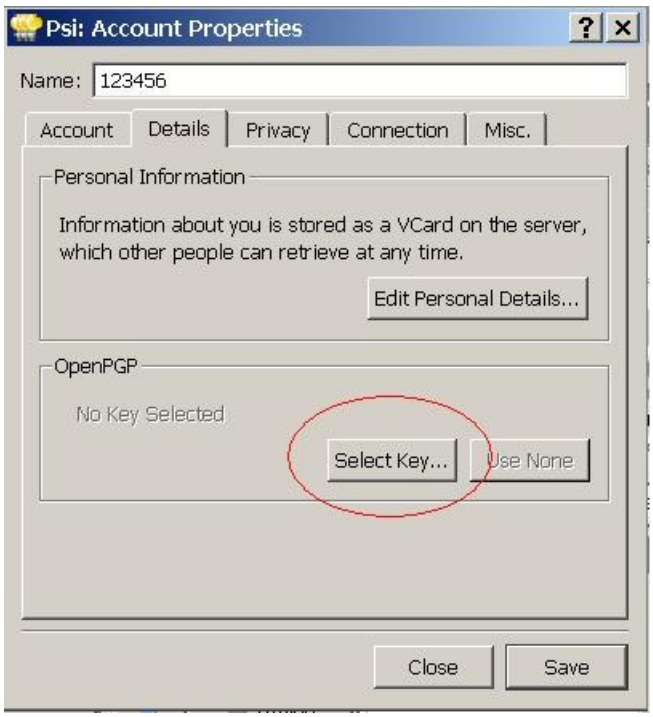
вы будете шифровать файл с помощью этого ключа. Также, если необходимо вставить ключ из буфера обмена, нажмите просто Ctrl+V и если вы корректно копировали в буфер обмена ключ то он импортируется в GnuPT.

Общение

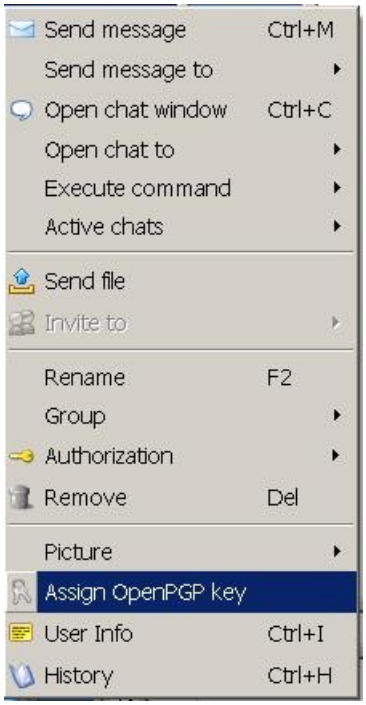
Теперь, для использования протокола шифрования для обмена сообщениями необходим IM клиент поддерживающий GnuPG. Я предпочитаю Jabber клиент Psi (http://psi-im.org/). Скачиваем, устанавливаем. На появившемся окошке:

Выбираем Register new account.
Там вводим сервер, нажимаем Next, на следующем окошке имя и пароль для логина. В дальнейшем ваш аккаунт будет выглядеть так имя@сервер. Далее — General → Account Setup

Там выбираешь ваш аккаунт. Нажимаем Modify. В открывшемся окне нажимаем Select Key.. И выбираем ваш ключ из списка. Потом, перезаходим в Psi.



Нажимаем правой кнопкой на того, с кем собираетесь общаться при помощи GnuPG. Выбираем Assign OpenPGP key.



В списке выбираем ключ собеседника. Нажимаем. Далее нажимаем дважды на ID корреспондента в списке Psi и в появившемся окошке справа от его Jabber ID должен быть замочек.

Если вы все настроили верно, и настроил все верно ваш собеседник, то после нажатия замочка вы сможете зашифрованно с ним/ней общаться.