МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
НАЦИОНАЛЬНАЯ МЕТАЛЛУРГИЧЕСКАЯ АКАДЕМИЯ УКРАИНЫ

Г.Г. ШВАЧИЧ, А.В. ОВСЯННИКОВ, В.В. КУЗЬМЕНКО,
А.В. ПАНАСЮК

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Раздел “Методы работы в программе PGP”

Утверждено на заседании Учёного совета академии
в качестве учебного пособия

Днепропетровск НМетАУ 2008

УДК 004 (075.8)
Основы защиты информации. Раздел “Методы работы в программе PGP”: Учеб. пособие / Г.Г. Швачич, А.В. Овсянников, В.В. Кузьменко, А.В. Панасюк. – Днепропетровск: НМетАУ, 2008. – 47 с.

Изложены основные методы работы в программе PGP.

Предназначено для студентов специальности 6.020100 – документоведение и информационная деятельность, а также для студентов всех специальностей и иностранных студентов.

Илл. 64. Библиогр.: 10 наим.

Издается в авторской редакции.

Ответственный за выпуск Г.Г. Швачич, канд. техн. наук, проф.

Рецензенты: Б.И. Мороз, д-р техн. наук, проф. (АТСУ)
Д.Г. Зеленцов, д-р. техн. наук, доц. (УГХТУ)

ТЕМА 1. СОЗДАНИЕ ПАРЫ КЛЮЧЕЙ

Для того чтобы начать работу с программой **PGP**, следует сначала сгенерировать пару ключей, выбрав в меню **Keys программы PGPkeys** пункт **«New Key»**. Это можно выполнить, используя «Помощник генерации ключей» (**PGP key Generation Wizard**).

Необходимо сделать следующее:

1. Нажать Пуск → Все программы → **PGP** → **PGPkeys**

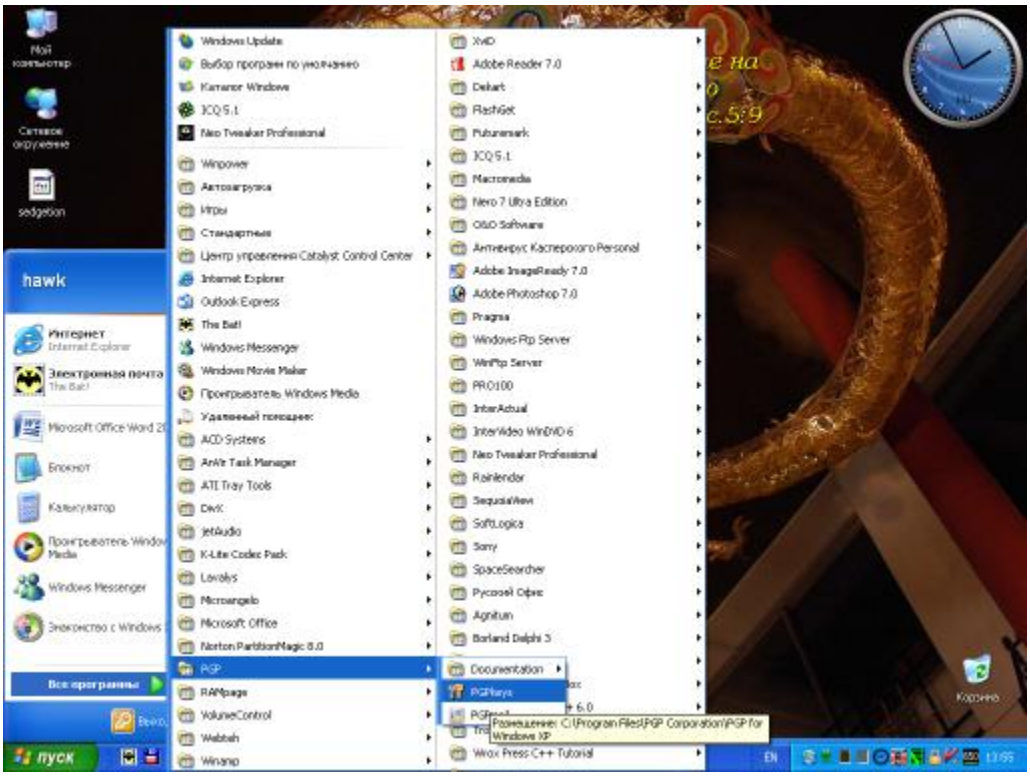

Рис. 1.1. Генерация пары ключей

2. Откроется окно вид, которого показан на рис. 1.2. Если впервые открываете программу **PGPkeys**, то окно **PGPkeys** будет пустым, если на компьютере уже есть какие-либо сгенерированные и подсоединенные пары ключей, то они отобразятся в окне программы.

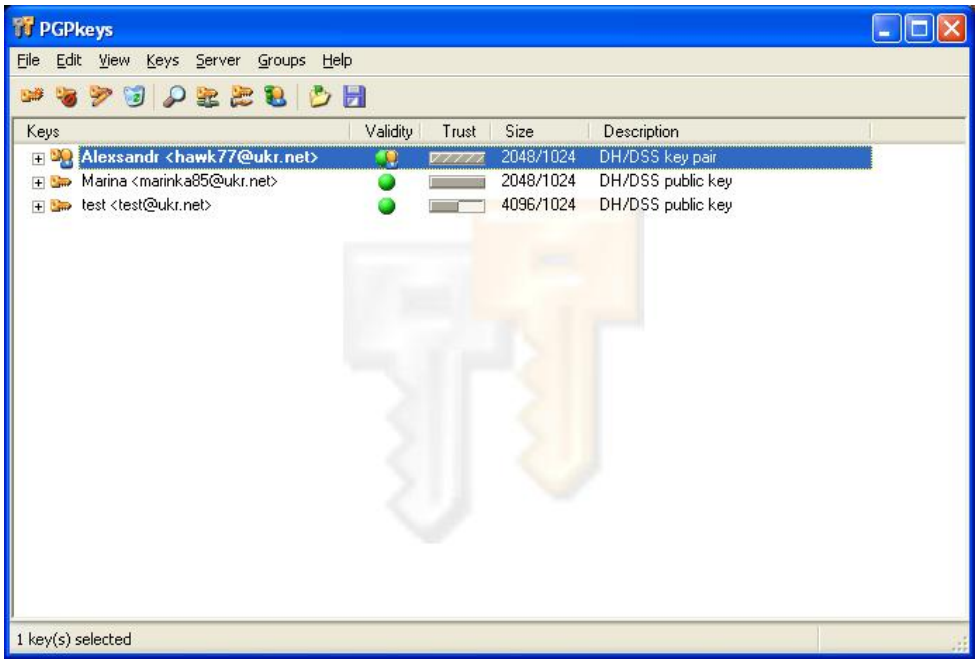

Рис. 1.2. Подсоединение пары ключей

3. Создаем новую пару ключей. Нажимаем **New Key** из меню **Keys**.

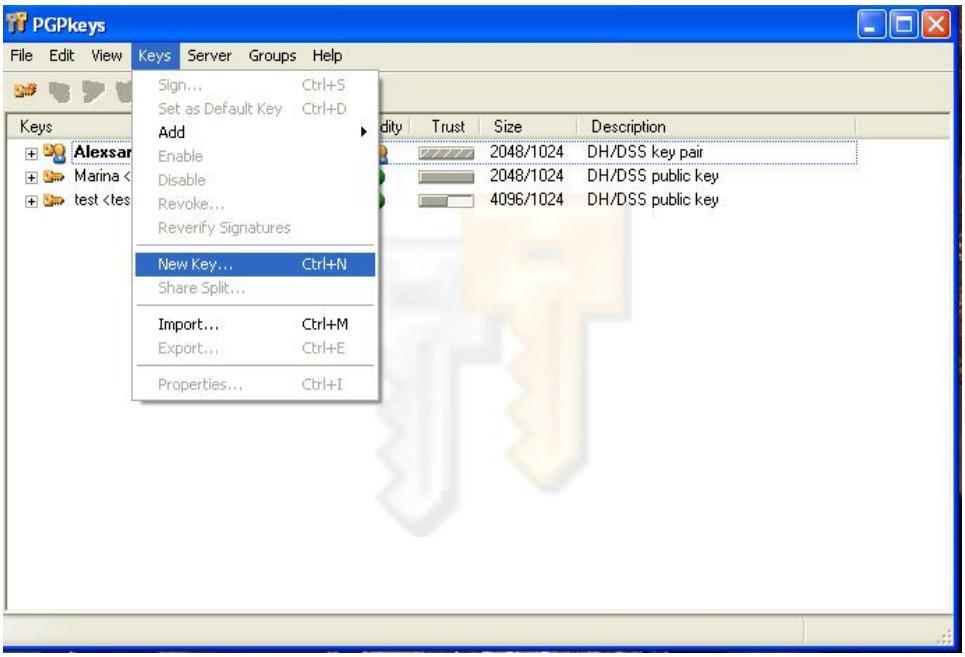

Рис. 1.3. Создание новой пары ключей. Шаг 1

4. Откроется окно **PGP key Generation Wizard**. В этом окне нажимаем кнопку **Expert.**

Рис. 1.4. Создание новой пары ключей. Шаг 2

5. В открывшемся окне вводим следующие данные в соответствующие поля.

Full Name: (Полное имя) Тут вводите свое имя (в данном примере имя «Test»)

Email address: Test@ukr.net

Key type: (Diffie-Helman/DSS, RSA, RSA Legacy). Здесь необходимо выбрать тип ключей, в нашем примере выбираем Diffie-Helman/DSS. Ключи Diffie-Helman/DSS могут сделать невозможной коммуникацию с пользователями более ранних версий программы PGP. Diffie-Helman/DSS – это новый тип ключей, являющихся по крайней мере столь же надежным, что и ключи RSA той же длины. Ключи Diffie-Helman/DSS не поддерживаются ранними версиями PGP, это означает невозможность обмена зашифрованными данными с пользователями, которые еще не перешли на версию 5.0 или выше программы **PGP.** Использование ключей **Diffie-Helman/DSS** во много раз сокращает время для шифрования и дешифрования данных.

Key Size: (размер ключа) Выбираем размер ключа от 1024 до 4096.

При работе с **Key Expiration,** выбираем **«Never»** и указываем дату, до которой будет действовать данная пара ключей.

После всех заполнений наше окно должно выглядеть так:

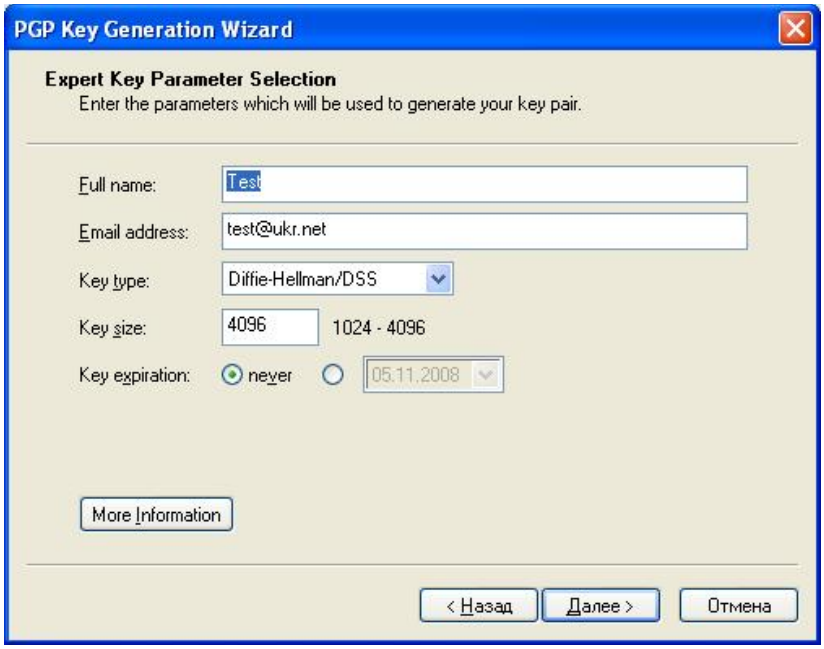

Рис. 1.5. Вид окна после заполнения всех записей о ключах

6. Нажимаем кнопку «Далее» и переходим в окно **«Passphrase Assignment».** В поле ввода «пароль» (**passphrase**) введите последовательность символов или слов, которую будете использовать для исключительного доступа к своему закрытому ключу. Для подтверждения пароля перейдите в поле **«Confirmation»** и повторите пароль. Обычно, для безопасности на экране не отображаются вводимые символы, но если уверенны, что за Вами никто не наблюдает и хотите видеть вводимые символы, то снимите «флаг» в поле **«Hide Typing».** В нашем примере используем пароль test_test.

Совет: Пароль должен содержать несколько слов, и может включать пробелы, цифры и другие печатные символы. Придумайте что-нибудь, что легко запомнить, а другим – непросто отгадать и помните, что в пароле строчные и заглавные буквы различаются. Чем длиннее пароль и чем шире набор символов, которые он содержит, тем он более надежен. Попытайтесь

включить равное количество строчных и заглавных букв, цифр, знаков препинания и т.п.

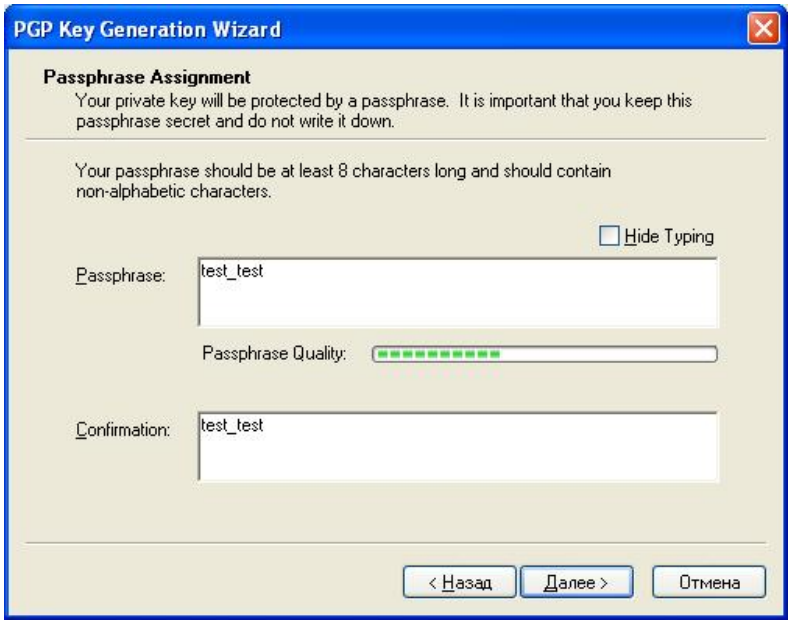

Рис. 1.6. Окно с паролем

7. Щелкните «Далее» для запуска процесса генерации ключей.
8. Когда процесс закончится, то мы увидим окно:

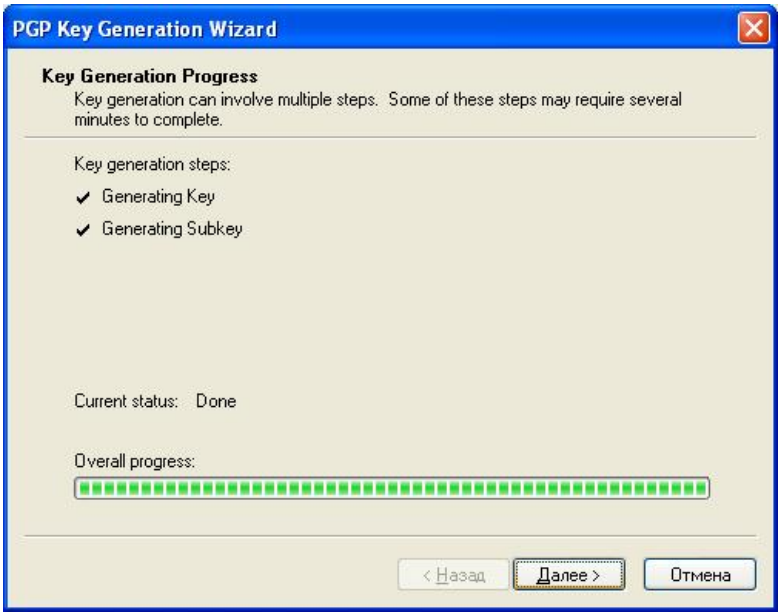

Рис. 1.7. Завершение создания пары ключей

Ключ и подключи сгенерированы. Нажимаем «Далее» и затем «Готово».

В окне PGPkeys появится новая связка ключей, которая будет называться Test<test@ukr.net>.

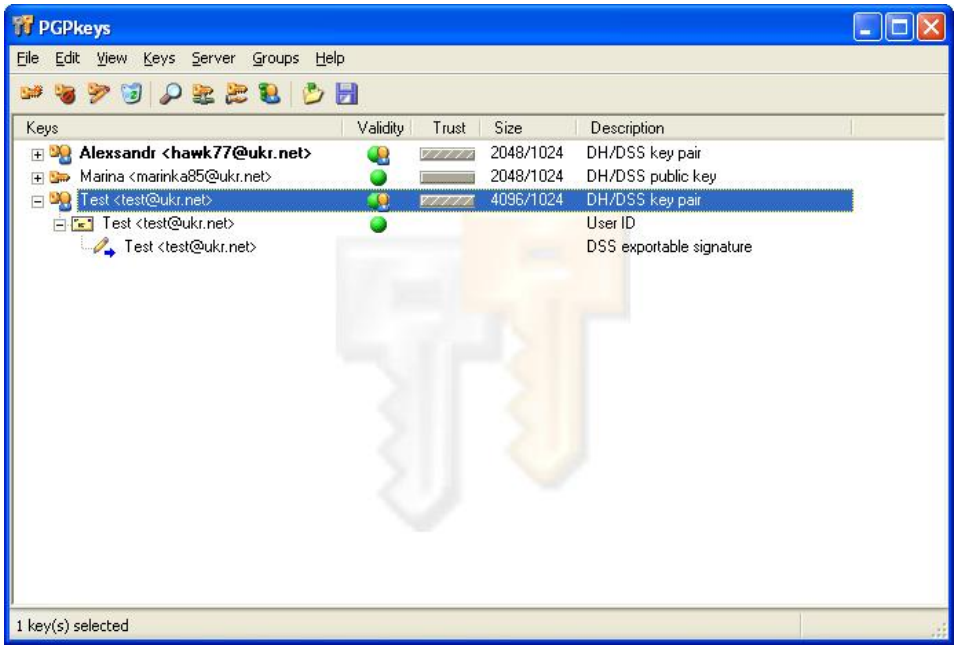

Рис. 1.8. Появление новой связки ключей

Значок, с парой ключей, появившийся в окне PGPkeys, символизирует новую пару ключей. В RSA – ключи представлены серым цветом, а DSS/DH – оранжевым. В окне представленном выше показаны все ключи с шифром DSS/DH.

ТЕМА 2. ОБМЕН КЛЮЧАМИ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ. ЭКСПОРТ ПАРЫ КЛЮЧЕЙ

После генерации пары ключей можем начать защищенную переписку с другими пользователями PGP. Для этого нам необходимы копии их открытых ключей, а им – копия нашего открытого ключа. Так как открытый ключ может быть представлен в виде фрагмента текста, обменяться ключами совсем просто. Мы можем вставить этот фрагмент текста в сооб-

щение электронной почты, передать в виде файла, или поместить на сервер открытых ключей в сети Internet.

Для того, чтобы послать, или передать свой открытый ключ своему абоненту необходимо сделать следующее:

1. Открыть программу PGPkeys (Пуск → Все программы → PGP → PGPkeys).

Рис. 2.1. Передача ключа абоненту

2. Выделить нужный нам ключ и в меню **Keys** выбрать подменю **Export**.

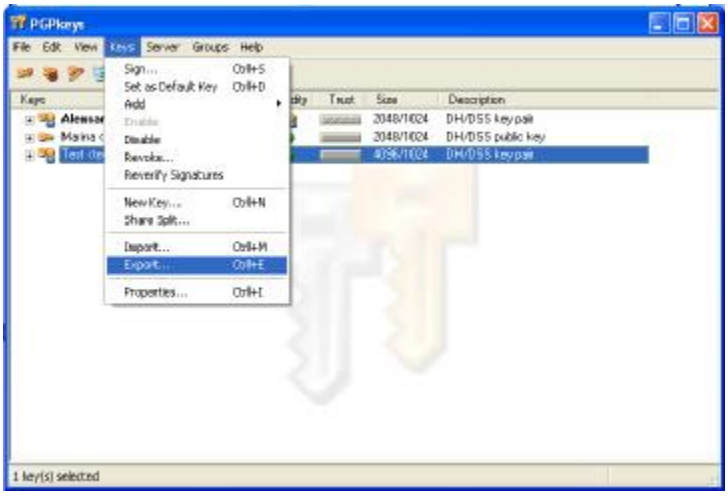

Рис.2.2 Выделение необходимого для передачи ключа

3. В открывшемся окне указываем имя файла и путь его сохранения. Ставим флажок возле надписи Include 6.0 Extensions и нажимаем «Сохранить».

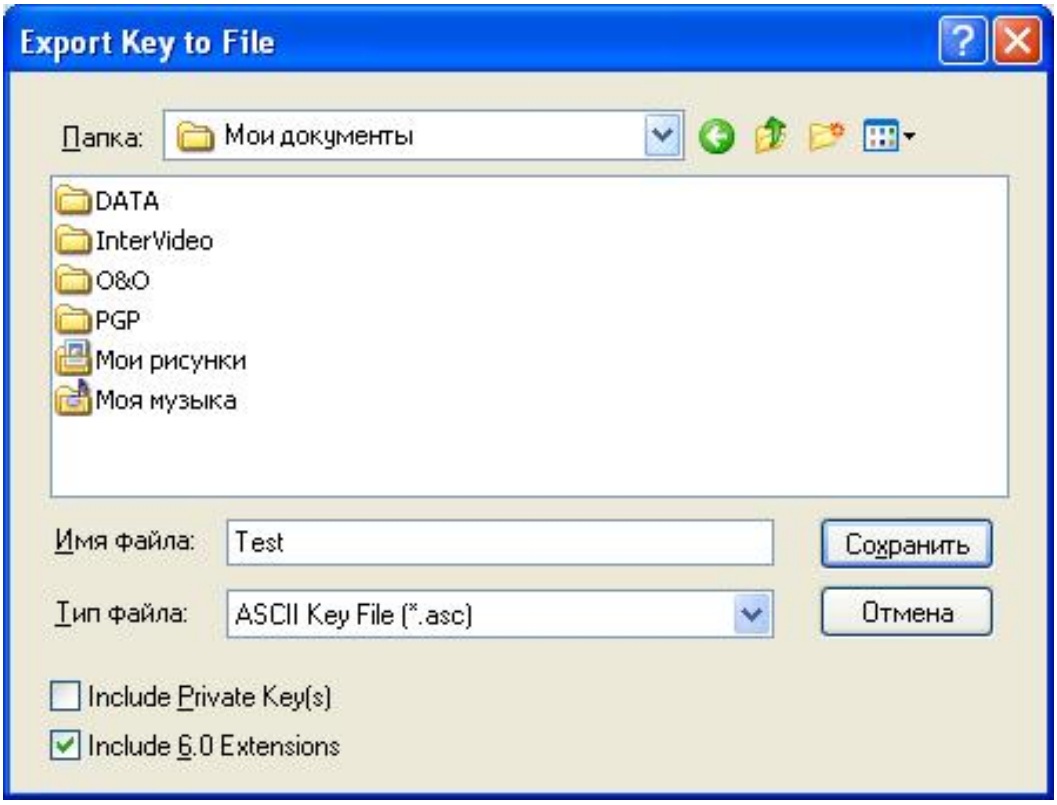

Рис. 2.3. Сохранение файла

4. Если открыть сохранённый файл с помощью программы «блокнот», то увидим файл, сохраненный с расширением *.asc – открытый ключ (рис. 2.4.).

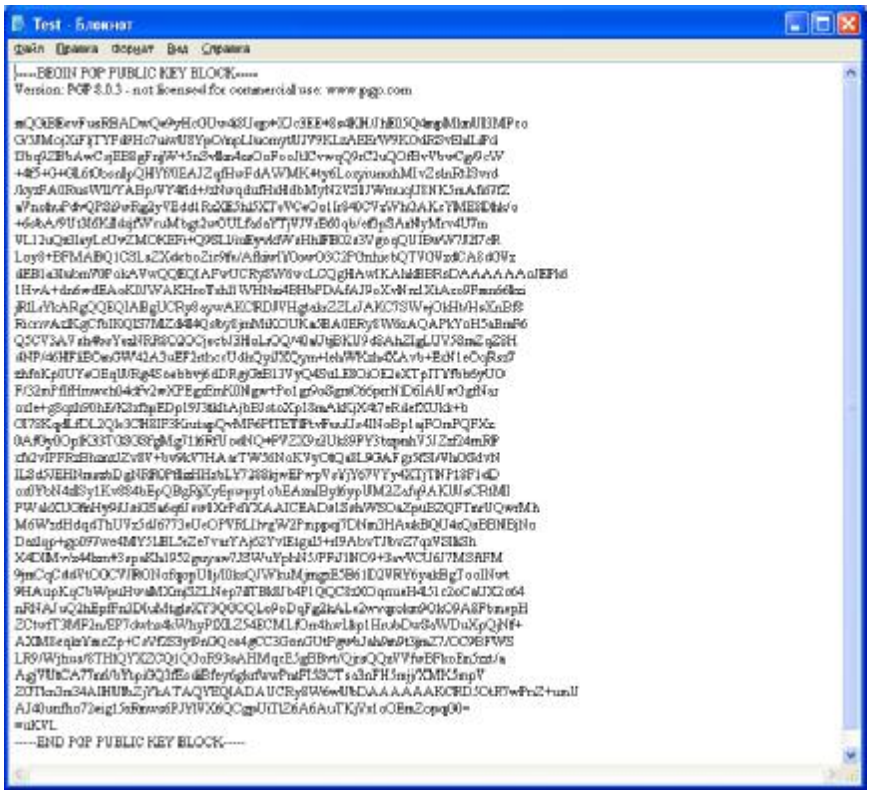

Рис. 2.4. Файл, сохраненный с расширением *.asc – открытый ключ

5. Теперь необходимо файл с расширение *.asc передать тому с кем мы хотим переписываться шифрованным текстом. Это можно сделать с помощью внешнего носителя.

Когда абонент получит файл с открытым ключом, в нашем случае test .asc, то ему всего лишь необходимо «кликнуть» на этом файле 2 раза, чтобы добавить его к своей базе ключей.

ТЕМА 3. ОБМЕН КЛЮЧАМИ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ

Импорт чужого ключа

Когда получаем чей-то открытый ключ (в данном примере используется открытый ключ Test2) в файле с расширением *.asc, то, чтобы воспользоваться ключом необходимо «кликнуть» на полученном файле дважды. Откроется окно (рис. 3.1.)

Рис. 3.1. Использование чужого ключа

В окне (рис. 3.1.), будет отображаться открытый ключ, который необходимо «привязать» на собственные пары ключей. В новом открывшемся окне можем просмотреть подлинность полученного ключа, через его отпечаток (fingerprint). Об отпечатке и подписи ключей будет сказано в следующих лабораторных работах. Становится возможным посмотреть тип ключа, его **ID**, размер, дату создания, срок действия, шифр. Для этого необходимо выделить ключ и «нажать» на нем правой клавишей мыши, высветится надпись «**Key properties**». При «клике» по ней, откроется окно (рис. 3.2.).

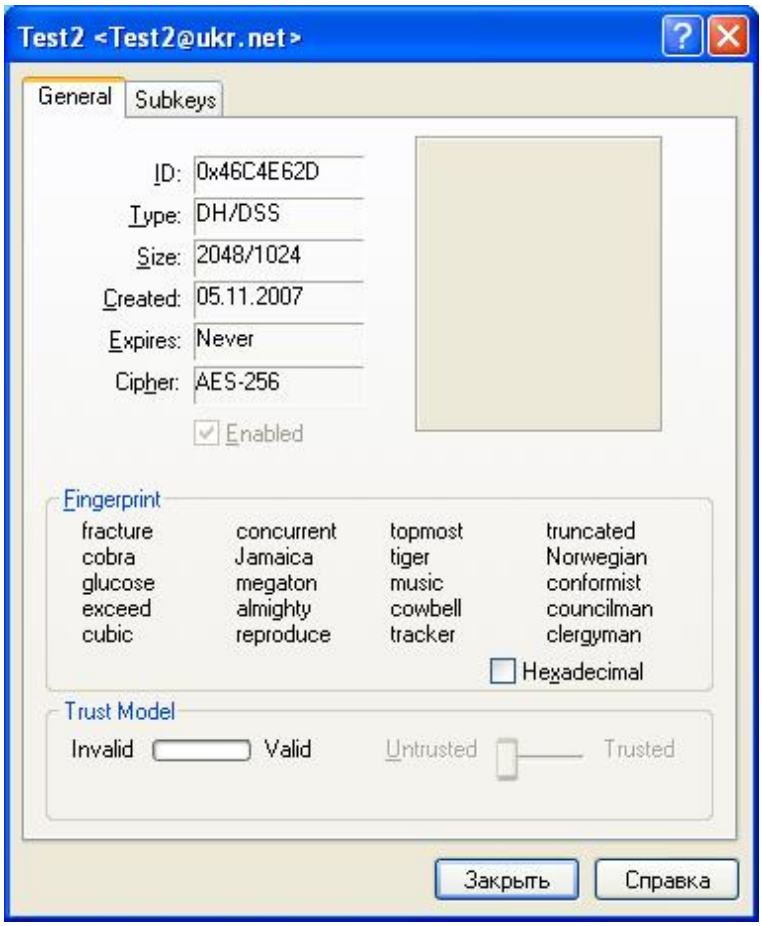

Рис. 3.2. «Привязка» ключа к собственным парам ключей

В заголовке «**Fingerprint**» предварительно поставив «галочку» возле надписи «**Hexadecimal**» можно будет увидеть «**отпечаток**» данного ключа (рис. 3.3.), как в текстовом варианте, так и в шестнадцатеричной системе исчисления. Данный «отпечаток» можно сравнить с отпечатком, который предварительно отослал автор данного открытого ключа и удостовериться в его подлинности.

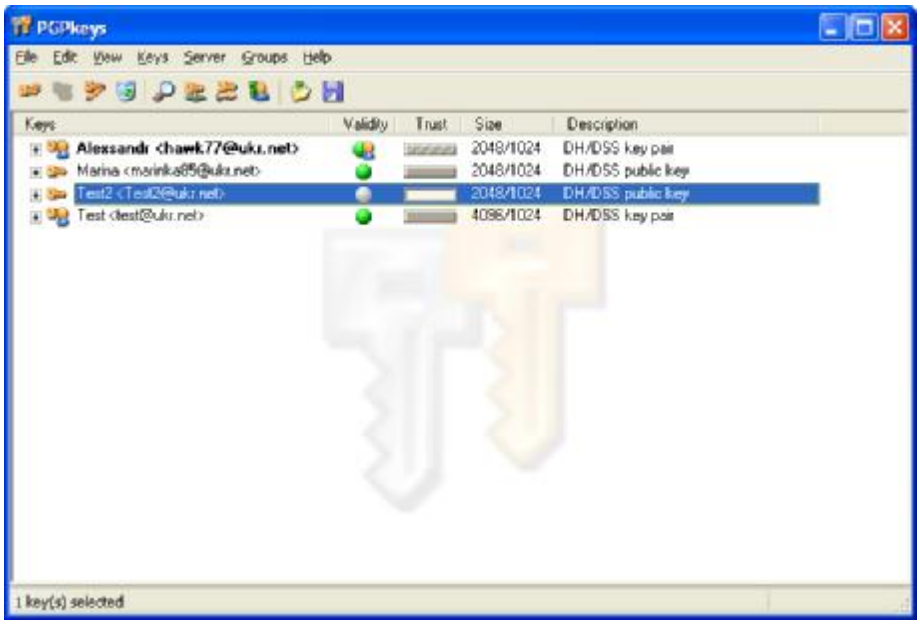

Рис. 3.3. «Отпечаток» ключа в текстовом варианте и в шестнадцатеричной системе исчисления

После ознакомления со свойствами ключа, необходимо нажать на кнопку «**закрыть**» и возвратиться к предыдущему окну, после чего нажать кнопку «**Import**». В программе **PGPkeys** увидим, что добавился новый ключ **Test2<test2@ukr.net>**

Теперь необходимо подписать данный ключ, чтобы дать **PGP** знать, что считаем безопасным использование данного ключа. Для этого, «кликнем» по серому «шарику» напротив ключа в столбце **«Validity»** и открывается окно (рис. 3.4.)

Рис. 3.4. «Подпись» ключа, чтобы сделать его безопасным

Ставим «флаг» напротив «**Allow signature to be exported. Others may rely upon your signature**». Это позволит идентифицировать подпись экспорта. Другие могут доверить подписи эксперта. Далее нажимаем «**Ок**». Чтобы подпись вступила в силу необходимо ввести пароль связки ключей, пользователя данного компьютера. Обычно пиктограмма пользователя отображается в окне программы **PGPkeys** жирным черным цветом.

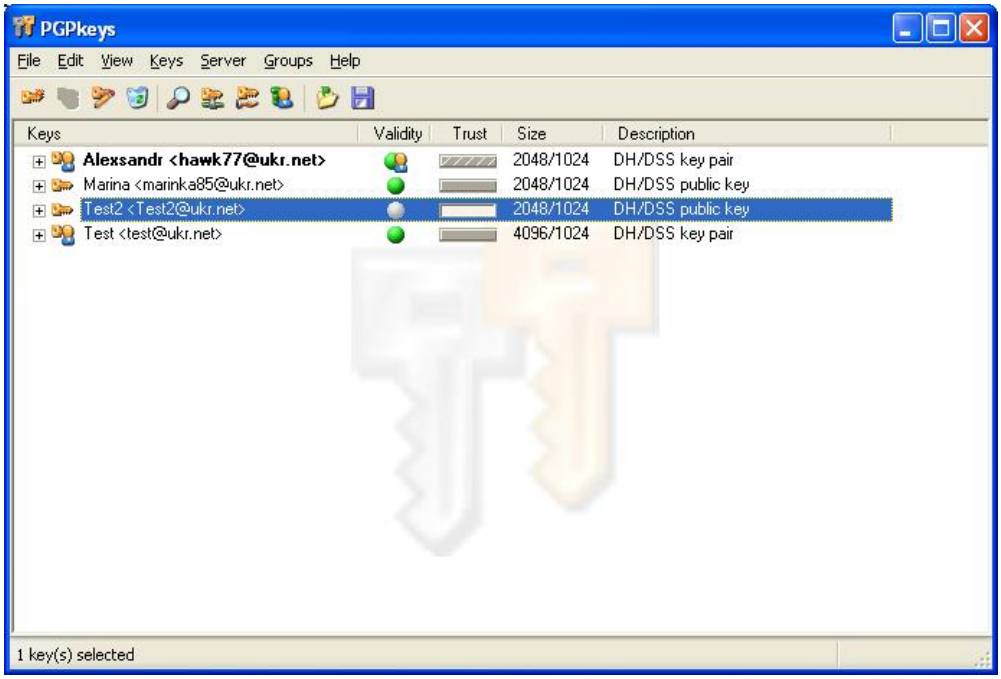

Рис. 3.5. Идентификация подписи эксперта

В нашем случае это будет пароль связки ключей, которая была создана на Вашем компьютере. Если на компьютере создавали более чем одну связку ключей, то необходимо установить какую-либо из этих связок по умолчанию. В противном случае программа **PGPkeys** не пропустит дальше, пока этого не сделаете. Чтоб указать связку ключей по умолчанию необходимо выделить нужную связку, в меню **Keys** нажать **Set as Default Key.** Если на компьютере была создана всего лишь одна связка ключей, то она автоматически устанавливается, как связка по умолчанию. После введения пароля в окне **PGPkeys** ключ Test2 будет выглядеть, так как показано на рис. 3.6.

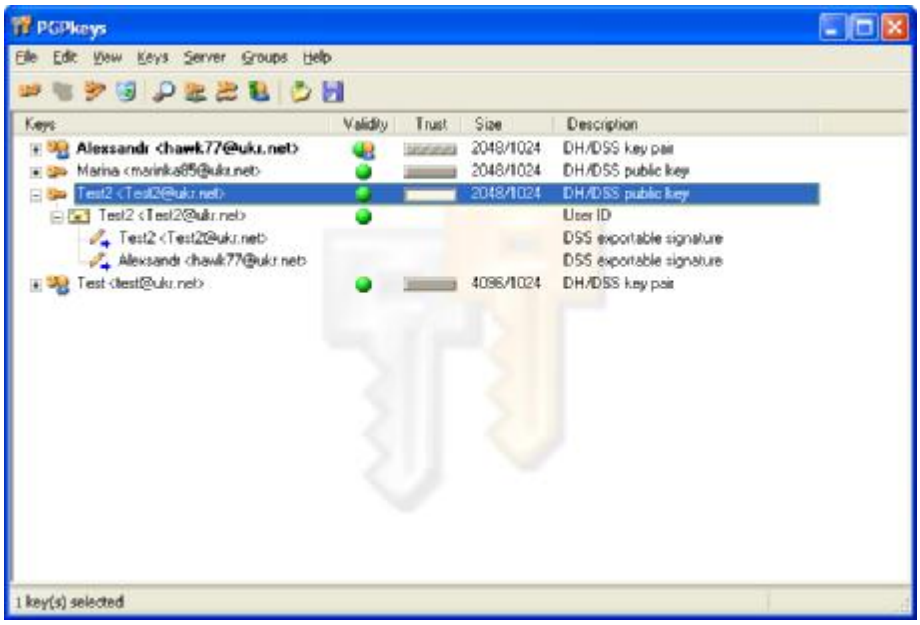

Рис. 3.6. Установка связки ключей по умолчанию

В данном окне видно, что ключ Test2 подписан Alexsandr<hawk77@ukr.net>. Это означает подлинность подписи перед третьими лицами. Как видно в столбце Trust прямоугольник напротив ключа Test2 пуст. Это значит, что PGP не «доверяет» этому ключу. Процедуру доверия можно инициализировать следующим образом. Зайти меню Keys – Properties откроется окно (рис. 3.7.)

Рис. 3.7. Инициализация процедуры доверия

В разделе **Trust Model** «ползунком» установите степень доверия (**Untrusted-Middle-Trusted**), которую определяете данному ключу. Если у ключа степень доверия будет ниже среднего, то при подписи какой-либо шифрограммы этим ключом, **PGP** будет появляться напоминание о том, что степень доверия у данного ключа не полная. После выбора степени доверия прямоугольник напротив ключа Test2 становится заполненным, а не пустым.

Тема 4. Проверка подлинности ключа. Сертификация чужого ключа. Указание уровня доверия

Отпечаток (fingerprint) – уникальный идентификационный номер, генерируемый при создании пары, и являющийся основным средством контроля подлинности ключа. Хорошим способом проверки отпечатка является его диктовка владельцем по телефону для последующего сравнения с отпечатком имеющейся копии.

Часто трудно быть уверенным, что ключ принадлежит определенному лицу, если не получили этот ключ лично от абонента на съёмном носителе или по электронной почте. Такой способ обмена ключами не всегда практичен (кроме электронной почты), особенно для пользователей, живущих на расстоянии многих километров друг от друга.

Для проверки отпечатка ключа существуют разные способы. Наиболее надежно – позвонить владельцу и попросить его прочитать отпечаток по телефону. Вы также можете попросить вашего собеседника, чтоб он прислал свой отпечаток по E-mail или другим для него доступным способом.

Как узнать отпечаток ключа

1. Выделите ключ в окне программы PGPkeys, отпечаток которого хотите проверить.
2. Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Key Properties**.

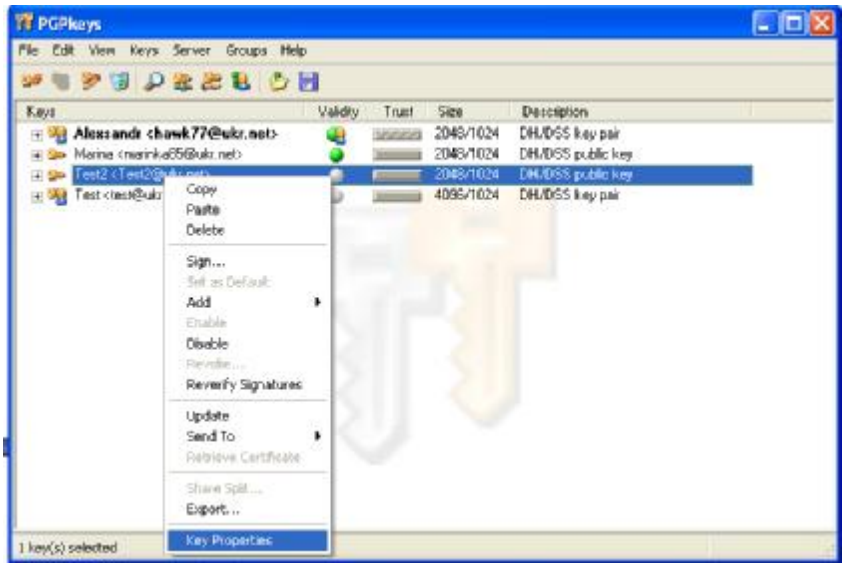

Рис. 4.1. Распознавание подлинности ключа

3. В открывшемся окне (рис.21) посмотрите на отпечаток **(fingerprint)** и сравните его с оригиналом. Отпечаток может быть представлен, как в шестнадцатеричной системе исчисления, так и в текстовом варианте.

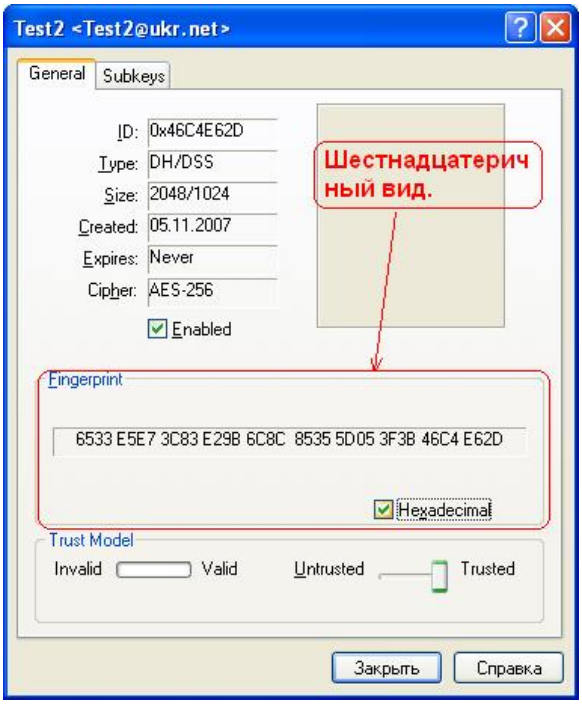

Рис. 4.2. Отпечаток ключа представленный в шестнадцатеричной системе исчисления

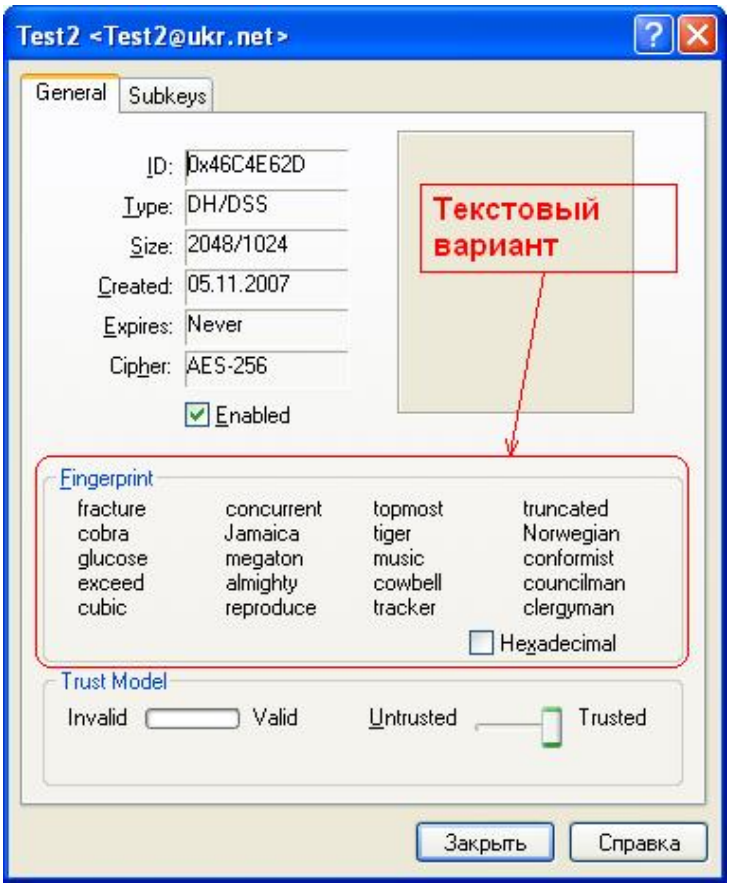

Рис. 4.3. Отпечаток ключа представленный в текстовом варианте

Сертификация чужого открытого ключа

Когда генерируете пару ключей, она автоматически подписывается с помощью закрытого ключа. После того как убедились, что открытый ключ принадлежит его истинному владельцу, можете подписать этот ключ (сертифицировать), тем самым, показывая, что уверены в этом ключе.

Как подписать чужой открытый ключ

1. Выделите в окне программы PGPkeys интересующий ключ. В нашем примере рассмотрим ключ **Test2**.
2. Выберите из меню **Keys** или из контекстного меню при щелчке правой кнопкой мыши по ключику пункт **Sign**. Появится окно предупреждения (рис. 4.4.)

Рис. 4.4. Подпись чужого ключа

Подписывая ключ пользователя, Вы ручаетесь за его подлинность. Перед тем как его подписать убедитесь, что ключ достался вам из надежного источника, то есть от его обладателя.

В данном окне поставьте галочку возле надписи «Allow signature to be exported. Others may rely upon your signature».

3. Нажмите Ok. Появится диалоговое окно, где предлагается ввести пароль.

Рис. 4.5. Окно введения пароля

Ввод пароля

В данном случае вводится пароль не ключа Test2<test2@ukr.net>, а пароль пользователя, которым необходимо подписать данный ключ. В нашем случае это ключ Alexsandr<hawk77@ukr.net>.

Если есть другая пара ключей, и хотите подписать ключ с ее помощью, то следует «нажать на стрелку» и выбрать нужный ключ.

Рис. 4.6. Ввод пароля

4. После того, как ключ был сертифицирован, в списке сопровождающих его подписей появится строчка со значком карандаша и вашим именем.

Рис. 4.7. Сертифицированный ключ

Указание уровня доверия

Кроме сертификации принадлежности ключа владельцу, можете присвоить его владельцу определенный уровень доверия. Это значит, что если когда-либо получите от кого-то ключ, подписанный лицом, которого обозначили как заслуживающего доверия, ключ может рассматриваться как действительный, даже если не проверяли его подлинность сами.

Присвоение ключу уровень доверия

1. Выделите ключ в окне программы PGPkeys уровень доверия к владельцу которого вы хотите изменить.
2. Выберите из меню **Keys** или из контекстного меню выделенного ключа пункт **Key Properties.** Появится диалоговое окно свойств ключа. В нашем примере ключ Test2.

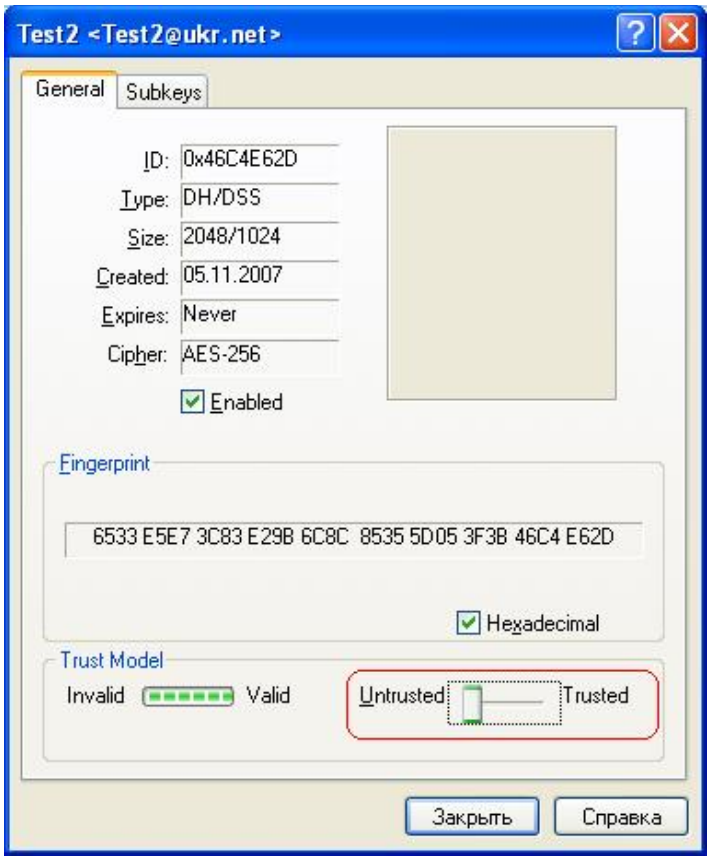

Рис. 4.8. Присвоение ключу уровня доверия

3. Для установки соответствующего уровня доверия, используем движок уровня доверия под меню **Trust Model**. Выбираем между уровнями «надежный» (Trusted), средней надежности (Middle), «ненадежный» (Untrusted). Для завершения операции нажимаем **Ok.**

От степени надежности, установленной каждому ключу, прямоугольники возле каждого из них будут выглядеть так, как показано на рис. 4.9.

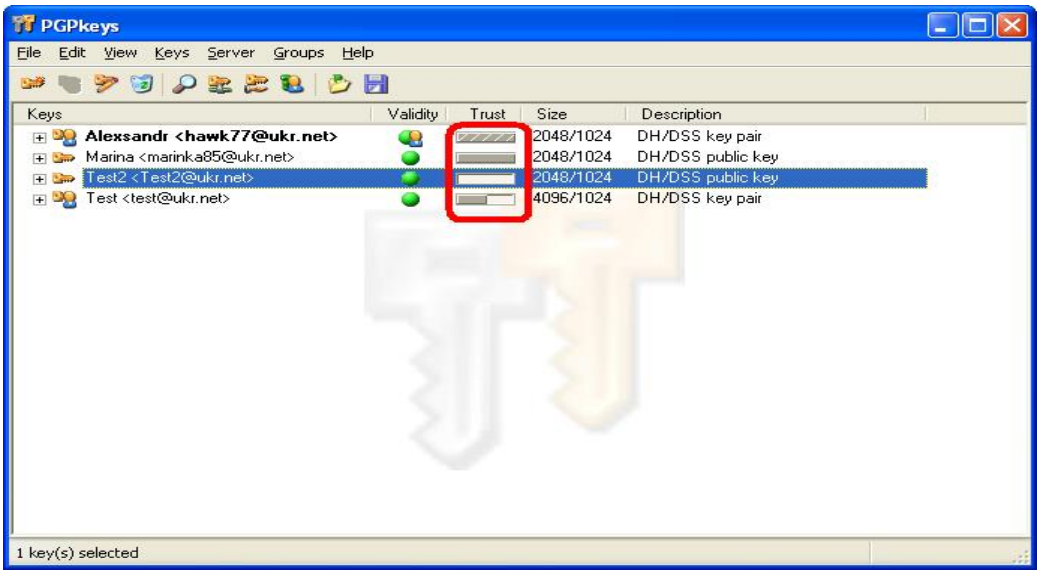

Рис. 4.9. Установка степени надёжности ключа

ТЕМА 5. ЗАПРЕТ И РАЗРЕШЕНИЕ ИСПОЛЬЗОВАНИЯ КЛЮЧЕЙ. УДАЛЕНИЕ КЛЮЧА, ПОДПИСИ ИЛИ ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ. ИЗМЕНЕНИЕ ПАРОЛЯ ДОСТУПА. ОТЗЫВ КЛЮЧА

Запрет и разрешение использования ключей

Иногда может возникнуть ситуация, когда необходимо временно запретить использование ключа. Эта возможность полезна, когда хотите сохранить ключ для использования в будущем, но не хотите, чтобы лишние ключи загромождали окно «Диалога выбора получателя» каждый раз, когда шифруете сообщение перед отправкой его по электронной почте.

Запрет на использование ключа

1. Выделите ключ в окне программы PGPkeys, который хотите запретить.
2. Выберите из меню **Keys** или из контекстного меню пункт **Disable.**

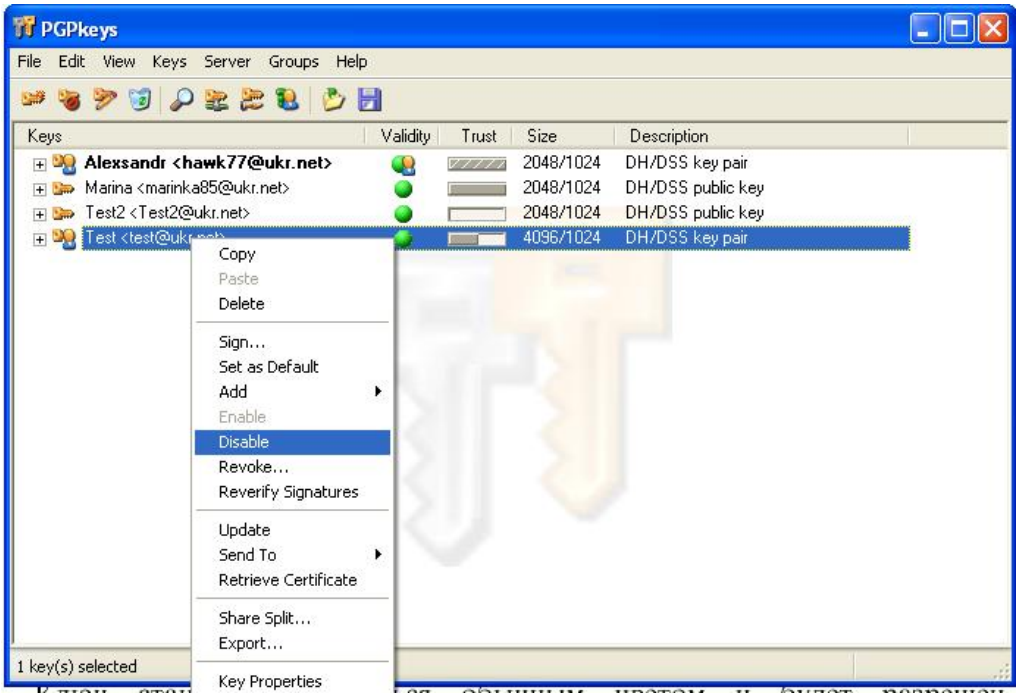

Рис. 5.1. Запрет использования ключа

3. Ключ станет прозрачным и будет временно запрещен к использованию (рис. 5.2.).

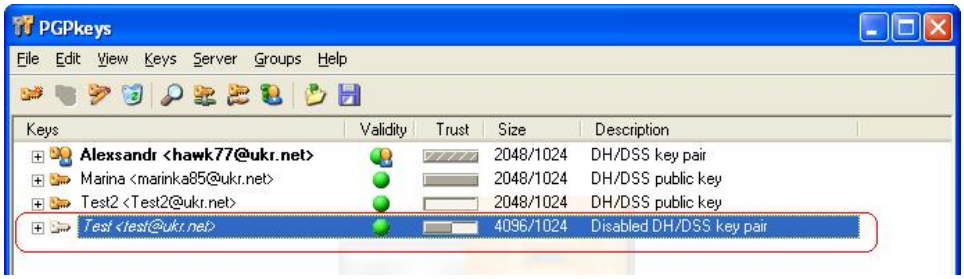

Рис. 5.2.

4. Для разрешения использования воспользуйтесь тем же алгоритмом действий, только вместо пункта **Disable** нажмите **Enabled**. Ключ будет отображаться обычным цветом и будет разрешен к использованию.

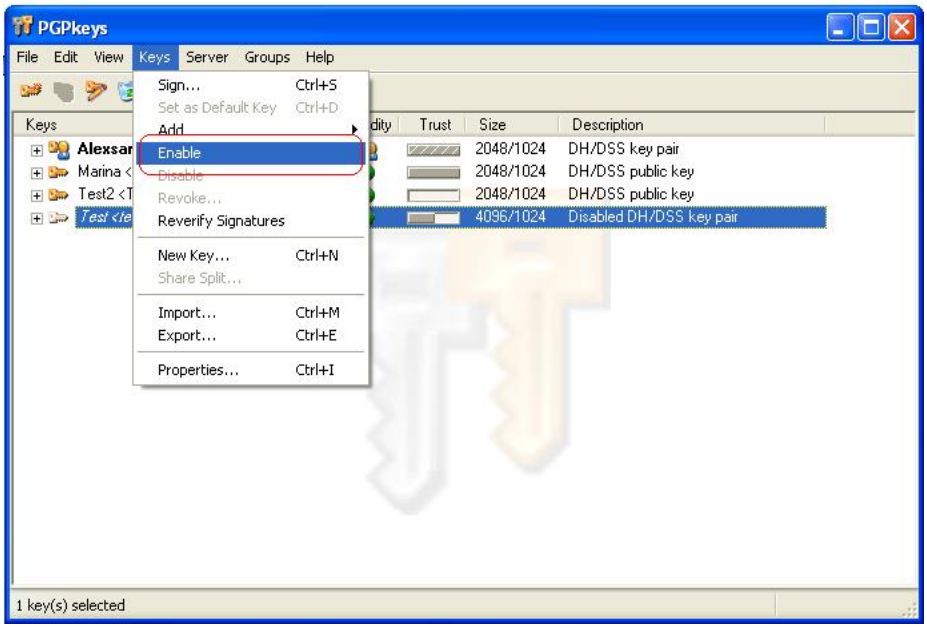

Рис. 5.3. Разрешение использования ключа

Удаление ключа, подписи или идентификатора пользователя

1. Выделите ключ в окне программы PGPkeys, который хотите запретить.
2. Выберите из меню Edit или из контекстного меню выбранного ключа пункт Delete.

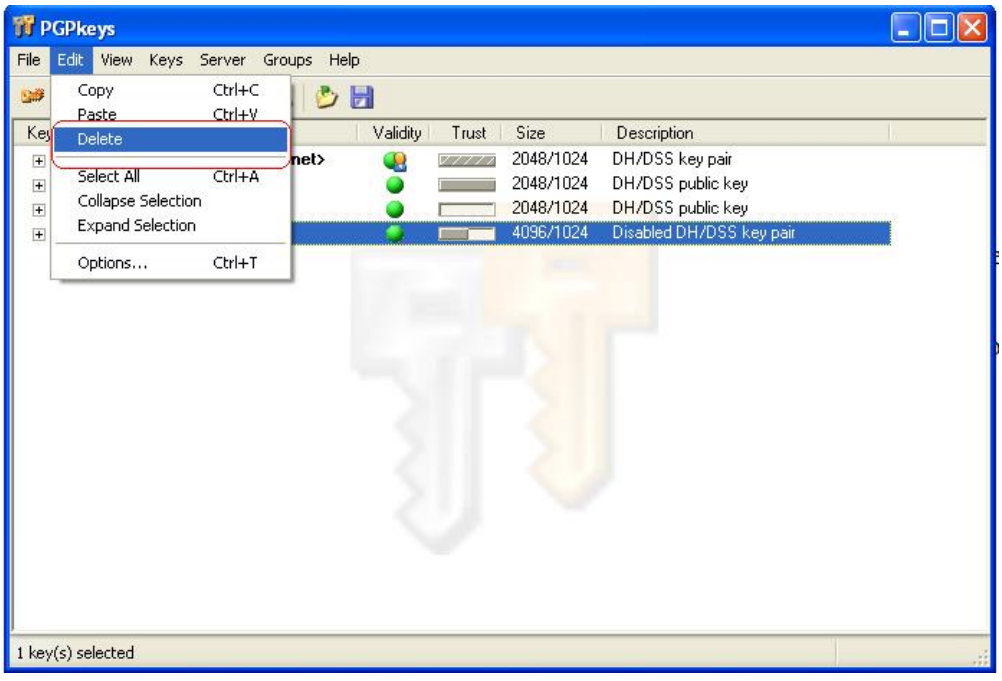

Рис. 5.4. Удаление ключа, подписи или идентификатора пользователя

Изменение пароля доступа

1. Выделите требуемую пару ключей в окне программы PGPkeys к которой хотите изменить пароль доступа. В нашем примере используем пару ключей Test<test@ukr.net>.
2. Выберите из меню **Keys** или из контекстного меню пункт Key **Properties**. Появится окно свойств выделенного ключа(Test).

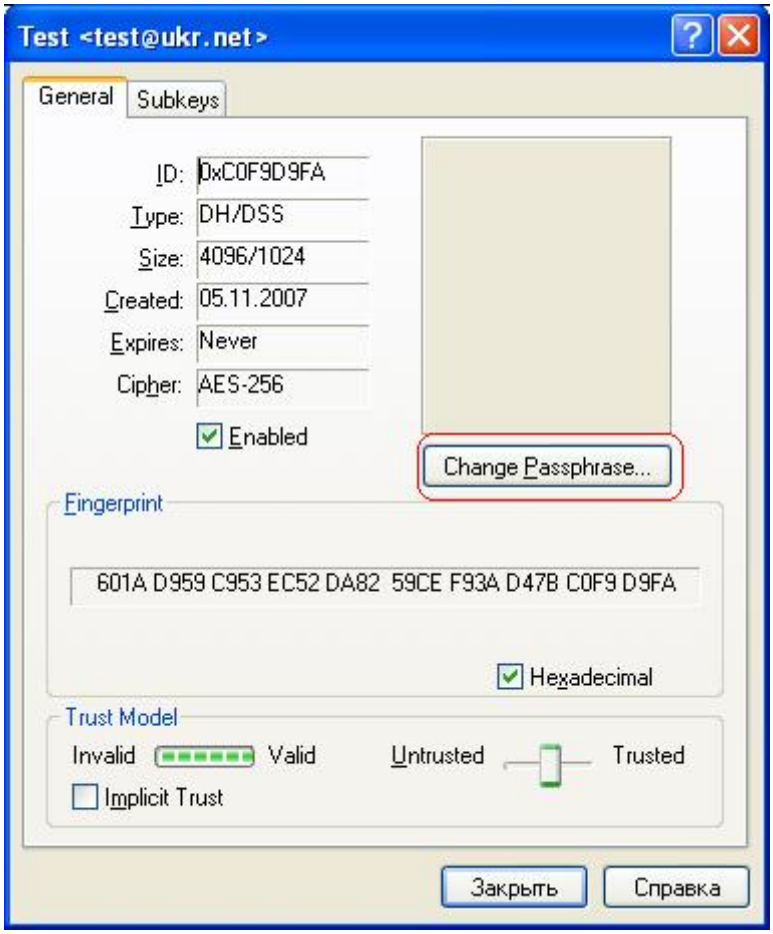

Рис. 5.5. Изменение пароля доступа

3. Щелкните на кнопке «Change Passphrase…». Появится диалоговое окно, где будет предложено ввести текущий пароль данного ключа для того, чтоб перейти в диалоговое окно смены пароля. После введения текущего пароля откроется диалоговое окно смены пароля.

Рис. 5.6. Диалоговое окно ввода текущего пароля

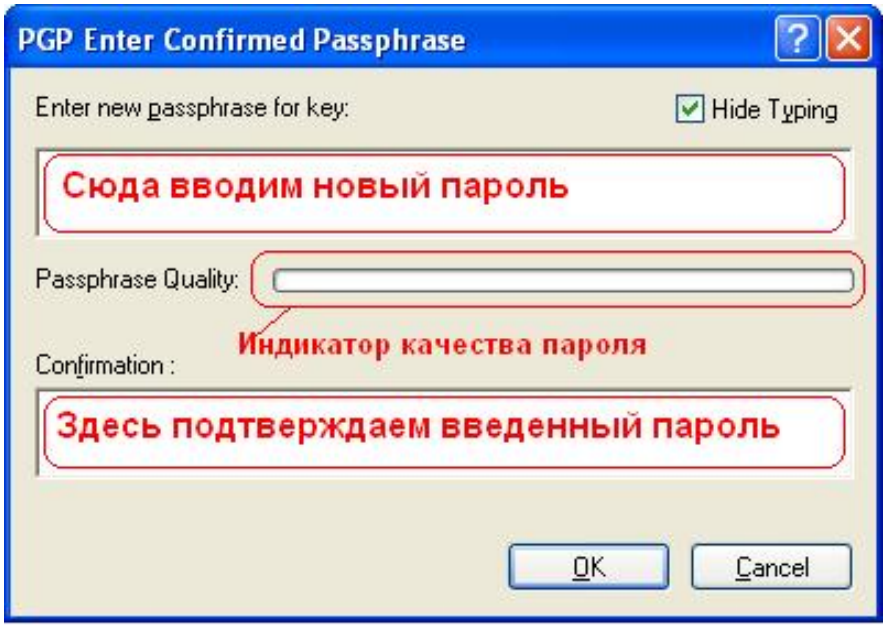

Рис. 5.7. Окно ввода нового пароля

4. После введения нового пароля нажимаем **Ok** и получаем следующее окно. В котором, говорится, что пароль был изменен (рис. 5.8.).

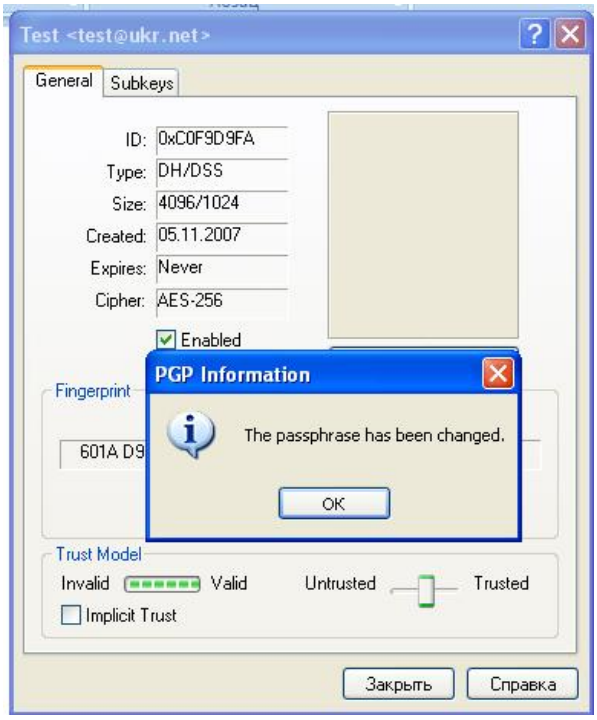

Рис. 5.8. Сообщение об изменении пароля

Отзыв ключа

Если когда-либо возникнет ситуация, в которой не сможете больше доверять своей персональной паре ключей, то следует выпустить сертификат отзыва ключа, сообщающий всем, что соответствующий открытый ключ не должен больше использоваться. Лучший способ распространить сертификат это «выложить» его на сервере открытых ключей.

Как отозвать ключ

1. Пометьте пару ключей, которую хотите отозвать. В нашем примере будем отзывать связку ключей Test.
2. Выберите из меню **Keys** или из контекстного меню пункт **Revoke.**
3. Появится предупреждающее окно о последствиях отзыва и действительно ли вы хотите отозвать пару ключей.

Рис. 5.9. Сообщение об отзыве ключа

4. Для подтверждения отзыва нажмите «Да». Появится диалоговое окно, в котором будет предложено ввести пароль доступа к данной паре ключей (рис. 5.10.).

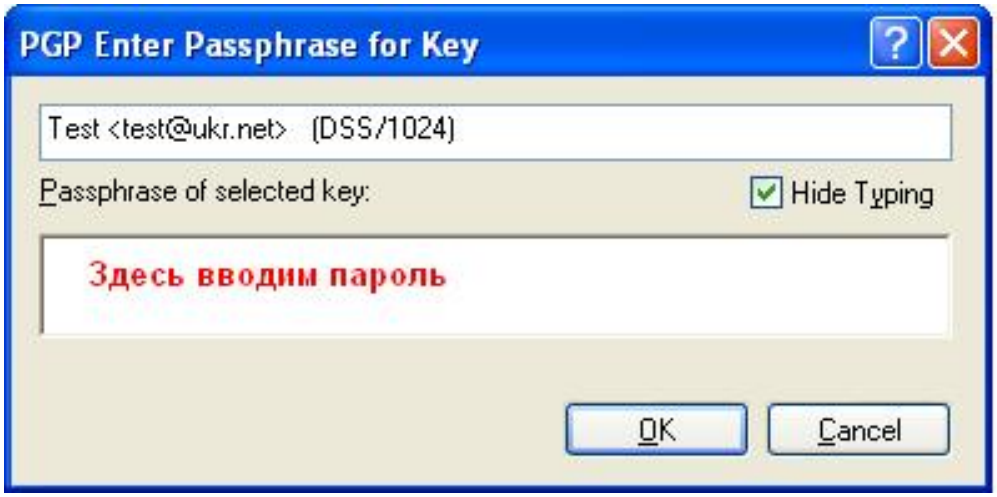

Рис. 5.10.

5. Введите пароль и нажмите «Ok».

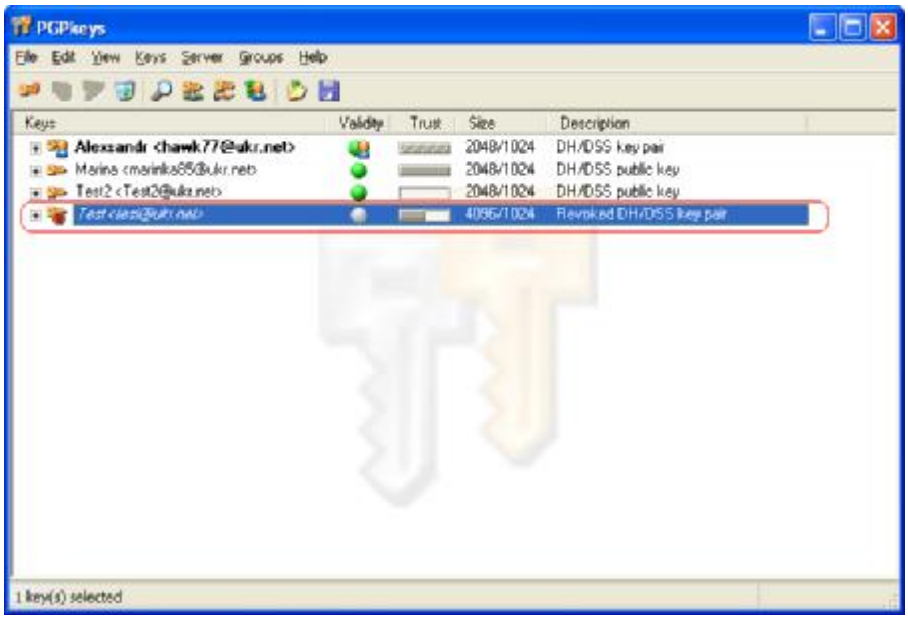

Рис. 5.11. Отозванный ключ символизируется

Рис. 5.12. Свойства ключа

6. Отправьте отозванный ключ на сервер, чтобы все знали, что пользоваться им нельзя.

ТЕМА 6. ШИФРОВАНИЕ СООБЩЕНИЙ И ФАЙЛОВ. НАЛОЖЕНИЕ ПОДПИСИ

Шифрование (подпись) содержимого «буфера обмена»

Перед тем как начать шифровать или дешифровать необходимо, сделать одно из важных действий. В области системных индикаторов должен появился значок замка (это программа PGPtray).

Рис. 6.1. Значок замка – программа PGPtray

По умолчанию при установке самой PGP, программа **PGPtray** выставляется в установках так, чтобы при загрузке компьютера эта программка также загружалась. Ярлык PGPtray следует добавить в «**Автозагрузку**» Для этого необходимо: во-первых, создать ярлык для иконки **PGPtray;** во-вторых, поместить этот ярлык в C:\Documents and Settings\All Users\Главное меню\Программы\Автозагрузка

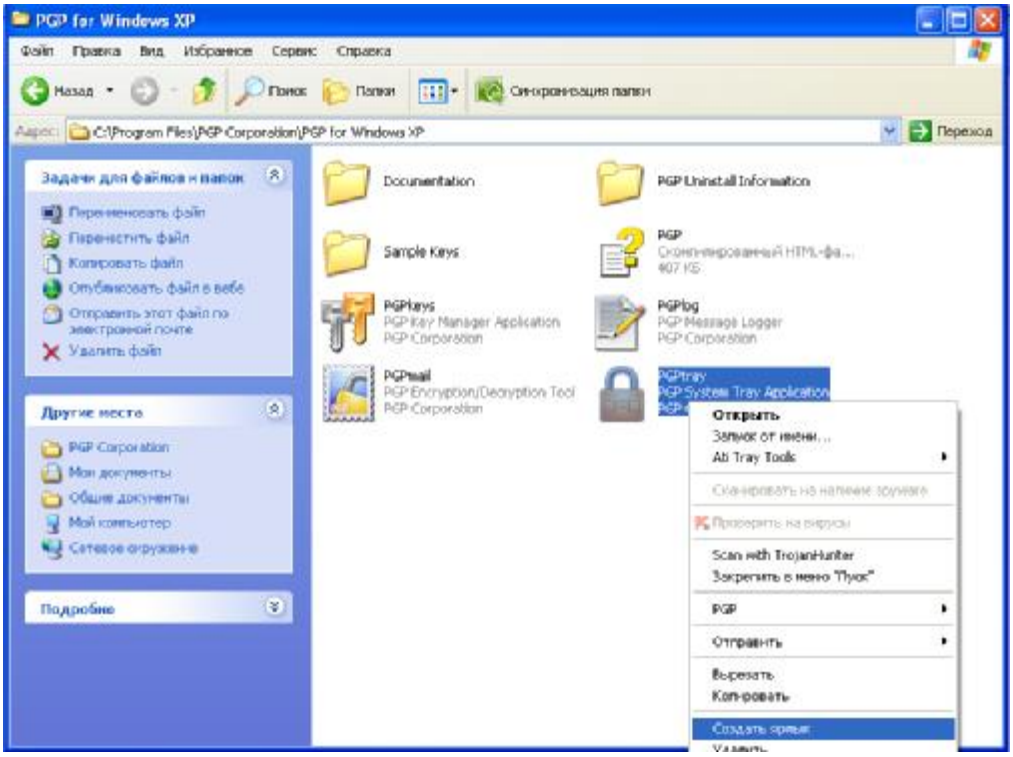

Рис. 6.2. Добавление ярлыка PGPtray в «Автозагрузку»

Процедура шифрования и наложения подписи через Буфер обмена осуществляется следующими действиями:

1. Наберите текст в любом, из существующих текстовых редакторов, например, Microsoft Word, Notepad (Блокнот), WordPad и т.д.

Откройте «блокнот» и напишете в нем что-то, что мы хотите зашифровать, например, Учение – Свет, а неученее – Тьма (рис. 6.3.).

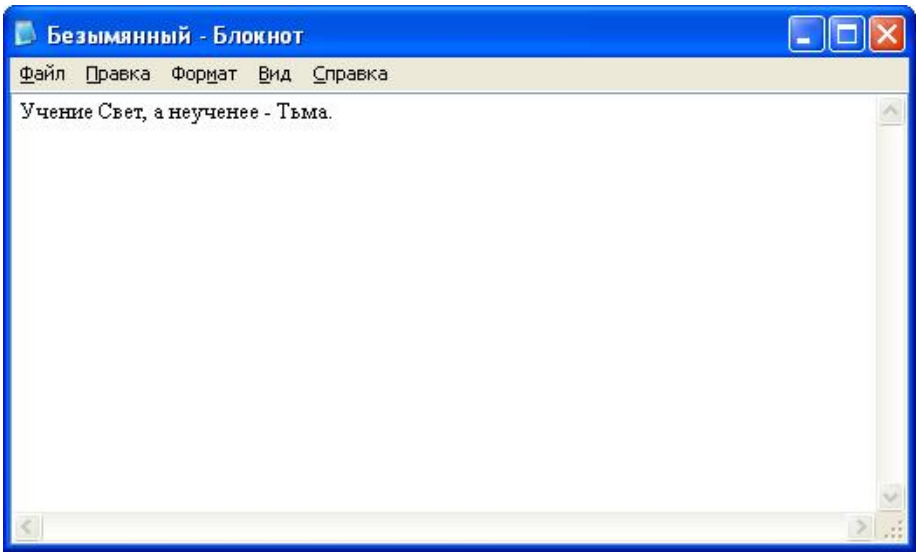

Рис. 6.3. Сообщение, набранное в программе «блокнот» для шифрования

2. Выделите текст известным способом, например Ctrl-A.
3. Выберите копировать из меню **Правка**. Каждый раз, когда копируете или вырезаете текст из окна приложения, то он временно хранится в **буфере обмена**.
4. Щелкните на значке замочек (любой клавишей мыши) в «области» системных индикаторов и выберите **Clipboard – Encrypt & Sign (**рис. 6.4.**).**

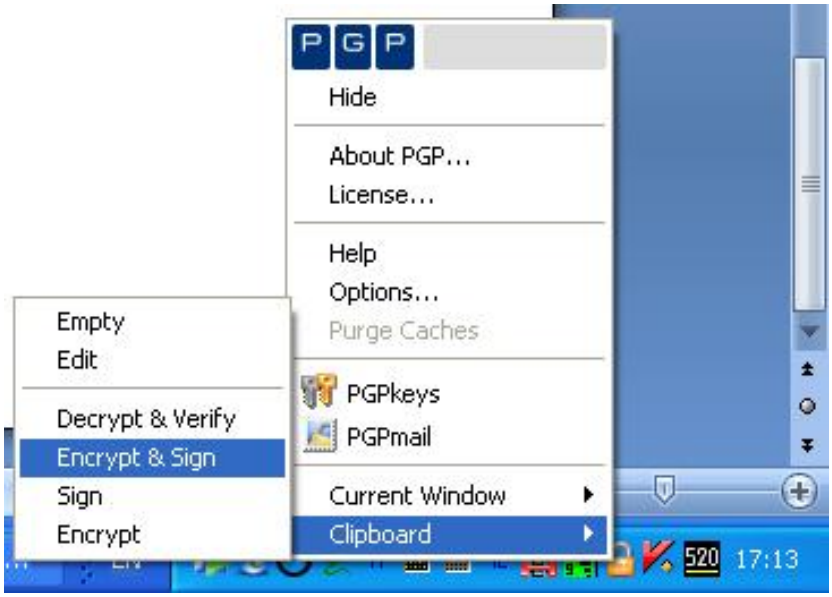

Рис. 6.4.

5. Появится окно выбора ключа (Key Selection Dialog) (рис. 6.5.).

Рис. 6.5.

6. Перетащите открытый ключ получателя из верхнего окна в нижнее. В нашем случае будем шифровать на имя Test<test@ukr.ney>. После перетаскивания ключа в нижнее окно оно должно выглядеть так, как показано на рис. 6.6.

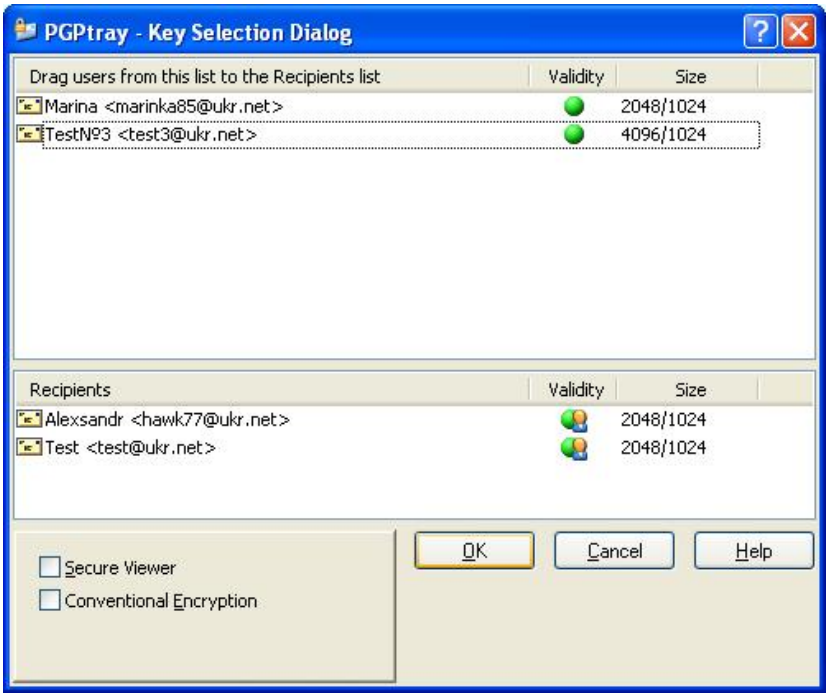

Рис. 6.6.

7. Щелкните далее кнопку «**Ок**»

Если была выбрана опция наложения подписи до того, как сообщение будет отправлено, появится диалоговое окно пароля (**Passphrase**), требующее введения пароля Вашего закрытого ключа по умолчанию. Если есть другие пары ключей, то следует нажать на стрелочку вверху окна и выбрать нужный ключ.

8. Введите свой пароль и нажмите «**Ок**» (рис. 6.7.).

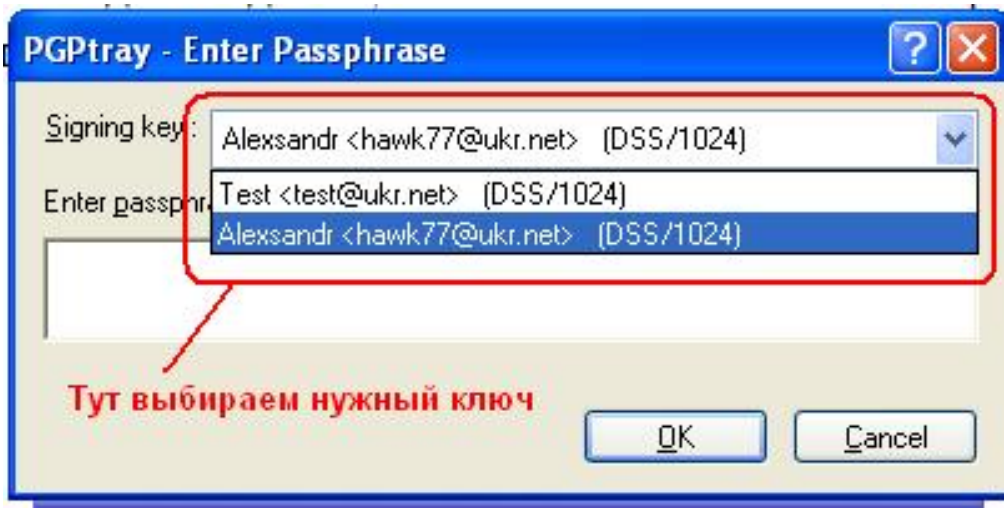

Рис. 6.7.

9. Вернитесь в окно текстового редактора или в окно почтового пакета и выберите пункт **Вставка(Paste)** меню **Правка (Edit)**. Этим действием скопируете зашифрованное (подписанное) сообщение в тело сообщения. В нашем случае копируем в тот же «блокнот», где изначально писали «Учение – Свет, а неученее – Тьма». Теперь «блокнот» должен выглядеть так, как показано на рис. 6.8.

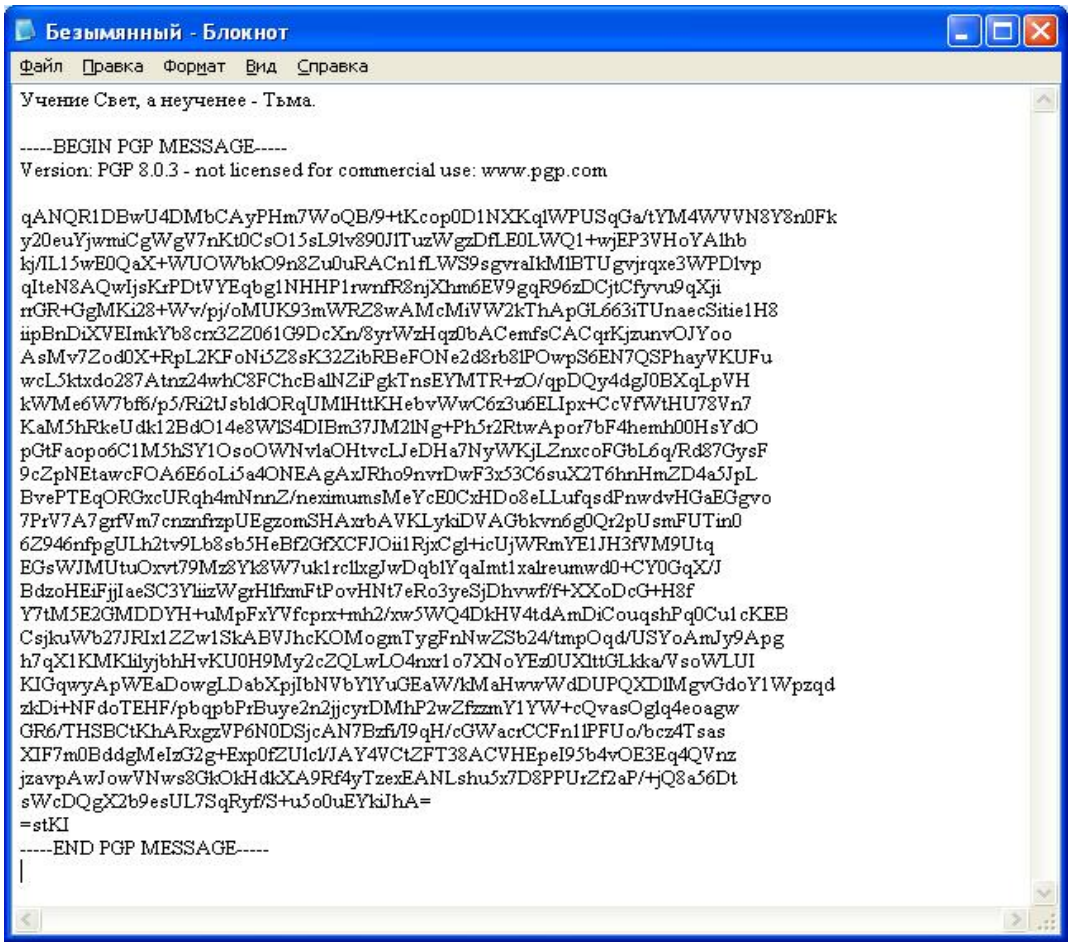

Рис. 6.8. Копирование зашифрованного (подписанного) сообщения в тело сообщения

10. «Учение – Свет, а неученее – Тьма» из Блокнота можно удалить, а сообщение сохранить в любом текстовом файле или сразу отправить по электронной почте скопировав все, что находится между -----BEGIN PGP MESSAGE----- и -----END PGP MESSAGE----- включительно с этими же надписями, т.е. выделяем так как показано на рис. 6.9.

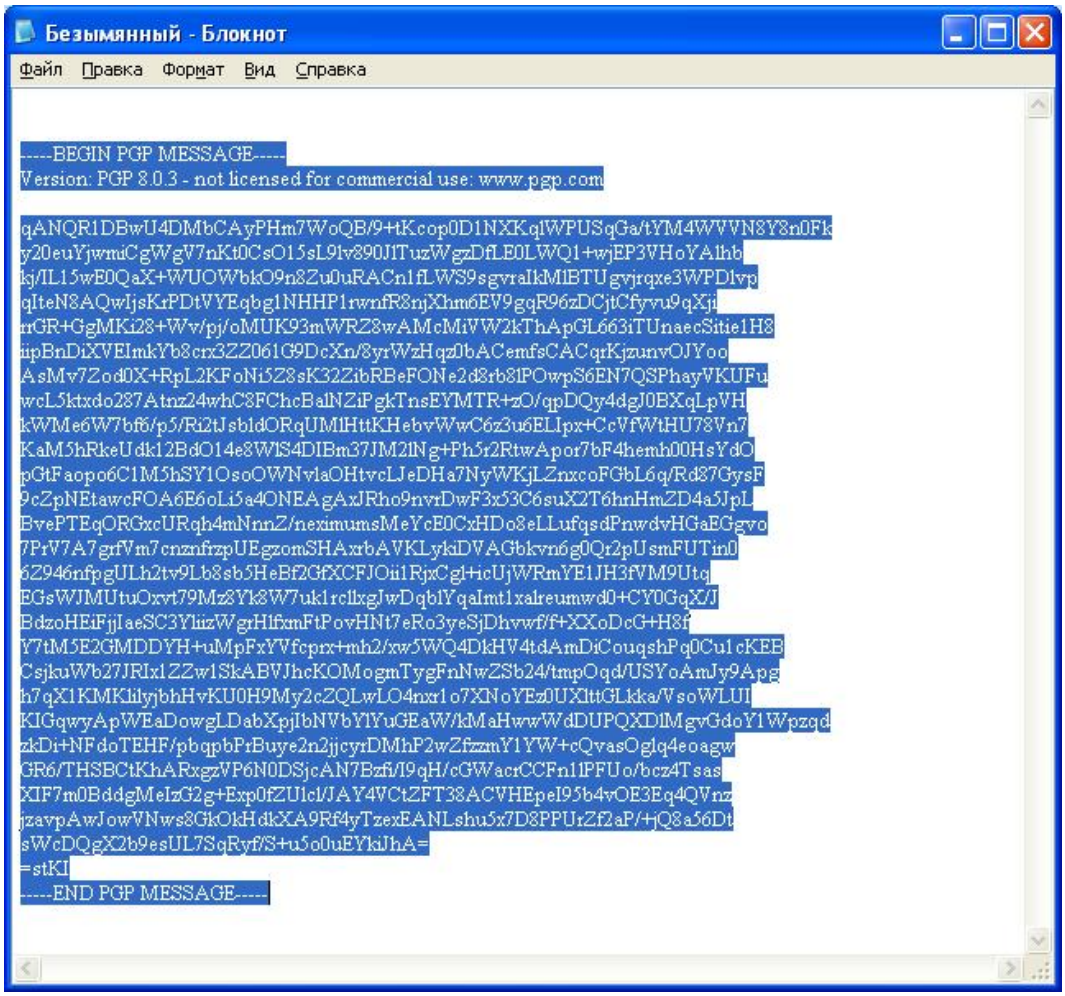

Рис. 6.9. Сохранение сообщения в текстовом файле

Шифрование и наложение подписи из окна Мой компьютер (Explorer)

Отправить зашифрованный (подписанный) файл в качестве приложения к сообщению или просто зашифровать файл, чтобы защитить его от нежелательного доступа со стороны третьих лиц, следует это сделать из того окна, где находимся, например, предполагаемый нами файл к шифрованию будет находиться в папке **«Мои документы».**

Шифрование и подпись файла

1. Откройте папку **Мои документы**.
2. Пометьте файлы, которые хотите зашифровать (подписать), в нашем варианте будет использоваться текстовый файл «**Шифровка.txt**» (рис. 6.10.).

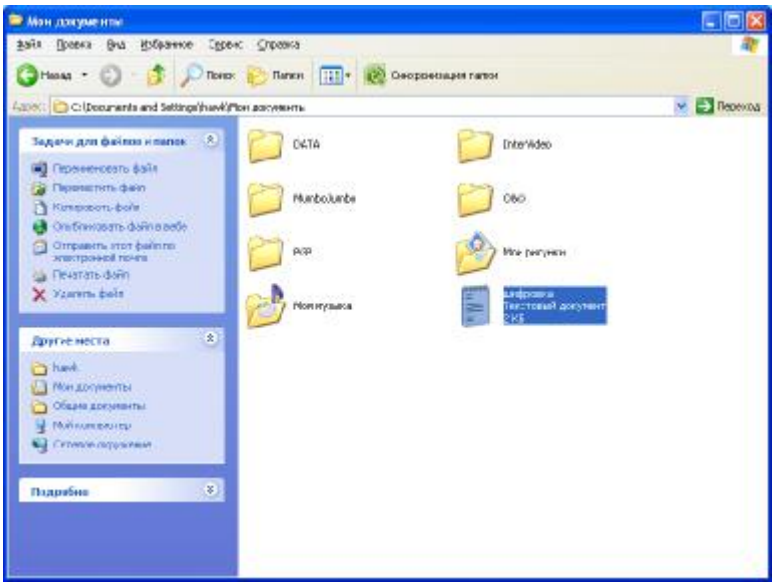

Рис. 6.10. Шифрование и подпись файла (шаг 1)

Можете пометить несколько файлов в папку, но шифроваться они будут по отдельности, даже если выбрали зашифровать эту папку.

3. Выбираем необходимую опцию из меню «Файл» или из контекстного меню, вызываемого щелчком правой кнопки мыши (рис. 6.11.).

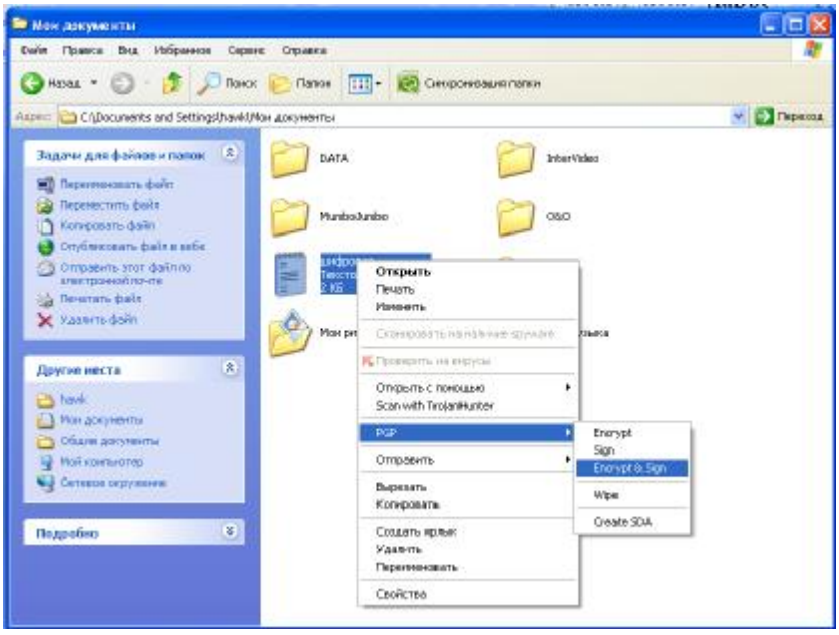

Рис. 6.11.

При шифровании файла появится диалоговое окно выбора ключа, в котором выбираем открытый ключ получателя (рис. 6.12.).

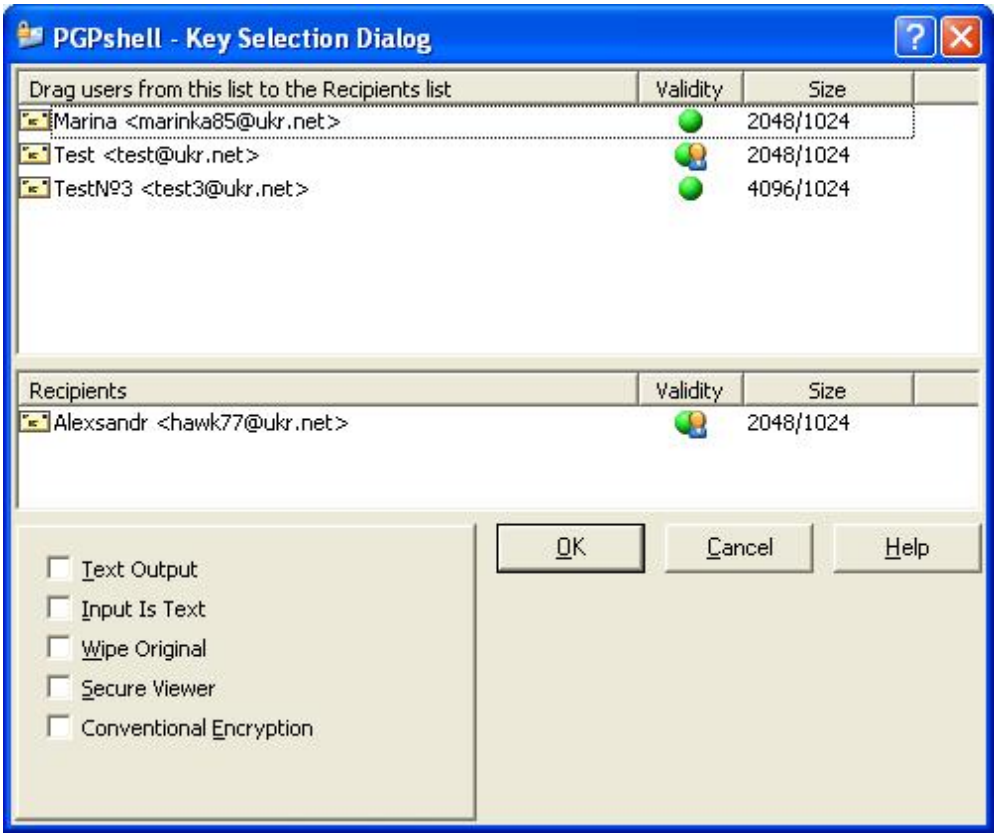

Рис. 6.12.

При отправке файлов в качестве приложений к сообщениям, при использовании некоторых почтовых пакетов может понадобиться отметить поле «текстовый вывод» (text output) для того, чтобы был сгенерирован файл в формате ASCII. Это требуется при использовании некоторых старых пакетов.

Если необходимо, чтоб файл был сгенерирован в формате ASCII и отмечено поле **Text Output**, то эта опция увеличивает объем файла на 30%.

4. Выбираем открытые ключи, «перетаскиваем» их из верхнего поля (Users) в нижнее (**Recipients**) и нажимаем «Ок».
5. Появится диалоговое окно пароля (**Passphrase**), требующее введения пароля. Вводим пароль и нажимаем «Ок».

6. В папке **Мои документы** должен появиться новый файл с расширением **.pgp** (рис. 6.13.). В нашем случае это **«шифровка.txt.pgp».** Далее этот зашифрованный файл можете отправить получателю.

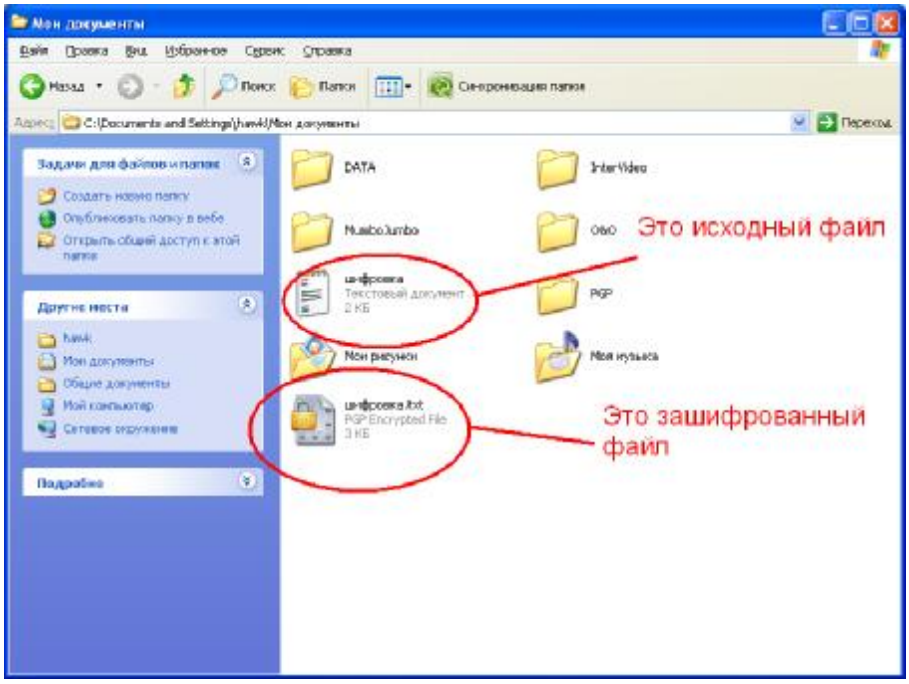

Рис. 6.13.

ТЕМА 7. РАСШИФРОВКА И ВЕРИФИКАЦИЯ ПОДПИСИ В СООБЩЕНИЯХ И ФАЙЛАХ

Перед тем как дешифровать сообщение, необходимо, чтобы в «области» системных индикаторов появился значок замка (это программа PGPtray), как показано на рис. 7.1.

Рис. 7.1.

Расшифровка почтового сообщения

1. Откройте почтовое сообщение обычным способом. В теле сообщения увидите блок шифровки (рис. 7.2.).

Рис. 7.2.

2. Выделите этот текст. Очень важно, чтобы выделили всё начиная от -----BEGIN PGP MESSAGE----- и заканчивая -----END PGP MESSAGE.

Рис. 7.3. Выделенный текст сообщения

Когда все выделено, нажмите «**Копировать».** Теперь шифрованный текст находится в Буфере обмена.

3. Щелкните на значке «замочек» в «области» системных индикаторов любой клавишей мыши (рис. 7.4.).

Рис. 7.4.

В появившемся меню выбираем **Clipboard**, а затем **Decrypt & Verify.** Как показано на рис. 7.5.

Рис. 7.5.

При расшифровке появится окно ввода пароля (**Enter Passphrase**), в котором необходимо ввести свой пароль, который указан по умолчанию в программе PGPkeys (рис. 7.6.).

Рис. 7.6. Окно ввода пароля

4. Введите пароль и нажмите «Ок». Появится окно (рис. 7.7.) в котором будет расшифрованное сообщение. В сообщении указано:

- автора сообщения;
- подписавший сообщение (Signer);
- время подписи (Signed);
- время проверки и расшифровки сообщения (Verified).

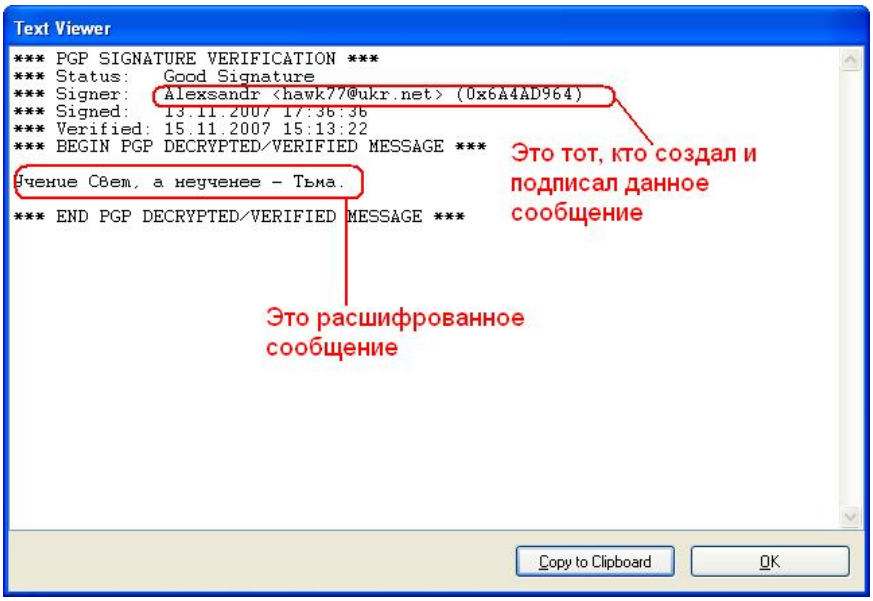

Рис. 7.7. Окно с расшифрованным сообщением

Расшифровка и верификация файла

Рассмотрим пример, когда зашифрованный файл находится в папке «**Мои документы**».

1. Зайдём в папку Мои документы и помечаем тот файл, который хотим расшифровать. В нашем примере будет файл «шифровка.txt.pgp». Выделим несколько файлов, но расшифровываться они будут по отдельности.
2. Выделим опцию **Decrypt &Verify** из меню **Файл** или из контекстного меню, вызываемого щелчком мыши. Как показано на рис. 7.8.

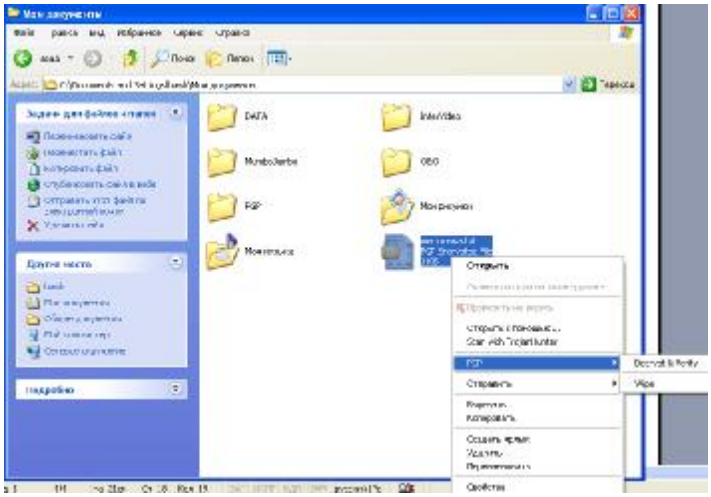

Рис.7.8.

3. При расшифровке появится Диалоговое окно пароля (Passphrase), требующее от вас введения пароля (рис. 7.9.).

Рис. 7.9.

4. Введите пароль и щелкните «Ок». Если файл подписан, то появится окно (PGPlog) с информацией о том, успешно ли прошла верификация (рис. 7.10.).

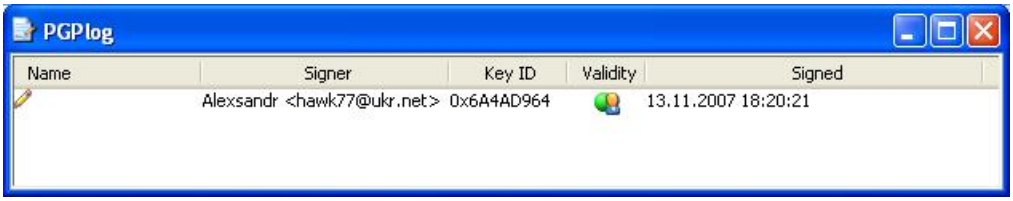

Рис. 7.10.

5. После ввода пароля в папке **Мои документы** появится расшифрованный файл «шифровка.txt» (рис. 7.11.).

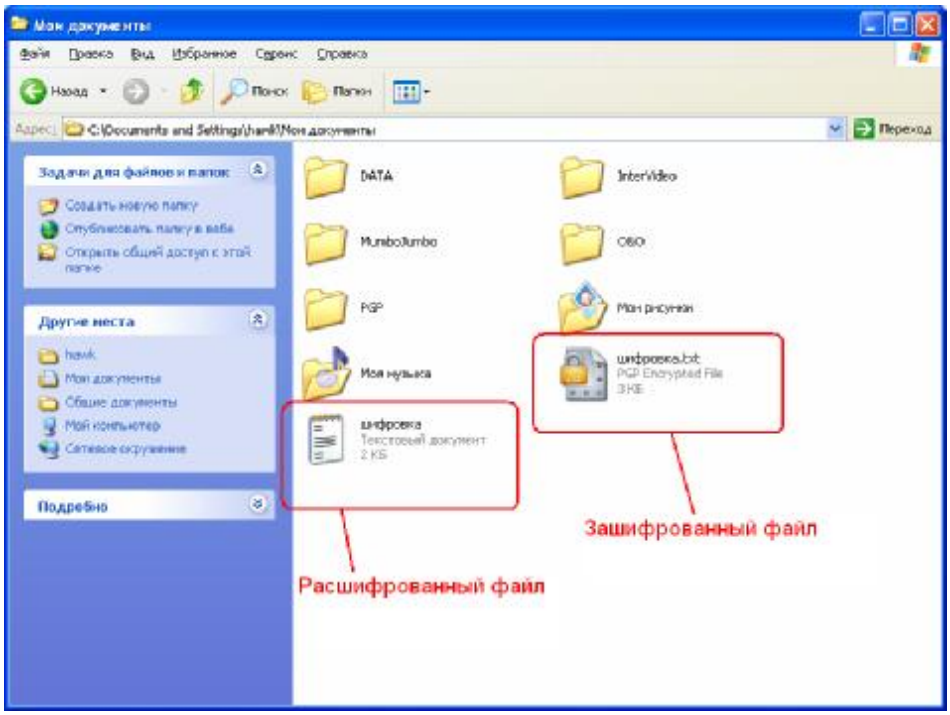

Рис. 7.11.

Литература

1. Айгер М. Комбинаторная теория. – М.: Мир, 1982. – 556 с.
2. Акимов О. Е. Дискретная математика. Логика, группы, графы. – М.: Лаборатория базовых знаний, 2001. – 376 с.
3. Горбатов В. А. Основы дискретной математики. – М.: Высшая школа, 1986. – 311 с.
4. Ершов Ю. Л. Теория нумераций. – М.: Наука, 1977. – 416 с.
5. Кузин Л. Т. Основа кибернетики. Т. 2. Основы кибернетических моделей. – М.: Энергия, 1979. – 584с.
6. Новиков Ф. А. Дискретная математика для программистов. – СПб.: Москва – Харьков, – Минск. 2002. – 301.с.
7. Боас Р., Фервай М., Гюнтер Х. Delphi 4 Полное руководство, – К.: BHV, 1998. – 448 с.
8. Developer’s Guide for Delphi 3, Borland Inprise Corporation, 100 Enterprise Way, Scotts Valley, CA 95066-3249
9. Developer’s Guide for Delphi 5, Borland Inprise Corporation, 100 Enterprise Way, Scotts Valley, CA 95066-3249
10. Object Pascal Language Guide, Borland Inprise Corporation, 100 Enterprise Way, Scotts Valley, CA 95066-3249

Содержание

Учебное издание

Швачич Геннадий Григорьевич
Овсянников Александр Васильевич
Кузьменко Вячеслав Витальевич
Панасюк Александр Владимирович

Основы защиты информации

Учебное пособие

Тем. план 2008, поз.

Подписано к печати _ _Формат 60х84 1/16. Бумага офсетная. Печать Times.
Уч.-изд. лист. Усл.-печ. лист. Тираж экз. заказ №

Национальная металлургическая академи Украины
49600, Днепропетровск – 5, пр. Гагарина, 4

Редакционно-издательский отдел НМетАУ