

Pretty Good Privacy™  
**PGP для Персональной Приватности**  
Версия 5.0

Для  
Windows® 95 и Windows NT

Руководство пользователя

PGP™, Inc.

© 1997 by Pretty Good Privacy, Inc. Все права сохранены.

Отпечатано в Норвегии

### **PGP для Персональной Приватности, версия 5.0**

Запишите порядковый номер со своего экземпляра лицензии здесь:

Copyright © [1990], 1997 by Pretty Good Privacy, Inc. All Rights Reserved.

PGP, Pretty Good, и Pretty Good Privacy являются зарегистрированными торговыми марками Pretty Good Privacy, Inc. Все другие упомянутые торговые марки или зарегистрированные торговые марки принадлежат их владельцам.

Pretty Good Privacy, Inc. может обладать патентами или поданными патентными заявками, связанными с затронутыми в данном документе вопросами. Приобретение этого документа или программного обеспечения не дает вам лицензии на использование таких патентов.

В PGP использованы алгоритмы, описанные в патентах США за номерами 4200770, 4218582, 4405829 и 4424414, исключительная лицензия на которые предоставлена Public Key Partners.

В PGP использован криптографический шифр IDEA, описанный в патенте США за номером 5214703, лицензия на который предоставлена Ascom Tech AG. IDEA является торговой маркой Ascom Tech AG.

Программа архивации, использованная в PGP, написана Марком Адлером и Жаном-Лу Гэйи и заимствована с разрешения из бесплатной реализации Info-ZIP.

Программное обеспечение, поставляемое с настоящей документацией, лицензируется для использования вами в ваших личных целях на условиях, изложенных в End User License Agreement, и на программное обеспечение предоставляется ограниченная гарантия. Информация, изложенная в настоящем документе, может изменяться без предварительного уведомления. Pretty Good Privacy, Inc. не гарантирует, что эта информация соответствует вашим конкретным запросам, или что она свободна от ошибок. Эта информация может включать технические неточности и типографские ошибки. В эту информацию могут вноситься изменения, которые будут включены в последующие издания настоящего документа, в случае, если, и в то время, когда внесение таких изменений будет возможно для Pretty Good Privacy, Inc.

Экспорт настоящего программного обеспечения и документации может подлежать ограничениям в соответствии с правилами, время от времени издаваемыми Отделом управления экспортом Министерства торговли Соединенных Штатов, который ограничивает экспорт и реэкспорт определенных продуктов и технических данных.

**PRETTY GOOD PRIVACY, INC.**

2121 South El Camino Real, Suite 902  
San Mateo, CA 94403

(415) 631-1747

(415) 572-1932 fax

[info@pgp.com](mailto:info@pgp.com)

<http://www.pgp.com>

ОГРАНИЧЕННАЯ ГАРАНТИЯ. Pretty Good Privacy, Inc. гарантирует, что настоящее программное обеспечение будет функционировать в существенном соответствии с прилагаемыми печатными материалами в течении 90 дней со времени первоначального приобретения. Совокупная ответственность Pretty Good Privacy, Inc. и ваши возможные претензии ограничиваются, по выбору Good Privacy, Inc., либо (а) возвратом суммы, уплаченной при приобретении лицензии, или (б) исправлением или заменой программного обеспечения, не соответствующего ограниченной гарантии, предоставляемой Good Privacy, Inc., которое должно быть возвращено за ваш счет Pretty Good Privacy, Inc. вместе с копией платежного документа. На любое исправленное или предоставленное взамен программное обеспечение предоставляется гарантия на срок 30 дней или оставшаяся часть первоначального гарантийного срока, в зависимости от того, какой из этих периодов дольше.

ЕСЛИ ЭКСПОРТ НАСТОЯЩЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БУДЕТ ЗАПРЕЩЕН (СМ. ВЫШЕ), ЭТИ УСЛОВИЯ НЕ РАСПРОСТРАНЯЮТСЯ ЗА ПРЕДЕЛЫ СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ. НЕ ПРЕДОСТАВЛЯЕТСЯ НИКАКИХ ГАРАНТИЙ, КРОМЕ ИЗЛОЖЕННЫХ ЗДЕСЬ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ДОКУМЕНТАЦИЯ ПОСТАВЛЯЮТСЯ "КАК ЕСТЬ", И PRETTY GOOD PRIVACY, INC. ОТКАЗЫВАЕТСЯ ОТ ПРЕДОСТАВЛЕНИЯ ЛЮБЫХ ДРУГИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ НО НЕ ОГРАНИЧИВАЯСЬ ПОДРАЗУМЕВАЕМОЙ ПРИГОДНОСТЬЮ ДЛЯ ПРОДАЖИ, ПРИГОДНОСТЬЮ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ, СООТВЕТСТВИЕМ ОПИСАНИЮ, И НЕНАРУШЕНИЕМ ПРАВ ТРЕТЬЕЙ СТОРОНЫ. НАСТОЯЩАЯ ОГРАНИЧЕННАЯ ЛИЦЕНЗИЯ ПРЕДОСТАВЛЯЕТ ВАМ ОПРЕДЕЛЕННЫЕ ПРАВА. ВЫ МОЖЕТЕ ИМЕТЬ И ДРУГИЕ ПРАВА, КОТОРЫЕ ИЗМЕНЯЮТСЯ ОТ ШТАТА К ШТАТУ. ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ. СОВОКУПНАЯ МАТЕРИАЛЬНАЯ ОТВЕСТВЕННОСТЬ PRETTY GOOD PRIVACY, INC. ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ, ПРОИСТЕКАЮЩАЯ ИЗ ПРЕТЕНЗИЙ, ТРЕБОВАНИЙ И ДЕЙСТВИЙ, ПРЕДПРИНЯТЫХ В СООТВЕТСТВИИ ИЛИ В СВЯЗИ С НАСТОЯЩИМ СОГЛАШЕНИЕМ, НЕ БУДЕТ ПРЕВЫШАТЬ СУММЫ, УПЛАЧЕННОЙ ПРИ ПРИОБРЕТЕНИИ ЛИЦЕНЗИИ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ GOOD PRIVACY, INC. И ЕЕ ПОСТАВЩИКИ НЕ БУДУТ ОТВЕТСТВЕННЫ ЗА ЛЮБОЙ КОСВЕННЫЙ, СЛУЧАЙНЫЙ, ВОСПОСЛЕДОВАВШИЙ ИЛИ ОСОБЫЙ УЩЕРБ ИЛИ ПОТЕРЮ ПРИБЫЛЕЙ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ УЩЕРБОМ ОТ ПОТЕРИ ДЕЛОВОЙ ПРИБЫЛИ, ЗАДЕРЖЕК В ВЕДЕНИИ БИЗНЕСА, ПОТЕРИ ДЕЛОВОЙ ИНФОРМАЦИИ, И ДРУГИХ КОСВЕННЫХ ПОТЕРЬ). ПОСКОЛЬКУ РЯД ШТАТОВ НЕ ДОПУСКАЕТ ИСКЛЮЧЕНИЯ ИЛИ ОГРАНИЧЕНИЯ ОТВЕТСТВЕННОСТИ ЗА ВОСПОСЛЕДОВАВШИЙ ИЛИ СЛУЧАЙНЫЙ УЩЕРБ, ПЕРЕЧИСЛЕННЫЕ ОГРАНИЧЕНИЯ МОГУТ К ВАМ НЕ ОТНОСИТЬСЯ.

---

---

Эта книга написана Майком Яннамико

особая благодарность Гэйлу Кеснеру Хасперту

перевод с английского и дополнение [Максима Отставнова](#)  
<[maksim@volga.net](mailto:maksim@volga.net)>

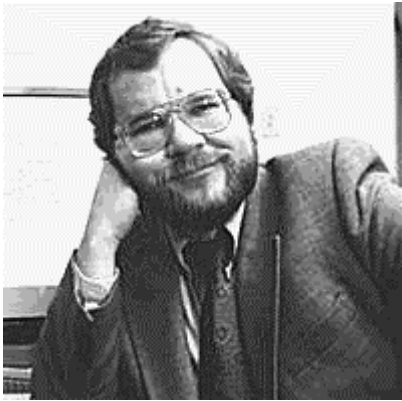
Версия перевода 1.0 (1 сентября 1997 г.)

**ЭТОТ ПЕРЕВОД РАСПРОСТРАНЯЕТСЯ ТОЛЬКО БЕСПЛАТНО, ЕСЛИ  
ИНОЕ НЕ БУДЕТ УСТАНОВЛЕНО ВЛАДЕЛЬЦЕМ АВТОРСКИХ ПРАВ**

## Содержание

Содержание .....	4
Уважаемый пользователь PGP!.....	6
PGP 5.0 Быстрый старт .....	8
Глава 1 Введение в PGP для Персональной приватности.....	10
Краткий обзор .....	11
Генерация пары из закрытого и открытого ключей .....	11
Обмен ключами между пользователями.....	12
Сертификация и верификация действительности ключей.....	12
Шифрование сообщений и файлов и наложение подписи .....	12
Расшифровка и верификация подписи на сообщениях и файлах.....	12
Об этом Руководстве .....	13
Глава 2 Приступая к работе .....	14
Системные требования .....	14
Совместимость с другими версиями.....	14
Модернизация предыдущей версии .....	15
Установка PGP .....	17
Запуск PGP .....	17
Запуск из Области индикаторов Панели задач.....	18
Запуск PGP из поддерживаемых пакетов электронной почты.....	20
Запуск PGP из Проводника.....	21
Выбор получателей.....	21
Сокращения и горячие клавиши.....	22
Глава 3 Генерация и распространение ключей.....	23
Основные понятия.....	23
Генерация пары ключей.....	24
Защита ваших ключей.....	32
Распространение вашего открытого ключа .....	33
Открытие доступа к открытому ключу через сервер ключей .....	34
Включение открытого ключа в почтовое сообщение.....	35
Экспорт открытого ключа в файл .....	35
Получение открытых ключей других пользователей PGP .....	35
Получение открытого ключа с сервера ключей.....	36
Получение ключа из тела почтового сообщения.....	37
Импорт открытого ключа из файла .....	37
Проверка подлинности ключа .....	38
Глава 4 Отправка и получение приватной электронной почты.....	40
Шифрование почты и наложение подписи .....	40
Шифрование и наложение подписи в поддерживаемых пакетах электронной почты .....	40
Шифрование и наложение подписи через Буфер обмена .....	42
Шифрование и наложение подписи из окна Проводника.....	44
Расшифровка и верификация почты .....	46
Расшифровка и верификация в поддерживаемых почтовых пакетах.....	47
Расшифровка и верификация через Буфер обмена .....	48
Расшифровка и верификация из окна Проводника.....	49
Глава 5 Управление ключами и установка предпочтений.....	51
Управление ключами.....	51
Окно PGPkeys .....	52
Исследование свойств ключей .....	54
Указание пары ключей, используемой по умолчанию .....	55
Добавление нового имени или адреса .....	55
Проверка отпечатка ключа .....	56
Сертификация чужого открытого ключа.....	57
Указание уровня доверия .....	58
Запрет и разрешение использования ключей.....	59
Удаление ключа, подписи или идентификатора пользователя .....	60

Изменение пароля доступа.....	60
Импорт и экспорт ключей .....	61
Отзыв ключа .....	62
<b>Установка пользовательских предпочтений.....</b>	<b>63</b>
Общие предпочтения.....	64
Предпочтения файлов со связками ключей .....	65
Предпочтения работы с почтой .....	66
Предпочтения сервера ключей.....	67
<b>Глава 6 Особенности модели безопасности и уязвимые места .....</b>	<b>68</b>
<b>Зачем я написал PGP.....</b>	<b>68</b>
<b>Основы криптографии .....</b>	<b>72</b>
Как работает криптография с открытым ключом .....	72
Как шифруются ваши файлы и сообщения.....	73
Симметричные алгоритмы PGP.....	74
Сжатие данных.....	76
О случайных числах, используемых в качестве сеансовых ключей .....	76
Как осуществляется расшифровка .....	77
Как осуществляется электронная подпись.....	77
О дайджесте сообщения.....	78
Как защищать открытые ключи от подмены.....	79
Как PGP следит за тем, какие ключи действительны?.....	83
Как защищать закрытые ключи от раскрытия .....	84
Что, если вы потеряете свой закрытый ключ? .....	85
<b>Осторожно: шарлатанские снадобья .....</b>	<b>86</b>
<b>Уязвимые места.....</b>	<b>90</b>
Скомпрометированные пароль и закрытый ключ .....	90
Подделка открытых ключей .....	91
Не до конца удаленные файлы .....	91
Вирусы и закладки .....	92
Файлы подкачки (виртуальная память).....	92
Нарушение режима физической безопасности .....	93
Радиоатака.....	94
Защита от фальшивых дат подписей .....	94
Утечка данных в многопользовательских системах.....	95
Анализ активности .....	95
Криптоанализ.....	96
Рекомендованная вводная литература .....	96
Другая литература.....	97
<b>Словарь терминов .....</b>	<b>97</b>
<b>Дополнение Ресурсы PGP, доступные в Internet.....</b>	<b>100</b>
PGP, Inc.'s Homepage.....	100
The International PGP Homepage.....	100
Русский Альбом <b>PGP</b> .....	100
MIT's PGP Homepage.....	100
PGP.net .....	100



Июнь 1997 г.

## Уважаемый пользователь PGP!

Ну вот и все. После трех лет работы, у нас, наконец, есть долгожданная *PGP 5.0* (ранее известная, как 3.0), и она готова к выпуску.

Это заняло больше времени, чем предполагалось – по разным причинам, и не в последнюю очередь из-за трехлетнего уголовного расследования, предпринятого против меня американским правительством. Последнее обстоятельство

действительно замедлило всю работу. Оно отняло почти всех моих добровольных помощников, усилия которых были столь полезны при работе над *PGP 2.0* и последующими версиями. Для тех из вас, кто не знаком с этим делом: правительство США заняло позицию, согласно которой шифровальное программное обеспечение не должно экспортироваться без разрешения Государственного департамента. Поскольку в 1991 г. *PGP* была бесплатно опубликована в Интернет и впоследствии распространилась по всему миру, правительство сочло, что имело место нарушение закона. Это привело к формированию работавшей в основном бесплатно группы правовой защиты, созданию Фонда правовой защиты и трем годам почти ежедневных интервью. Пресса была в массе своей настроена против такого преследования, и вопрос о политике в области криптографии возбудил гнев всей компьютерной промышленности.

Однако, в январе 1996 г. следствие было закрыто без предъявления обвинения. Вскоре после этого я основал свою собственную компанию, *PGP, Inc.* Мы наняли команду первоклассных инженеров для разработки продуктов, таких, как наш новый продукт, *PGP для Персональной приватности, версия 5.0.*

Эта версия предусматривает множество новых возможностей. Предыдущая версия *PGP (2.6.2, выпущенная МТИ)*, предназначалась только для *MS-DOS* и *Unix*. Новая версия с самого начала рассчитана на то, чтобы предоставить среду графического пользовательского интерфейса (ГПИ). Уже есть версии, работающие под *Windows 95* и *Windows NT*, а также версия для *Apple Macintosh*. У нас также есть версия без ГПИ для *Unix*, начиная с платформы *Linux*. ГПИ придает продукту новое дыхание, допуская прозрачную интеграцию в существующие пакеты для работы с электронной почтой, начиная с популярной программы *Eudora* (фирмы *Qualcomm*), *Microsoft Exchange* и *Microsoft Outlook*. Теперь использование *PGP* для шифрования и расшифровки почты – дело всего лишь пары щелчков мыши.

Новая версия также предусматривает использование дополнительных алгоритмов шифрования. Может быть, наиболее примечательно использование нового алгоритма шифрования с открытым ключом, который должен послужить альтернативой *RSA*. Сроки действия патента Диффи и Хеллмана, а также патента Хеллмана и Меркли истекают в этом году, открывая дверь к свободному от отчислений использованию алгоритмов шифрования с открытым ключом. От этого выиграют все, так как всей компьютерной промышленности приходилось иметь дело с патентной монополией на использование открытых ключей, которая затормозила внедрение этих алгоритмов на многие годы. Теперь эта область становится открытой.

Кроме того, теперь для каждого пользователя создается две отдельные пары ключей, одна из которых служит для шифрования/расшифровки (Диффи-Хеллман), а другая – для наложения/верификации подписи (*DSS*), в стандарте, предложенном Национальным институтом стандартизации США (*NIST*). Сегодня они представлены пользователю как одна пара ключей. В последующих релизах мы предоставим пользователю возможность изменять *DH*-ключ без изменения *DSS*-ключа. С этой новой технологией открывается целый ряд новых возможностей, включая улучшение показателей скорости и безопасности. Для получения преимуществ в полном масштабе, будет полезно, чтобы в миграции к новым алгоритмам криптографии с открытыми ключами Участвовала как можно большая часть сообщества пользователей *PGP*.

Мы также реализовали новые блочные шифры для шифрования основного массива данных, предоставляя выбор между *тройным DES* и *CAST*, при этом продолжая поддерживать шифр *IDEA*, используемый в предшествующих версиях *PGP*. Мы также предоставляем новый алгоритм хеширования, *SHA-1*, для вычисления цифровой подписи. По своим характеристикам он превосходит *MD5*, разработанный в *RSA Data Security, Inc.* Для использования *SHA* пользователи должны перейти на технологию цифровой подписи *DSS*, так как в технологии подписей *RSA* в целях обеспечения обратной совместимости с предшествующими версиями продолжает использоваться хеширование *MD5*.

Особенно примечательной новой возможностью является интеграция *PGP* с серверами открытых ключей. Теперь *PGP* позволяет искать открытые ключи непосредственно на удаленном сервере ключей, например, поддерживаемом MIT. Когда вы генерируете новую пару ключей, *PGP* предлагает подгрузить открытый ключ на удаленный сервер ключей. Каждому будет доступен чей угодно открытый ключ, как только он понадобится. Это объединит всех пользователей *PGP* в глобальное сообщество, с инфраструктурой открытых ключей в национальном масштабе<sup>1</sup>. Такой возможности не может предоставить ни один другой криптографический продукт. Такая инфраструктура будет расти органически, как рос Internet.

В соответствии с моей собственной традицией, установленной еще до того, как была основана эта компания, мы открыто публикуем все исходные коды для того, чтобы инициировать их подробное изучение. Это позволяет каждому убедиться в том, что мы не оставили никаких “черных ходов”, которые могли бы угрожать безопасности. Сначала все коды будут опубликованы в виде книги<sup>2</sup>.

Я надеюсь, вы согласитесь со мной – новая версия *PGP* стоила того, чтобы ее ждать.

Искренне ваш,

Филип Зиммерманн,

главный технолог *Pretty Good Privacy, Inc.*

---

<sup>1</sup> Существующие серверы открытых ключей доступны всем пользователям **Internet**, так что их инфраструктура является в действительности глобальной.—здесь и далее—прим. перев.

<sup>2</sup> Эта книга уже вышла: *Pretty Good Privacy 5.0 Platform Independent Source Code. Ed. by Philip R. Zimmermann & Mark H. Weaver. USA: Warthman Associates, June 14, 1997.*

## PGP 5.0 Быстрый старт

- **Если вы используете PGP в первый раз**, сначала вам нужно сгенерировать пару ключей, выбрав в меню **Keys** программы *PGPkeys* пункт **New Key**. Как правило, это можно сделать автоматически через Помощник генерации ключа. Затем вам нужно будет послать открытый ключ другому пользователю. Для этого перетащите мышью ключ из главного окна *PGPkeys* в окно почтового сообщения. После этого пользователь, который получил ваш ключ, сможет шифровать направляемую вам почту. Чтобы посылать зашифрованные письма ему, вам потребуется получить его открытый ключ. Подписывать письма вы можете и без отправки своего открытого ключа другим пользователям, но тогда никто не сможет верифицировать вашу подпись. Вы также можете отправить свой открытый ключ на доступный сервер открытых ключей, с которого этот ключ смогут получить другие пользователи.
- **Ключи Diffie-Hellman/DSS могут сделать невозможной коммуникацию с пользователями ранних версий PGP.** *Diffie-Hellman/DSS* - это новый тип ключей, являющихся по крайней мере столь же надежными, что и ключи *RSA* той же длины. Однако, ключи *DH/DSS* не поддерживаются более ранними версиями *PGP*, что означает невозможность обмена зашифрованной почтой с пользователями, которые еще не перешли к использованию версии *5.0* или выше. Использование ключей *DH/DSS* значительно сокращает время, необходимое для шифрования и расшифровки.
- **Импорт файлов с ключами из ранних версий PGP.** Ваши файлы с ключами должны быть скопированы в папку установки *PGP 5.0* при выполнении установки. Чтобы импортировать другие файлы с ключами, лучше всего физически заместить файлы с ключами по умолчанию "pubring.pkr" и "secring.skr" вашими старыми файлами "pubring.pgp" и "secring.pgp" в то время, когда *PGP* не запущена. При этом, информация о приписанных ключам степенях доверия сохраняется. Другой способ – это просто перетащить старые файлы с ключами из окна *Проводника (Explorer)* в главное окно *PGP* или выбрать пункт **Import** из меню **Keys** программы *PGPkeys*. При использовании этого способа информация о доверии не будет перенесена, так как если вы получили файл с открытыми ключами от кого-то другого, информация о его степени доверия к ним вам ни к чему. Если у вас на связке несколько закрытых ключей, вам нужно использовать команду **Set Default** из меню **Keys** программы *PGPkeys*, чтобы указать ключ, который при подписи других ключей, а также сообщений, будет использоваться по умолчанию.
- **Чтобы послать свой открытый ключ другому пользователю**, просто переместите его мышью в любое текстовое окно, или отправьте его на сервер ключей, а затем попросите своих друзей подгрузить его, используя *PGP 5.0* или браузер. Обычным является включение URL, указывающего на ключ, в стандартную подпись ваших сообщений. Такой URL выглядит следующим образом:

<<http://swissnet.ai.mit.edu:11371/pks/lookup?op=get&search=0x272727>>



Конечно, вам нужно заменить идентификатор ключа, которым заканчивается URL (0x27272727) на идентификатор вашего собственного ключа. Узнать идентификатор своего ключа вы можете, выбрав этот ключ в главном окне *PGPkeys* и использовав пункт **Properties** меню **Keys** этой программы.

- Прием “Перетащить и оставить” работает почти везде. Вы можете перемещать ключи, идентификатор пользователя, подписи непосредственно на поверхность рабочего стола, идентификаторы пользователей – из списка идентификаторов в список получателей и т.п.
- **Чтобы подписать ключ**, выделите его и выберите пункт **Sign** из меню **Keys** в *PGPkeys*. Вы можете затем указать степень доверия, с которой вы относитесь к данному ключу, щелкнув на нем правой кнопкой мыши и выбрав из контекстного меню пункт **Key Properties**. Если вы укажете, что степень доверия к этому ключу является *Полной (Complete)*, другие ключи, подписанные его владельцем, будут считаться действительными.
- **Чтобы отозвать ключ**, выделите его и выберите пункт **Revoke** из меню **Keys** в *PGPkeys*.
- **Имейте в виду, что новый интерфейс делает возможными многие вещи, которые раньше не были возможны** (или занимали слишком много времени). Это включает сертификацию одновременно нескольких ключей. Для этого, выделите все ключи, которые хотите подписать, и выберите **Sign** из меню **Keys**. Вы также можете удалять идентификаторы пользователя с ключей, удалять подписи, использовать перетаскивание мышкой для импорта связок ключей, на ходу управлять доверием и действительностью ключей. И так далее.

Мы надеемся, что новое поколение продуктов *PGP*, легких в использовании, вам понравится!

### Введение в PGP для Персональной приватности

Используя *PGP™* для *Персональной приватности*, вы легко сможете защитить приватность своих сообщений и файлов, шифруя их таким образом, чтобы только те, кому они предназначены, смогли их расшифровать. Вы можете также снабжать сообщения и файлы, которыми обмениваетесь, цифровой подписью, которая служит подтверждением того, что они пришли именно от того, кто обозначен в качестве отправителя, и что информация не была в пути изменена.

Самым удобным является использование *PGP* вместе с одним из популярных пакетов электронной почты, поддерживаемых посредством “встраиваемых модулей” (plug-ins). Это позволит вам шифровать, подписывать, расшифровывать и верифицировать сообщения во время отправки и чтения электронной почты. Кроме того, если вы переписываетесь с другим пользователем *PGP*, который также использует программу работы с электронной почтой, соответствующую стандарту *PGP/MIME*, вы можете выполнять все функции над сообщениями и присоединенными файлами, просто нажимая на кнопку во время отправки или получения почты.

Если вы используете пакет электронной почты, который не поддерживается посредством встраиваемых модулей, вы можете просто перенести текст сообщения в буфер обмена и осуществить необходимые преобразования над буфером. Вдобавок, если вам потребуется зашифровать или расшифровать целый присоединенный файл, вы можете выполнить это непосредственно из окна *Проводника (Explorer)*, выбрав соответствующий пункт контекстного (вызываемого щелчком правой кнопкой мыши) меню файла.

Вот некоторые из характеристик *PGP*:

- Пользующаяся широким признанием технология шифрования и расшифровки, применяющая наиболее сильные криптографические алгоритмы
- Технология наложения и верификации цифровой подписи для сертификации сообщений и файлов
- Быстрый доступ ко всем функциям посредством простого выбора пунктов меню
- Интегрированная поддержка популярных пакетов электронной почты посредством дополнительных модулей
- Реализация стандарта *PGP/MIME*, позволяющего быстро шифровать и расшифровывать сообщения и файлы при отправке и приеме почты
- Простая генерация ключей длиной до 4096 бит и поддержка различных форматов ключей (*RSA* и *DSS/Diffie-Hellman*)
- Развитая система управления ключами с графической репрезентацией свойств ключей
- Интегрированная поддержка распространения и поиска открытых ключей на серверах ключей

*Примечание:* Если вы используете версию *DSS/Diffie-Hellman*, она не будет генерировать ключей с использованием алгоритма *RSA*, а также не сможет шифровать, расшифровывать, подписывать и верифицировать подпись с помощью ключей, сгенерированных по этой технологии. Если вам необходимо генерировать *RSA*-ключи или другим образом использовать этот алгоритм, свяжитесь с тем, у кого вы приобрели свою копию программы *PGP*.

### Краткий обзор

*PGP* основана на широко распространенной технологии, известной как “криптография с открытыми ключами”, в которой для поддержания защищенной коммуникации используются два взаимодополняющих ключа. Один из ключей – закрытый, доступ к которому должны иметь только вы, а другой – открытый, который нужно свободно распространить среди пользователей *PGP*. Оба этих ключа, закрытый и открытый, хранятся в файлах, называемых “связками”, доступ к которым производится из окна программы *PGPkeys*. В этом окне выполняются все функции управления ключами.

Чтобы отправить кому-либо приватное почтовое сообщение, вы используете для шифрования копию открытого ключа этого лица. Расшифровать информацию с использованием своего закрытого ключа сможет только он. И наоборот, когда кто-нибудь захочет отправить зашифрованное послание вам, он использует копию вашего открытого ключа. Расшифровать это послание сможете только вы, так как только вы обладаете доступом к своему закрытому ключу.

Вы можете также использовать свой закрытый ключ для наложения на отправляемые сообщения цифровой подписи. Получатель затем использует копию вашего открытого ключа для проверки того, действительно ли сообщение отправлено именно вами, и не претерпело ли оно в дороге каких-либо изменений. Когда кто-либо отправляет вам почту со своей цифровой подписью, вы используете копию его открытого ключа для верификации подписи, показывающей, что сообщение никем не изменено.

Используя программу *PGP*, вы с легкостью можете создавать ключи, управлять ими и осуществлять доступ к функциям шифрования, расшифровки, а также наложения и верификации подписи на сообщениях и файлах.

Следующий раздел коротко описывает все процедуры, которым вам нужно следовать в процессе использования *PGP*. За деталями, касающимися любой из этих процедур, обращайтесь к соответствующим главам этой книги, где они объяснены исчерпывающим образом.

### Генерация пары из закрытого и открытого ключей

До того, как начать использовать *PGP*, вам нужно сгенерировать пару ключей, состоящую из закрытого, доступ к которому должны иметь только вы, и открытого, который вы можете свободно копировать и делать доступным для всех, с кем общаетесь электронной почтой. Вам будет предложено создать пару ключей непосредственно после того, как вы закончили установку *PGP*. Вы также можете сделать это в любое время из окна программы *PGPkeys*.

## Обмен ключами между пользователями

После генерации пары ключей, вы можете начать защищенную переписку с другими пользователями *PGP*. Для этого вам нужны копии их открытых ключей, а им – копия вашего открытого ключа. Так как открытый ключ может быть представлен в виде фрагмента текста, обмениваться ключами совсем просто. Вы можете вставить этот фрагмент текста в сообщение электронной почты, передать в виде файла или поместить на сервер открытых ключей, откуда каждый может его скопировать, как только в этом возникнет необходимость.

## Сертификация и верификация действительности ключей

Получив копию чье-либо открытого ключа, вы можете добавить его на свою связку открытых ключей. Затем вы должны убедиться, что ключ не был подделан, и что он действительно принадлежит его номинальному владельцу. Сделать это вы можете, сравнив уникальный “отпечаток” своей копии его ключа с “отпечатком” оригинальной копии. После того, как вы убедитесь в действительности ключа, вы подписываете его, чтобы дать *PGP* знать, что вы считаете безопасным его использование. Кроме того, вы можете указать степень доверия, которую испытываете к владельцу ключа, в смысле его способности ручаться за подлинность ключей третьих лиц.

## Шифрование сообщений и файлов и наложение подписи

После того, как вы сгенерировали свою пару ключей и обменялись открытыми ключами с другими пользователями, вы можете начать использовать шифрование и цифровую подпись при отправке сообщений и файлов.

- Если вы используете пакет электронной почты, поддерживаемый посредством дополнительных модулей, вы можете шифровать и подписывать сообщения, щелкая мышью на соответствующих кнопках панели инструментов этого пакета. Кроме того, если вы переписываетесь с другими пользователями *PGP*, которые применяют версию, соответствующую стандарту *PGP/MIME*, вы можете шифровать и подписывать сообщения автоматически при их отправке.
- Если ваш пакет электронной почты не поддерживается *PGP* посредством дополнительных модулей, вы можете скопировать сообщение в буфер обмена и выполнить соответствующие функции над его содержимым. Если вы хотите присоединить к сообщению какой-либо файл, вы можете зашифровать и подписать его в окне *Проводника (Explorer)* до того, как присоединять к сообщению.

## Расшифровка и верификация подписи на сообщениях и файлах

Когда вы получаете от кого-либо зашифрованную почту, вы можете расшифровать сообщение и верифицировать сопровождающую его подпись, чтобы убедиться, что данные исходят от номинального отправителя, и что они не претерпели изменения.

- Если вы используете пакет электронной почты, поддерживаемый посредством дополнительных модулей, вы можете расшифровать сообщение и верифицировать подпись, щелкая мышью на

соответствующих кнопках панели инструментов этого пакета. Кроме того, если вы переписываетесь с другими пользователями *PGP*, которые применяют версию, соответствующую стандарту *PGP/MIME*, вы можете расшифровывать сообщения и верифицировать подпись автоматически при их чтении.

- Если ваш пакет электронной почты не поддерживается *PGP* посредством дополнительных модулей, вы можете скопировать сообщение в буфер обмена и выполнить соответствующие функции над его содержимым. Если вы хотите расшифровать присоединенный файл или верифицировать подпись на нем, вы можете сделать это в окне *Проводника (Explorer)*

## Об этом Руководстве

Это Руководство организовано следующим образом

### Глава 1. Введение в PGP для Персональной приватности

- Описывает назначение программы, вводит понятия криптографии с открытыми ключами и цифровой подписи и содержит краткий обзор использования программы.

### Глава 2. Приступая к работе

- Описывает по шагам установку и запуск программы с кратким обсуждением ее главных компонентов и основных функций.

### Глава 3. Генерация и распространение ключей

- Объясняет, как сгенерировать пару из закрытого и открытого ключей и описывает способы обмена ключами, их защиты и аутентификации.

### Глава 4. Отправка и получение приватной электронной почты

- Объясняет, как отправлять и получать сообщения и присоединенные файлы в зависимости от конкретного пакета электронной почты, который используется вами и вашими партнерами по переписке.

### Глава 5. Управление ключами и установка предпочтений

- Объясняет, как исследовать и изменять атрибуты ключей, и как устанавливать пользовательские предпочтения в *PGP*.

### Глава 6. Особенности модели безопасности и уязвимые места

- Эта глава написана Филом Зиммерманном и описывает основные понятия шифрования с открытыми ключами, а также исследует некоторые уязвимые места модели безопасности, реализованной *PGP*.

## Глава 2 Приступая к работе

В этой главе объясняется, как запустить *PGP*, и приводится краткий обзор процедур, которым вам нужно будет следовать в процессе использования программы. Основываясь на этой информации, вы получите достаточно хорошее представление о том, как использовать *PGP*. Это будет особенно полезно для тех, кто не хочет читать все Руководство до того, как приступить к использованию программы.

### Системные требования

- Windows 95 или NT
- 8 МВ оперативной памяти
- 15 МВ свободного дискового пространства

### Совместимость с другими версиями

После того, как в 1991 году *PGP* была выпущена Филом Зиммерманном в качестве бесплатного продукта, она прошла через множество изменений, а количество находящихся в использовании копий превысило 2 миллиона. Хотя настоящая версия *PGP* в значительной степени переделана и использует совершенно новый пользовательский интерфейс, при ее разработке предусмотрена совместимость с предшествующими версиями *PGP*. Это означает, что вы можете обмениваться защищенной электронной почтой с теми, кто продолжает использовать более ранние версии программы<sup>3</sup>:

- *PGP 2.6* (Выпущена *MIT*)
- *PGP 4.0* (Выпущена *Viacrypt*)
- *PGP 4.5* (Выпущена *PGP, Inc.*)

Кроме нового пользовательского интерфейса и других усовершенствований, особенностью этой версии, отличающей ее от предшествующих, является возможность генерации ключей нового типа. Кроме ключей *RSA*, использовавшихся в предыдущих версиях, *PGP* предоставляет вам возможность использовать ключи, основанные на технологии шифрования и цифровой подписи *DSS/Diffie-Hellman*. Хотя использование таких ключей предлагается в качестве альтернативы традиционным ключам *RSA*, вы можете пользоваться ими только если обмениваетесь электронной почтой с пользователями работающей с ними версии. Учитывая то, что переход к широкому использованию ключей *DSS/Diffie-Hellman* потребует некоторого времени, вам, возможно, стоит зарезервировать пару ключей *RSA* для того, чтобы продолжать переписываться с теми, кто использует более ранние версии *PGP*.

Если вы шифруете сообщение сразу нескольким получателям, из которых одни обладают *RSA*-ключами, а другие – *DSS/DH*-ключами, сообщение

---

<sup>3</sup> Это относится и к "международным релизам" *PGP (2.xi)*, используемым за пределами США.

будет зашифровано соответствующим ключом для каждого получателя. Однако, чтобы прочитать такое “смешанное” сообщение, пользователи более ранних версий *PGP* должны произвести соответствующую модернизацию своей программы<sup>4</sup>.

Еще одно дополнение, внесенное в новую версию *PGP* – это реализация стандарта *PGP/MIME* для некоторых дополнительных модулей, которые интегрируют функции *PGP* прямо в популярные пакеты электронной почты. Если вы используете один из таких пакетов, вы сможете шифровать и расшифровывать сообщения, а также накладывать и верифицировать подпись автоматически при отправке или получении почты. Однако, отправка электронной почты в стандарте *PGP/MIME* тем, кто использует пакет, не поддерживающий этот стандарт, может привести к неудобствам для получателя.

### Модернизация предыдущей версии

Если вы модернизируете предыдущую версию *PGP* (выпущенную *PGP, Inc.* или *Viacrypt*), возможно, вам потребуется удалить старую версию до установки новой, чтобы освободить место на диске. Будьте осторожны, и **не удалите при этом связки закрытых и открытых ключей!** На этих связках хранятся все ключи, которые вы сгенерировали и собрали за время использования предыдущей версии программы. Когда вы устанавливаете *PGP*, вам предоставляется возможность сохранить существующие файлы связок закрытых и открытых ключей, чтобы потом не импортировать их отдельно. Для модернизации предыдущей версии следуйте нижеизложенным процедурам.

#### Модернизация PGP 2.6.2 (MIT Freeware)<sup>5</sup>

1. Убедитесь, что вы закрыли все программы, запущенные на компьютере.
2. Найдите связки закрытых и открытых ключей и сделайте их резервные копии на другом диске. Связка открытых ключей хранится в файле “pubring.pgp”, связка закрытых – в “secring.pgp”.

*Примечание:* Для вящей сохранности лучше сделать по две резервных копии связок ключей на двух флоппи-дисках. Особую осторожность следует проявить в отношении связки закрытых ключей: ведь если вы ее потеряете, вы уже никогда не сможете расшифровать ни одного сообщения или файла, зашифрованного с помощью соответствующего открытого ключа. Сохраните связки ключей в надежном месте, где никто, кроме вас, не получит к ним доступа.

3. После того, как копии старых связок сделаны, удалите или заархивируйте старую программу *PGP 2.6.2*. Вы можете сделать это двумя способами:
  - удалив ручную папку “PGP262” со всем ее содержимым;
  - удалив ручную файл “pgp.exe” и заархивировав остальные файлы, особое внимание уделив файлам связок и “config.txt”.

<sup>4</sup> Пользователи **PGP 2.6.2** должны перейти к использованию **PGPfreeware, Version 5.0**; пользователи **4.0** – к **4.0.1**; пользователи **4.5** – к **4.5.1** (см. *PGP 5.0 for Windows Technical FAQ*).

<sup>5</sup> Модернизация версии **PGP 2.6.xi**, используемой за пределами США, производится аналогичным образом.

*Примечание:* Если у вас установлена модернизированная версия *PGP264* от MIT, ваша старая программа *PGP 2.6.x* сможет работать с *RSA*-ключами на связках ключей в формате *5.0* и не собьется, встретив ключ *DSS/DH*.

4. Установите *PGP 5.0*, запустив полученный исполняемый модуль.
5. Когда программа установки спросит, есть ли у вас связки ключей, ответьте утвердительно (щелкните на кнопке **Yes**), укажите местоположение ваших старых связок и следуйте инструкциям для того, чтобы скопировать эти ключи на ваши новые связки в формате *5.0*.
6. Перезагрузите компьютер.

#### Модернизация PGPmail 4.0

Выполните те же процедуры, что и *PGP 2.6.2 (ViaCrypt PGP)* нужно удалить и/или заархивировать вручную). Обязательно сделайте резервные копии связок. Прочитайте также файл "ReadMe" для *PGP 4.0.1* для DOS и UNIX, который описывает модернизацию этой версии для того, чтобы она могла работать со связками *PGP 5.0*.

#### Модернизация PGPmail 4.5

1. Убедитесь, что вы закрыли все программы/процессы, запущенные на компьютере.
2. Завершите процесс *PGP Enclyptor* (*enclrypt\_32.exe*), который, возможно, выполняется (с тем, чтобы исполняемый файл мог быть удален).

Для того, чтобы определить, запущен ли *Enclyptor*, поищите его окно или минимизированный значок на Панели задач. В качестве альтернативного метода, вы можете нажать *Control+Alt+Delete*, и в появившемся окне выбрать процесс *The Enclyptor* и щелкнуть на кнопке **Завершить задачу (End Task)**.

3. Откройте в меню Пуск (Start) пункт Установки|Панель управления (Settings|Control Panel).
4. Два раза щелкните на Установить/Удалить Программы (Add/Remove Programs).
5. Выберите пункт **PGPmail 4.5**.
6. Щелкните на кнопке **Установить/Удалить (Add/Remove)**. Позвольте программе удаления автоматически удалить все файлы и очистить параметры Реестра.

*Примечание:* Если во время процесса удаления вам будет задан вопрос, нужно ли удалять файлы ".dll", ответьте утвердительно. При установке *PGP 5.0* будут установлены последние версии этих файлов.

7. Нажмите **ОК** для завершения удаления, и после завершения закройте окно.
8. Установите *PGP 5.0*, запустив полученный исполняемый модуль. Рекомендуется, хотя это и не обязательно, установить программу в папку по умолчанию.
9. Когда программа установки спросит, есть ли у вас связки ключей, ответьте утвердительно (щелкните на кнопке **Yes**), укажите местоположение ваших старых связок и следуйте инструкциям для того, чтобы скопировать эти ключи на ваши новые связки в формате *5.0*.
10. Перезагрузите компьютер.



### Модернизация бета-версий PGP 5.0

1. Убедитесь, что вы закрыли все программы/процессы, запущенные на компьютере.
2. Завершите процесс *PGPTray*, который, возможно, исполняется (с тем, чтобы исполняемый файл мог быть удален).  
Для того, чтобы определить, запущен ли “*PGPTray.exe*”, найдите его минимизированный значок на Области индикаторов Панели задач в виде маленького “конвертика”. Для завершения программы нажмите на этот значок и в самом низу открывшегося меню выберите пункт **Quit PGPTray**. Вы можете также нажать **Control+Alt+Delete**, и в появившемся окне выбрать процесс *pgptray* и щелкнуть на кнопке **Завершить задачу (End Task)**.
3. Откройте в меню Пуск (Start) пункт Установки|Панель управления (Settings|Control Panel).
4. Два раза щелкните на Установить/Удалить Программы (Add/Remove Programs).
5. Выберите пункт **PGP 5.0bNN**.
6. Щелкните на кнопке Установить/Удалить (Add/Remove).

*Примечание:* Если во время процесса удаления вам будет задан вопрос, нужно ли удалять файлы “.dll”, ответьте утвердительно. При установке *PGP 5.0* будут установлены последние версии этих файлов.

7. Нажмите **ОК** для завершения удаления, и после завершения закройте окно.
8. Установите *PGP 5.0*, запустив полученный исполняемый модуль. Рекомендуется, хотя это и не обязательно, установить программу в папку по умолчанию.
9. Когда программа установки спросит, есть ли у вас связки ключей, ответьте утвердительно (щелкните на кнопке **Yes**), укажите местоположение ваших старых связок и следуйте инструкциям для того, чтобы скопировать эти ключи на ваши новые связки в формате *5.0*.
10. Перезагрузите компьютер.  
Теперь вы можете запускать новую программу *PGP 5.0*!

### Установка PGP

Для установки PGP с компакт-диска

1. Запустите Windows
2. Вставьте компакт-диск
3. Запустите программу Setup
4. Следуйте указаниям программы установки

Для установки PGP с Web-сервера PGP, Inc.

1. Подгрузите программу *PGP* на свой жесткий диск
2. Щелкните два раза на значке программы инсталляции *PGP*
3. Следуйте указаниям программы установки

### Запуск PGP

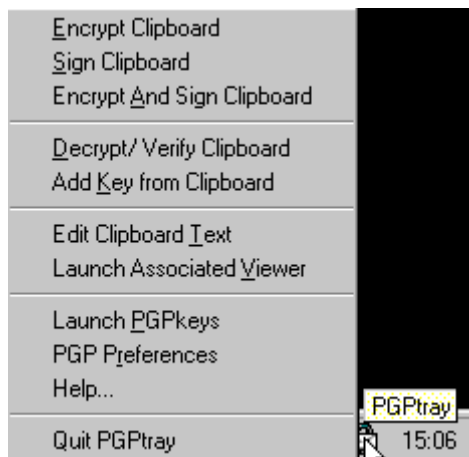
*PGP* работает с данными, генерируемыми другими приложениями, а соответствующие функции *PGP* разработаны таким образом, чтобы они

были непосредственно доступны из приложения, с которым вы в данный момент работаете. Существует три основных способа запуска *PGP*:

- из Области индикаторов Панели задач;
- из поддерживаемого пакета электронной почты;
- из меню **Файл (File) Проводника (Explorer)**.

### Запуск из Области индикаторов Панели задач

Вы можете выполнить большинство основных функций, вызвав меню щелчком на значке, обычно расположенном в Области индикаторов Панели задач (если этого значка нет<sup>6</sup>, следует запустить **PGPtray** из меню **Пуск (Start)**), и выбрав соответствующий пункт.



### Выполнение функций PGP над содержимым Буфера обмена

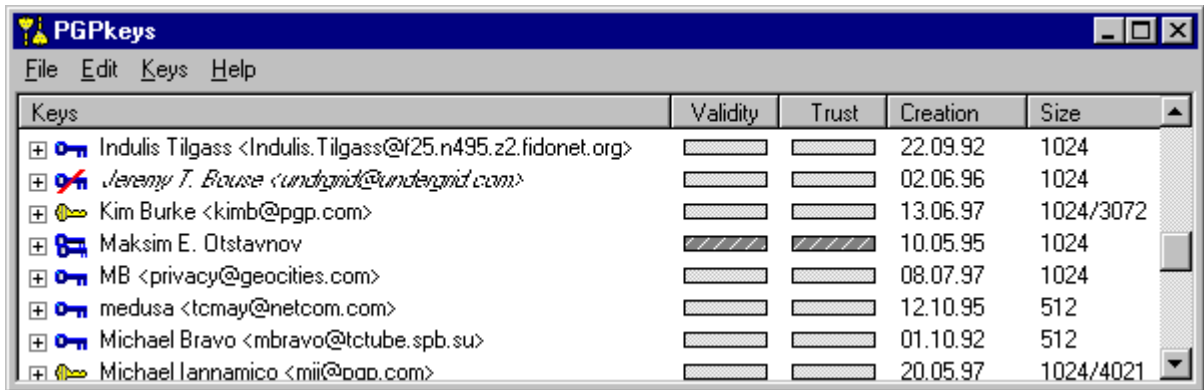
Вы заметите, что многие из пунктов этого меню относятся к функциям *PGP*, выполняемым над содержимым Буфера обмена. Если вы используете пакет электронной почты, который не поддерживается *PGP* с помощью дополнительных модулей, или вы работаете с текстом, сгенерированным каким-то другим приложением, функции шифрования/расшифровки и наложения/верификации подписи выполняются посредством Буфера обмена.

Например, для того, чтобы зашифровать или подписать текст, вы копируете его из окна приложения в Буфер обмена, выполняете над ним соответствующие функции, а затем вклеиваете его назад в окно приложения до того, как отправить получателю. Когда вы получаете зашифрованное или подписанное сообщение, вы просто выполняете этот процесс в обратном порядке: копируете сообщение в Буфер обмена, выполняете над ним соответствующие операции, а затем просматриваете содержимое Буфера. Просмотрев сообщение, вы решаете, стоит ли его сохранить в расшифрованном виде, или хранить лишь в зашифрованном.

### Запуск PGPkeys

Выбрав из меню **PGPTray** пункт **Launch PGPkeys**, вы открываете окно *PGPkeys*, в котором представлены пары ваших открытых/закрытых ключей, а также все открытые ключи, которые есть у вас на связках. (Если вы еще не создали себе пару ключей, *Мастер ключей (PGP Key Wizard)* проведет вас через необходимый для ее создания процесс. Однако, прежде чем начать генерацию ключей, вам нужно прочитать Главу 3, где подробно рассказано о различных опциях их создания.

<sup>6</sup> Этот значок присутствует, если программа *PGPTray* включена в меню **Автозапуск (Startup)** или запущена вручную.

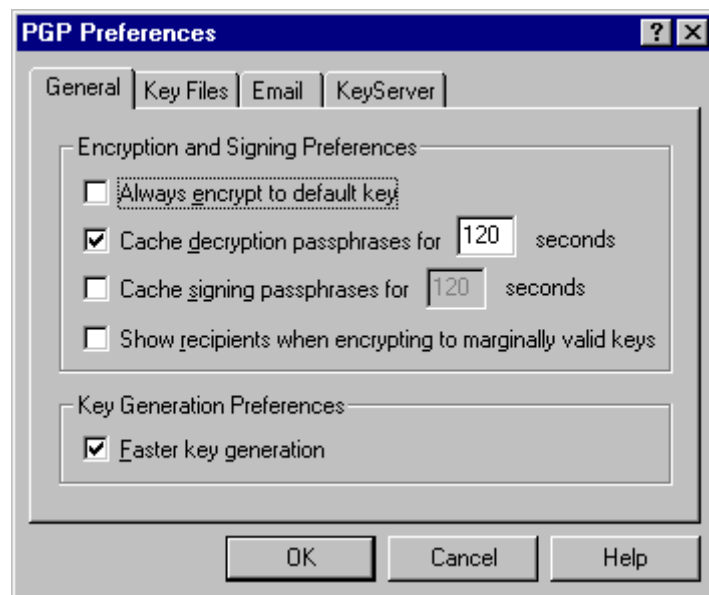


В окне *PGPkeys* вы можете создавать новые пары ключей и управлять всеми ключами, находящимися на ваших связках. Например, именно здесь вы можете исследовать атрибуты каждого ключа, указывать степень уверенности в том, что ключ действительно принадлежит номинальному владельцу, и степень доверия к владельцу ключа в отношении его способности быть поручителем за подлинность ключей других лиц. За полным разъяснением функций управления ключами, доступных из окна *PGPkeys*, обращайтесь к Главе 5.

### Установка предпочтений

Выбрав из меню **PGPtray** пункт **PGP Preferences**, вы открываете окно диалога *Предпочтения (Preferences)*, в котором указываются различные параметры, влияющие на работу *PGP*.

Выбрав соответствующую закладку, вы можете перейти к установке тех предпочтений, которые вы хотите изменить. За полным разъяснением установок предпочтений обращайтесь к Главе 5.



### Получение справки

Выбрав из меню **PGPtray** пункт **Help**, вы открываете систему помощи *PGP*, которая содержит общий обзор программы и инструкции к выполнению всех процедур. Многие диалоги также снабжены кнопкой вызова контекстно-зависимой справки, на которой можно щелкнуть, а затем указать курсором на интересующую вас область экрана для получения краткого пояснения.

### Выход из PGP

По умолчанию, программа *PGP* запускается всякий раз при загрузке *Windows*, что индицируется значком в Области индикаторов Панели задач. Если по какой-то причине вам нужно завершить работу *PGP*, вы можете сделать это, выбрав пункт **Quit PGP** из меню **PGPtray**.

## Запуск PGP из поддерживаемых пакетов электронной почты

Если вы пользуетесь одним из популярных пакетов электронной почты, поддерживаемых *PGP* с помощью дополнительных модулей, вы можете вызывать необходимые функции *PGP* простым щелчком на соответствующих кнопках панели инструментов почтового пакета. Например, вы щелкаете на кнопке с замком, чтобы зашифровать сообщения, или – на кнопке с пером, чтобы подписать его.

Когда вы получаете сообщение от другого пользователя *PGP*, вы расшифровываете его или верифицируете подпись щелчком на значке с открытым конвертом.



Кнопка с ключом и конвертом позволяет добавить все ключи, содержащиеся в сообщении, на вашу связку. Кроме того, вы можете в любой момент открыть окно *PGPkeys* щелчком на кнопке с двойным ключом.

Если вы пользуетесь пакетом электронной почты, для которого существует дополнительный модуль поддержки стандарта *PGP/MIME*, и переписываетесь с пользователем, чей пакет электронной почты также поддерживает этот стандарт, вы можете шифровать и расшифровывать сообщения и файлы, а также подписывать их и верифицировать подпись автоматически при приеме и отправлении почты. Все, что для этого нужно сделать – это включить соответствующие функции в диалоге установки предпочтений *PGP*.

Когда вы получаете почту, зашифрованную или подписанную в стандарте *PGP/MIME*, она отображается в виде значка, указывающего на тип сообщения *PGP/MIME*.

```
X-Sender: mji@mail.pgp.com (Unverified)
X-Mailer: QUALCOMM Windows Eudora Pro Version 3.0.2 b4 (32)
Date: Wed, 21 May 1997 10:02:32 -0700
To: mji@pgp.com
From: Mike Iannamico <mji@pgp.com>
Subject: test
```

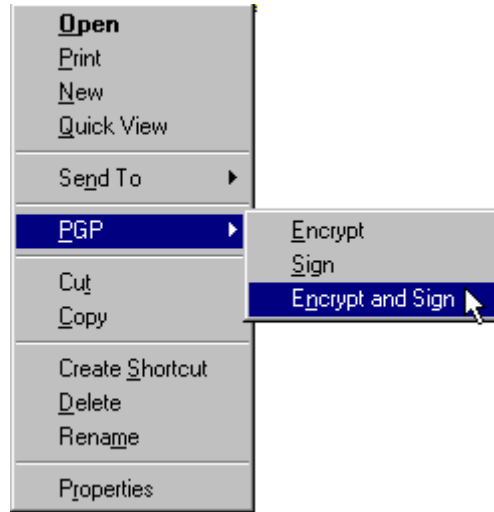


Decrypt PGP/MIME Message

Все, что вам в таком случае нужно сделать для расшифровки или верификации подписи – это два раза щелкнуть на значке с открытым конвертом.

### Запуск PGP из Проводника

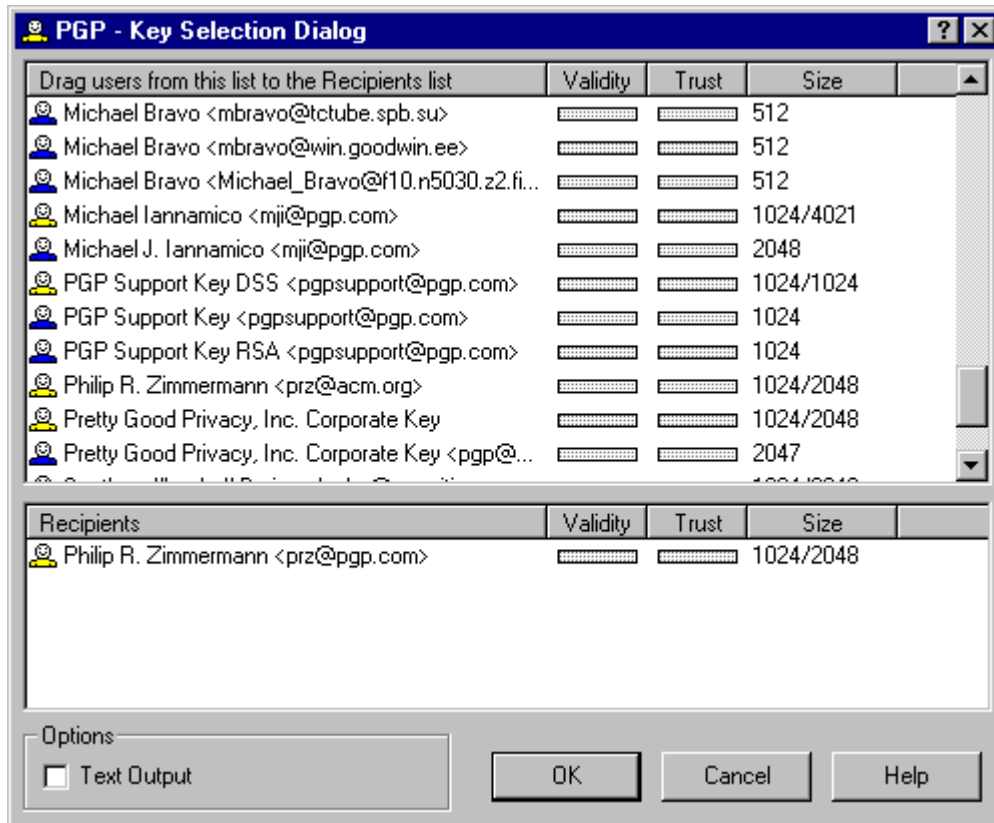
Вы можете шифровать и расшифровывать, а также верифицировать и накладывать подпись на файлы (например, документы текстовых процессоров, электронные таблицы, видеоклипы) непосредственно из окна *Проводника (Explorer)*. Если вы используете пакет электронной почты, который не поддерживает стандарт *PGP/MIME*, вы должны использовать этот метод для шифрования присоединяемых к почтовым сообщениям файлов. В некоторых случаях, вам даже может понадобиться шифровать и расшифровывать файлы, хранящиеся на вашем собственном компьютере для предотвращения доступа посторонних к их содержанию. Для вызова функций *PGP* из *Проводника*, выберите соответствующий пункт подменю **PGP** меню **File**.



Опции, которые при этом доступны, зависят от качества помеченного в данный момент файла. Если файл еще не зашифрован и не подписан, будут доступны эти функции. Если файл уже зашифрован или подписан, будут доступны функции расшифровки и верификации подписи.

### Выбор получателей

Когда вы отправляете почту кому-либо, чей пакет электронной почты поддерживается посредством дополнительных модулей, почтовый адрес получателя определяет, какой ключ будет использован для шифрования. Однако, если вы ввели имя или адрес, которым не соответствует ни один ключ на связке открытых ключей, или вы шифруете содержимое Буфера обмена, или запускаете *PGP* из *Проводника*, вы должны вручную выбрать открытый ключ из *Окна диалога выбора ключа (PGP Key Selection Dialog box)*.



Для того, чтобы выбрать открытые ключи получателей, вам нужно лишь перетащить значки, представляющие их, в список *Получатель (Recipient)* и щелкнуть на кнопке **ОК**. За полными инструкциями, касающимися шифрования, расшифровки, наложения и верификации подписи, обращайтесь к Главе 4.

### Сокращения и горячие клавиши

Вы увидите, что использовать *PGP* совсем просто. Для того, чтобы ее функции можно было выполнять еще быстрее, предусмотрен ряд сокращений и “горячих клавиш”, им соответствующих. Например, когда вы управляете своими ключами из окна *PGPkeys*, вы можете щелкнуть правой кнопкой мыши и получить доступ ко всем необходимым функциям, не обращая к строке меню. Вы также можете перетащить файл, содержащий ключ, в окно *PGPkeys*, чтобы добавить его к своей связке. Для большинства операций, доступных из меню, также предусмотрены “горячие клавиши”, состоящие из **Ctrl** и еще одной клавиши. Эти сокращения показаны во всех меню *PGP*, и их использование описано в соответствующем контексте в главах настоящего Руководства.

## Глава 3

### Генерация и распространение ключей

В этой главе описывается, как сгенерировать пары закрытых и открытых ключей, необходимые для того, чтобы переписываться с другими пользователями *PGP*. Также объясняется, как распространить открытый ключ и получить открытые ключи других пользователей, чтобы вы смогли начать обмениваться защищенной и подписанной почтой.

#### Основные понятия

*PGP* основывается на широко распространенной и получившей достаточное признание системе “шифрования с открытым ключом”, в соответствии с которой вы, так же, как и другие пользователи *PGP* генерируете пару ключей, состоящую из закрытого и открытого ключей. Закрытый ключ, как и следует из его названия, доступен только вам. Но для того, чтобы вы смогли общаться с другими пользователями *PGP*, вам нужны копии их открытых ключей, а им – копии вашего. Закрытый ключ вы используете для подписи сообщений и файлов, которые отправляете другим, а также для расшифровки сообщений и файлов, отправляемых вам. Открытые ключи других вы используете для шифрования почты, направляемой им, и для верификации их цифровой подписи.

*Примечание:* Даже тем, кого не слишком занимают технические подробности, возможно, интересно будет узнать, что с помощью системы шифрования с открытым ключом шифруется не само сообщение. Вместо этого, для шифрования данных используется намного более быстрый алгоритм шифрования с одним ключом, и именно этот ключ и шифруется с помощью открытого ключа получателя. Получатель затем использует свой закрытый ключ для расшифровки этого временного ключа, который дает ему возможность расшифровать данные.

Ваш закрытый ключ также используется для наложения подписи на содержимое сообщения или файла. Любой, обладающий копией вашего открытого ключа может верифицировать вашу цифровую подпись и удостовериться в том, что содержимое не было изменено во время передачи. Аналогично, если у вас есть копия открытого ключа отправителя, вы можете верифицировать его цифровую подпись или проверить целостность посланного вам сообщения..

Настоящая версия *PGP* поддерживает два различных типа ключей: ставшие традиционными ключи *RSA*, использовавшиеся в предыдущих версиях, и ключи нового типа, называемые ключами *DSS/DH*, которые базируются на последних достижениях криптографии. Если вы собираетесь обмениваться почтой с теми, кто использует версию *PGP for Personal Privacy 5.0*, или более позднюю, вы можете воспользоваться всеми преимуществами новых ключей *DSS/DH*. Если же вы переписываетесь с пользователями предыдущих версий *PGP*, для общения с ними вам нужно пользоваться традиционными *RSA*-ключами.

*Примечание:* Если вы ранее пользовались *PGP*, вы, вероятно, уже сгенерировали пару ключей и сообщили открытый ключ тем, с переписываетесь. В этом случае вам не нужно выполнять процедуру

генерации новой пары ключей (описанную в следующем разделе). Вместо этого, во время установки программы укажите местоположение ваших ключей, и вы увидите их, открыв окно *PGPkeys*. Если у вас уже есть ключи, но вы не указали их местоположение во время установки, вы можете перейти на страницу Key Files в окне диалога Preferences программы *PGPkeys*, и ввести путь к существующим файлам с ключами.

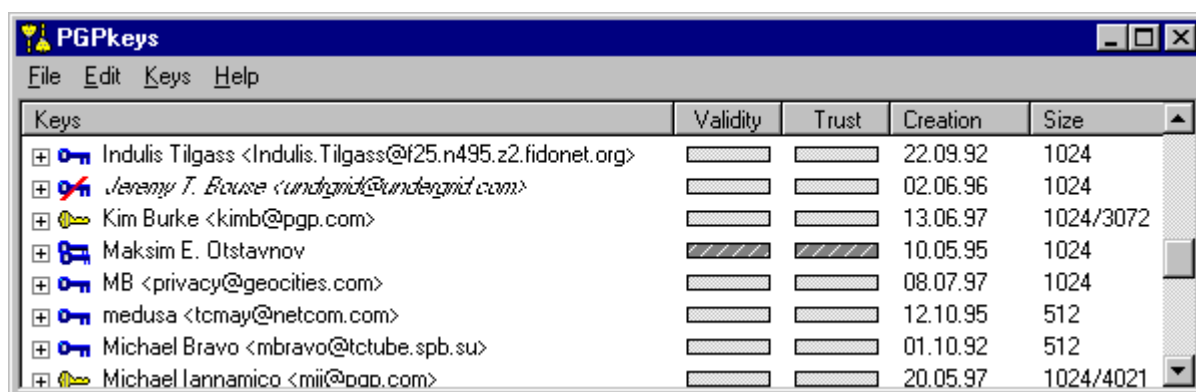
### Генерация пары ключей

Если вы не сгенерировали пару ключей, используя предыдущую версию *PGP*, ее генерация – это первая процедура, которую нужно выполнить до того, как вы сможете использовать программу для отправки и приема защищенной и подписанной почты. Пара ключей состоит из закрытого ключа (доступ к которому имеет только вы) и открытого ключа (который вы свободно распространяете среди тех, с кем переписываетесь). Процедура генерации новой пары ключей осуществляется из окна *PGPkeys* с использованием Помощника генерации ключей (*PGP Key Wizard*), проводящего вас через этот процесс.

#### Генерация новой пары ключей

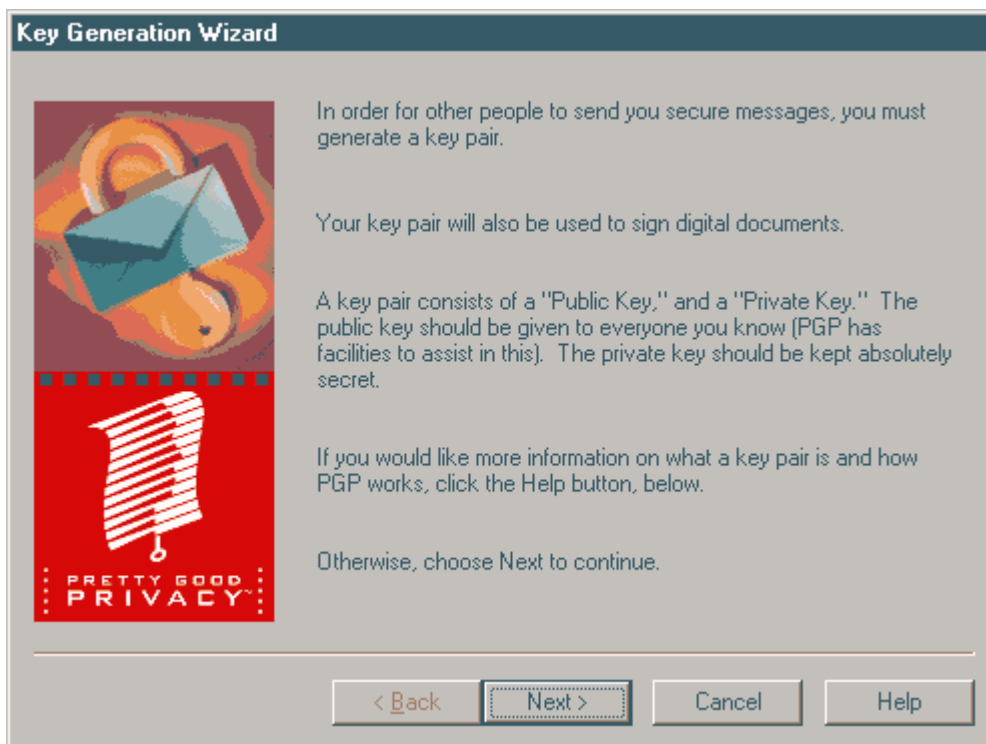
- Щелкните на кнопке **Пуск (Start)** и выберите пункт **PGPkeys** из подменю *PGP* меню **Программы (Programs)**, или щелкните на значке с конвертом и ключом в Области системных индикаторов (*System tray*) и выберите пункт **Launch PGPkeys**. Еще один способ запустить *PGPkeys* – это щелкнуть на значке с двумя ключами на панели инструментов пакета электронной почты.

После этого откроется окно *PGPkeys*.

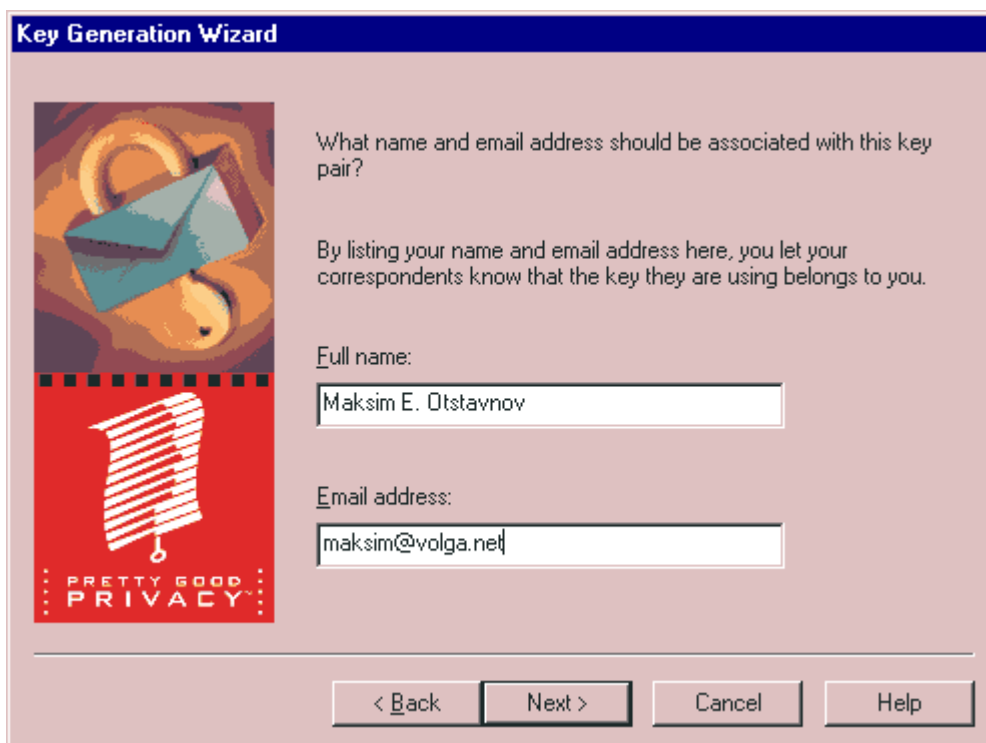


- Выберите из меню **Keys** пункт **New Key**.  
В первом окне Помощник генерации ключей приводит некоторую вводную информацию.





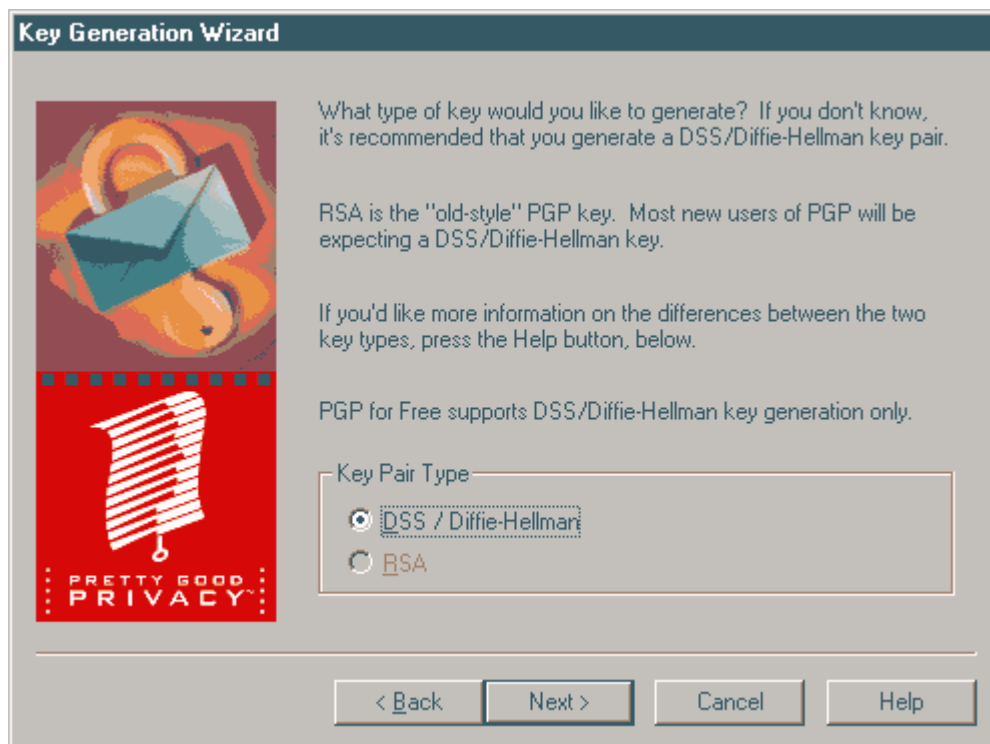
3. Прочитав содержимое первого окна, нажмите **Next** для перехода к следующему окну диалога. Помощник генерации ключей попросит вас ввести ваше имя и адрес электронной почты.



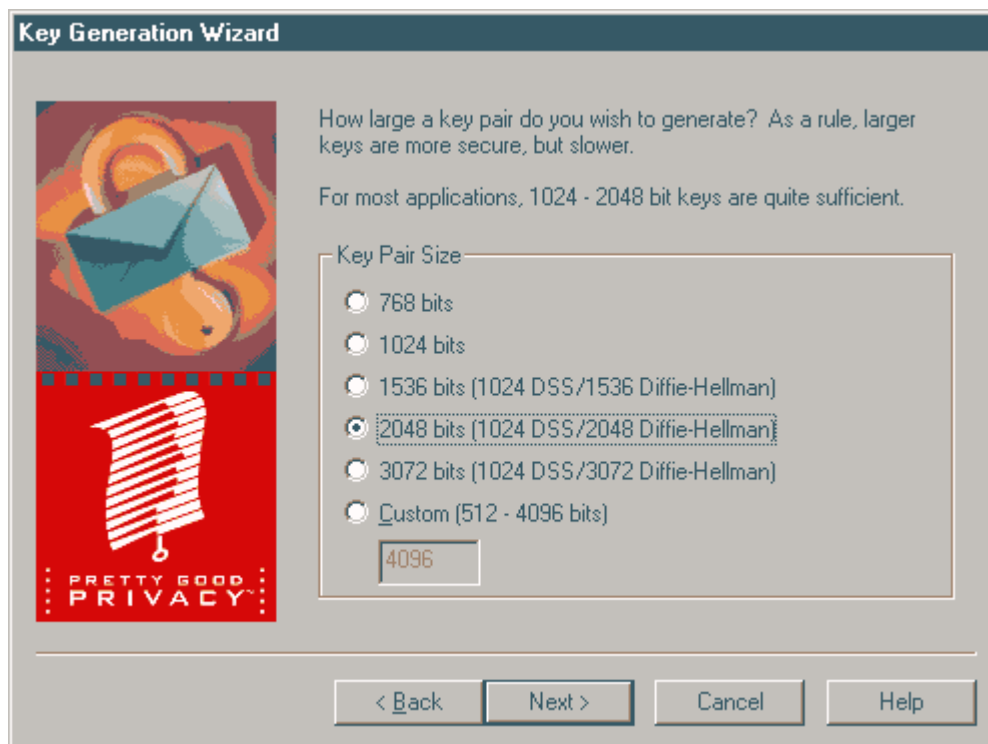
4. Введите ваше имя в первой строке и ваш адрес электронной почты – во второй. Совершенно необязательно вводить свое настоящее имя или даже адрес электронной почты. Однако, использование настоящего имени поможет другим опознать вас как владельца открытого ключа. Указание же

правильного адреса позволит вам и другим получить преимущества от возможностей встраиваемых модулей, которые будут автоматически искать на связке соответствующие ключи при отправке письма определенному адресату.

- Щелкните **Next** для перехода к следующему окну диалога. Помощник генерации ключей попросит вас указать тип ключа.



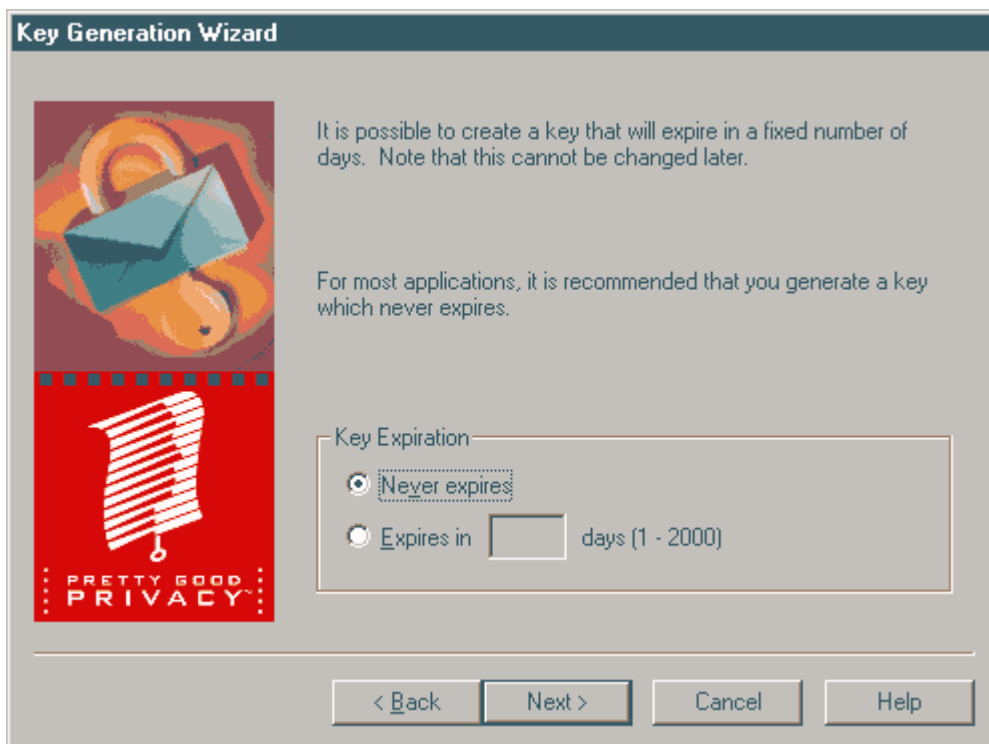
- Выберите тип ключа (*DSS/DH* или *RSA*).  
Прежние версии *PGP* использовали более старую технологию, известную как *RSA*. Начиная с этой версии *PGP* предоставляет вам возможность генерации и использования ключей, базирующихся на более передовой технологии *DSS/DH*.
  - Если вы планируете переписываться с теми, кто продолжает использовать старые *RSA*-ключи, вам нужно сгенерировать пару *RSA*-ключей, которая совместима с предыдущими версиями программы.
  - Если вы планируете переписываться с теми, кто использует новейшую версию *PGP*, вы можете воспользоваться преимуществами новой технологии и сгенерировать пару *DSS/ DH*-ключей.
  - Если вы хотите обмениваться почтой со всеми пользователями *PGP*, вам нужно сгенерировать как пару *RSA*-ключей, так и пару *DSS/ DH*-ключей, и затем использовать соответствующую пару в зависимости от версии *PGP*, используемой вашим партнером по коммуникации.
- Щелкните **Next** для перехода к следующему окну диалога. Помощник генерации ключей попросит вас указать длину ваших новых ключей.



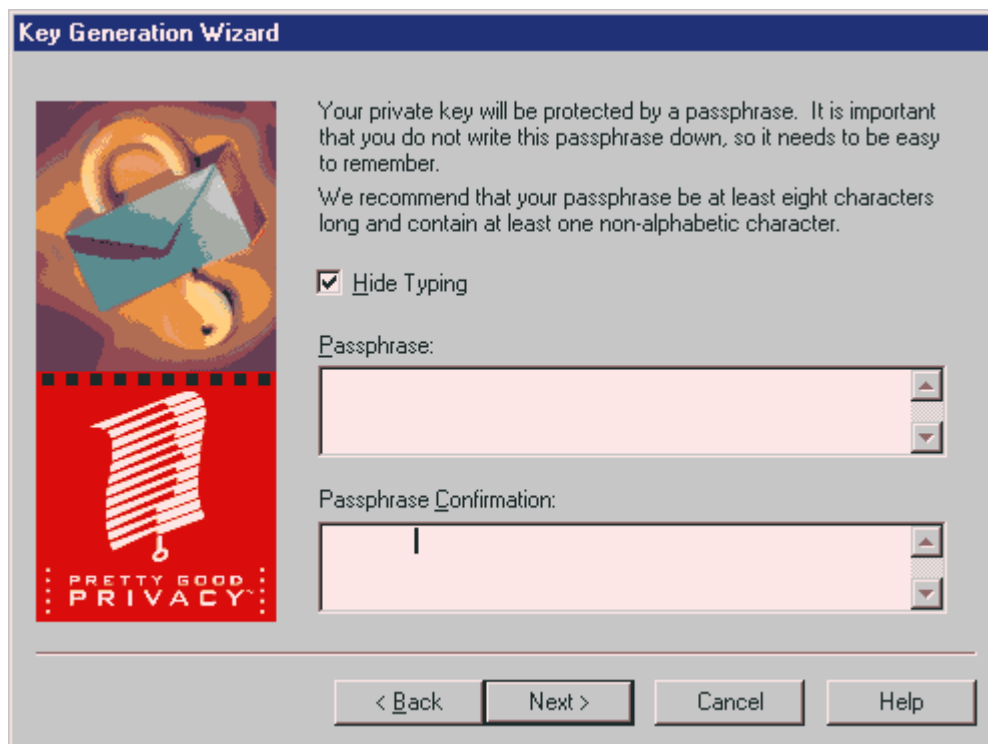
8. Выберите длину ключа из списка (от 768 до 3072 бит) или введите длину (от 512 до 4096 бит). Длина *RSA*-ключей ограничена 2048-ю битами для сохранения совместимости с предыдущими версиями *PGP*. Длина ключа соответствует количеству бит, используемых для генерации вашего ключа. Чем длиннее ключ, тем меньше шансов, что кто-либо когда-нибудь сумеет его взломать. Но чем длиннее ключ, тем дольше будет выполняться процесс шифрования и расшифровки. Вам нужно соблюдать баланс между удобством быстрого выполнения функций *PGP* при более коротком ключе и повышенным уровнем безопасности, обеспечиваемым более длинным ключом. Если вы не работаете с чрезвычайно ценной секретной информацией, в доступе к которой кто-либо может быть заинтересован настолько, чтобы предпринять очень дорогостоящую и долговременную атаку, длина ключа в 1024 бита будет достаточной.

*Примечание:* При генерации *DSS/DH*-ключей, длина компонента *DSS* (используемого при наложении и верификации цифровой подписи) принимает ряд дискретных значений. Ее длина меньше, чем длина компонента *DH* (используемого при шифровании и расшифровке), и ограничена 1024-мя битами.

9. Щелкните **Next** для перехода к следующему окну диалога. Помощник генерации ключей попросит вас указать дату, после которой пара ключей не должна использоваться.



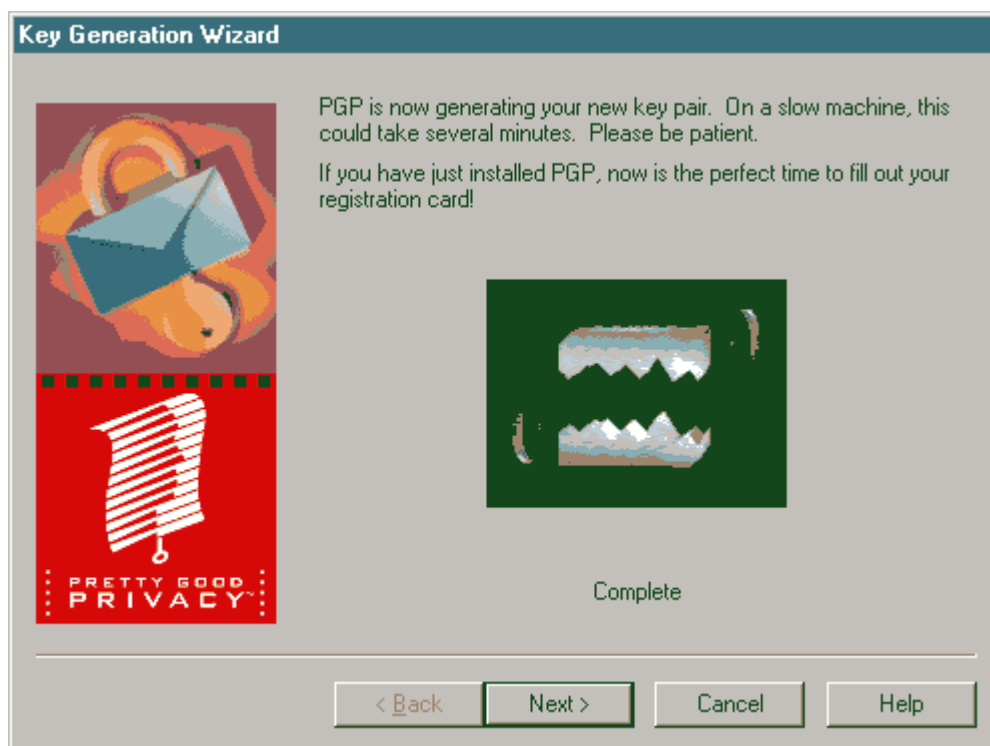
10. Укажите срок прекращения использования ключей. Вы можете сохранить выбор по умолчанию “никогда” (never), или указать конкретное количество дней, по истечении которых ключи станут недействительными.  
Обычно, сгенерировав пару ключей, (и распространив открытый ключ), вы так и будете с этого времени ее использовать. Однако, при определенных условиях, вам может понадобиться создать особый набор ключей, которые вы планируете использовать лишь в течение определенного периода времени. В этом случае, после того, как истечет указанный срок, открытый ключ уже не сможет быть использован для шифрования адресуемой вам почты, но им можно будет продолжать пользоваться для верификации вашей подписи. Точно так же, после истечения указанного срока закрытый ключ можно использовать для расшифровки направленной вам почты, но не для наложения подписи на почту, отправляемую другим.
11. Щелкните **Next** для перехода к следующему окну диалога. Помощник генерации ключей попросит вас ввести пароль.



12. В поле ввода *Пароль (Passphrase)* введите последовательность символов или слов, которую вы будете использовать для исключительного доступа к своему закрытому ключу. Для подтверждения вашего выбора, переместите курсор нажатием клавиши *Tab* на следующую строку и введите выбранный пароль еще раз. Обычно, для обеспечения лучшей безопасности, на экране не отображаются вводимые вами символы. Если вы, однако, уверены в том, что за вами никто не подглядывает, и хотите видеть вводимые вами символы пароля, снимите флажок в поле “Hide Typing”.

*Совет:* Пароль должен содержать несколько слов, и может включать пробелы, цифры и другие печатные символы. Придумайте что-нибудь, что вам легко запомнить, а другим – непросто отгадать, и помните, что в пароле строчные и заглавные буквы различаются. Чем длиннее ваш пароль, и чем шире набор символов, которые он содержит, тем он более надежен. Попробуйте включить равное количество строчных и заглавных букв, цифр, знаков препинания и т.п.

13. Щелкните **Next** для запуска процесса генерации ключей. Помощник генерации ключей покажет, что он занят генерацией новой пары ключей.

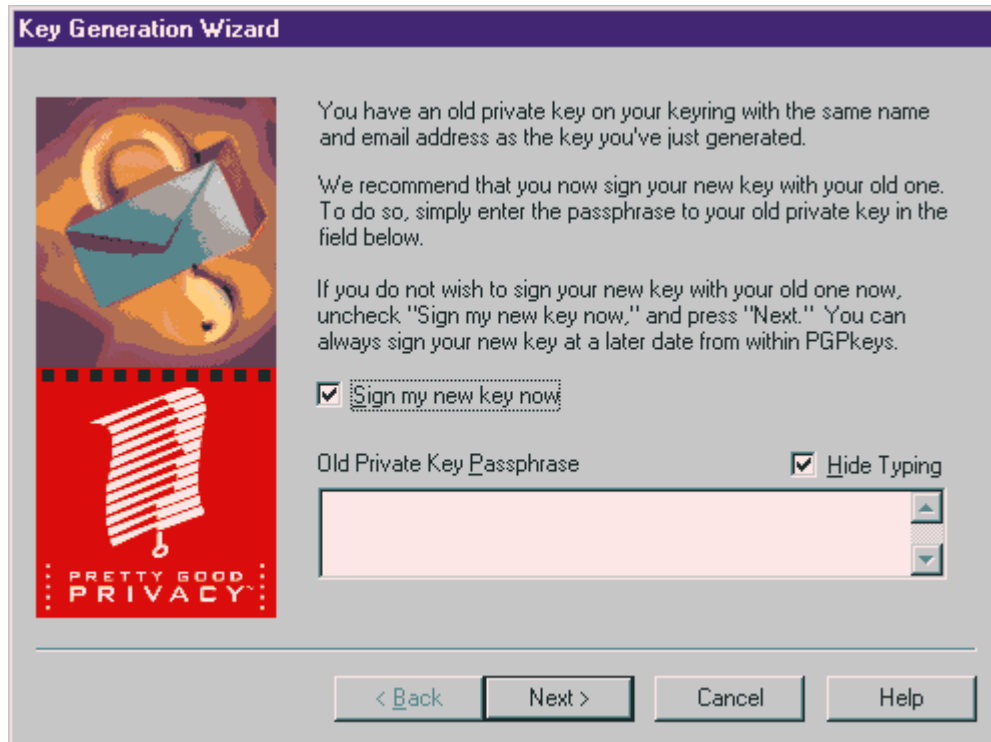


Если вы ввели неадекватный пароль, до запуска генерации ключей появится предупреждающее сообщение, и для продолжения вы должны либо подтвердить использование неудачного пароля, либо ввести новый пароль.

Если *PGP* не располагает достаточным для генерации ключа количеством случайных данных, появится диалог *Случайные данные (PGP Random Data)*. Как предлагается в тексте, поведите мышью и понажимайте клавиши клавиатуры, пока полоса индикации состояния в окне диалога не заполнится до конца. Движения мыши и нажатия клавиш генерируют случайную информацию, необходимую для создания уникальной пары ключей.

После запуска процесс генерации ключей может занять некоторое время. Если вы выберете нестандартную длину *DSS/DH*-ключа, опция “быстрой генерации” (*Fast Key Generation*) не будет задействована, и генерация может занять часы. Затем Помощник генерации ключей сообщит о завершении процесса.

- Щелкните **Next** для перехода к следующему окну диалога. Если вы создаете пару ключей с тем же именем и/или почтовым адресом, что и предыдущая, вам будет предоставлена возможность подписать новый ключ с помощью старого ключа. Когда кто-либо будет зацеплять ваш открытый ключ на свою связку, это придаст новому ключу тот же уровень действительности и доверия, что и старому. Действительность основывается на свидетельствах тех, кто подписал ваш предыдущий ключ, хотя эти подписи с нового ключа на старый и не переносятся.



15. Если это возможно и необходимо, подпишите ваш новый ключ с помощью старого и введите пароль старого ключа. Щелкните **Next**. Помощник генерации ключей укажет, что вы успешно сгенерировали новую пару ключей, и спросит, желаете ли вы отправить копию вашего нового открытого ключа на сервер открытых ключей.



16. Укажите, хотите ли вы отправить копию вашего нового открытого ключа на сервер открытых ключей и щелкните Next.

Отправив открытый ключ на сервер, вы делаете его доступным для любого, кому он понадобится. Подробнее это обсуждается в разделе “Распространение вашего открытого ключа” ниже в этой главе.

После завершения процесса генерации ключей, появляется завершающее окно диалога.



#### 17. Щелкните **Finish**.

Значок с парой ключей, появившийся в окне *PGP*, символизирует вашу новую пару ключей: *RSA*-ключи представлены синим цветом, а *DSS/DH* – желтым. Теперь вы можете исследовать эти ключи, выбрав пункт **Key Properties** (меню **Keys** или контекстного меню, доступного при щелчке правой кнопкой мыши). Возможно, вы также захотите добавить дополнительные имена или адреса. Подробнее эти процедуры описаны в Главе 5.

### Защита ваших ключей

После генерации пары ключей, разумно создать резервную копию и спрятать в надежное место на случай, если с оригиналом что-нибудь случится. Когда вы закрываете окно *PGPkeys* после генерации новой пары ключей, появляется подсказка, напоминающая о необходимости создания резервной копии.



Ваши наборы закрытых и открытых ключей хранятся в отдельных файлах-связках, которые вы можете копировать как любые другие файлы, в другую папку на жестком диске или на флоппи-диски. По умолчанию файлы со



связками закрытых (`secring.pkr`) и открытых (`pubring.skr`) ключей хранятся в папке *PGP*, вместе с другими файлами этой программы, но вы можете сохранять резервные копии где угодно.



Когда вы сообщаете *PGP*, что хотите создать резервную копию своих ключей, появляется *Окно выбора местоположения копии (Select Backup Destination)*, и вам нужно указать, где вы собираетесь сохранить файл.

Кроме создания резервной копии ваших ключей, вы должны позаботиться о правильном выборе места хранения оригинала вашего закрытого ключа. Хотя ваш закрытый ключ и защищен паролем, знать который должны только вы, остается вероятность того, что кто-либо узнает последний, и сможет использовать ваш закрытый ключ для расшифровки направленной вам почты или для подделки вашей цифровой подписи. Например, кто-нибудь может подглядеть пароль, когда вы набираете его, перехватить его сетевыми средствами или даже детектируя электромагнитное излучение вашего компьютера.

Чтобы предотвратить доступ к закрытому ключу постороннему, которому стал известен ваш пароль, вы должны хранить закрытый ключ только на своем собственном компьютере. Если ваш компьютер включен в сеть, вы также должны убедиться, что путь к файлам со связками ключей не включен в протоколы системного резервного копирования. Учитывая легкость, с которой можно получить доступ к любому компьютеру в сегодняшних сетях, если вы работаете с чрезвычайно секретной информацией, вам, возможно, стоит сохранять закрытый ключ лишь на дискете, и вставлять ее (как старомодную “ключевую дискету”) только на время, когда вы подписываете или расшифровываете частную почту.

В качестве еще одной меры предосторожности рассмотрите возможность придания другого имени файлу со связкой закрытых ключей и хранения его в иной папке, а не в папке по умолчанию (“*PGP*”), где его так легко найти. Для изменения местоположения связок ключей, используйте страничку *Keys* в диалоге **Preferences** программы **PGPkeys**.

### Распространение вашего открытого ключа

После того, как вы сгенерировали пару ключей, открытый ключ нужно сделать доступным для других, чтобы они смогли шифровать направляемую

вам почту и верифицировать вашу цифровую подпись. Для распространения своего открытого ключа у вас есть ряд возможностей:

- отправьте копию своего открытого ключа на сервер открытых ключей;
- включите копию открытого ключа в почтовое сообщение;
- экспортируйте открытый ключ, или скопируйте его в текстовый файл.

Поскольку открытый ключ может быть представлен в виде блока текста, сделать его доступным посредством сервера ключей, включить в почтовое сообщение или экспортировать в текстовый файл в равной степени просто. Получатель может затем добавить ваш открытый ключ на свою связку самым удобным для него способом.

### Открытие доступа к открытому ключу через сервер ключей

Возможно, наилучшим долговременным и удобным способом открытия доступа к вашему открытому ключу является размещение его копии на сервере открытых ключей, где он станет доступным каждому. Копирование ключа на сервер позволяет другим отправлять вам зашифрованную почту, не беспокоя вас предварительно просьбой прислать ключ. Это также освобождает пользователей *PGP* от необходимости хранить большое количество редко используемых копий открытых ключей.

Существует несколько серверов открытых ключей, один из которых поддерживается *PGP, Inc.*, которые позволяют сделать ваш ключ доступным каждому. Неважно, на какой сервер вы первоначально отправляете свой ключ, так как большинство основных серверов связаны таким образом, что однажды попавший в их сеть ключ становится известен всем остальным.

Различные серверы реализуют несколько отличающиеся варианты интерфейса для подгрузки новых открытых ключей, но в основном процедура остается одинаковой: вы должны скопировать текстовое представление своего открытого ключа и поместить его в должное место на сервере ключей. Однако, используя *PGP 5.0*, вы можете отправить свой открытый ключ на сервер автоматически сразу после генерации новой пары или в любое другое время, пользуясь программой *PGPkeys*.

### Как отправить свой открытый ключ на сервер

1. Откройте главное окно *PGPkeys*, щелкнув на значке с конвертом и ключом в Области системных индикаторов (*System tray*) и выбрав пункт **Launch PGPkeys**, или щелкнув на кнопке **Пуск (Start)** и выбрав пункт **PGPkeys** из подменю **PGP** меню **Программы (Programs)**.
2. Выберите значок, символизирующий открытый ключ, который вы хотите отправить на сервер ключей.
3. Выберите пункт **Send Selected Keys** из подменю **Keyserver** меню **Keys**, или из контекстного меню, вызываемого щелчком правой кнопкой мыши на значке ключа.

После того, как копия вашего открытого ключа помещена на сервер, вы можете сообщить тем, кто хочет отправить вам зашифрованную почту или верифицировать вашу цифровую почту, что они могут получить копию вашего ключа с сервера. Даже если вы не даёте явно ссылку на адрес своего открытого ключа, они могут найти его по вашему имени или адресу. Многие включают URL своего ключа в стандартную подпись своих писем, тогда

большинство пользователей электронной почты могут получить доступ к этому ключу простым двойным щелчком на этом указателе.

Если вы меняете свой почтовый адрес или используете другое имя, все, что вам нужно сделать, чтобы заменить старый ключ – это послать новую копию на сервер, и информация автоматически обновится. Однако, вы должны иметь в виду, что серверы открытых ключей могут лишь добавлять информацию, но не убирать старую. Если ваш ключ окажется скомпрометированным, вы должны отозвать его, чтобы дать всем знать, что ключу не следует больше доверять. Об отзыве ключей подробно написано в Главе 5.

### Включение открытого ключа в почтовое сообщение

Другим удобным методом отправки вашего открытого ключа является включение его в почтовое сообщение.

### Как включить свой открытый ключ в почтовое сообщение

1. Откройте главное окно *PGPkeys*, щелкнув на значке с конвертом и ключом в Области системных индикаторов (System tray) и выбрав пункт **Launch PGPkeys**, или щелкнув на кнопке **Пуск (Start)** и выбрав пункт **PGPkeys** из подменю **PGP** меню **Программы (Programs)**.
2. Пометьте значок, символизирующий вашу пару ключей, и выберите из меню **Edit** пункт **Copy**.
3. Откройте редактор, который вы используете для составления почтовых сообщений, поместите курсор в нужное место и выберите **Вставить (Paste)** из меню **Правка (Edit)**. В новых пакетах электронной почты, вы можете просто перетащить свой ключ из окна *PGPkeys* в окно почтового сообщения, чтобы вставить текстовый блок, представляющий ваш открытый ключ.

Когда вы посылаете кому-либо свой открытый ключ, обязательно подпишите сообщение. Тогда получатель сможет верифицировать подпись и убедиться, что сообщение не подделано и не изменено в пути.

### Экспорт открытого ключа в файл

Еще один метод распространить ваш открытый ключ – это скопировать его в файл и сделать этот файл доступным лицу, с которым вы хотите переписываться. Скопировать открытый ключ в файл можно разными способами:

- пометьте значок, символизирующий вашу пару ключей в окне *PGPkeys*, а затем выберите пункт **Export** из меню **Keys** и введите имя файла, в котором вы хотите сохранить ключ;
- перетащите значок, символизирующий вашу пару ключей из окна *PGPkeys* в окно *Проводника (Explorer)*, с открытой папкой;
- пометьте значок, символизирующий вашу пару ключей в окне *PGPkeys*, а затем выберите пункт **Copy** из меню **Edit**; затем в текстовом редакторе выберите **Вставить (Paste)** из меню **Правка (Edit)**.

### Получение открытых ключей других пользователей PGP

Точно так же, как ваш открытый ключ должен быть распространен среди тех, кто хочет отправлять вам зашифрованную почту и верифицировать вашу

цифровую подпись, вам нужно получить копии открытых ключей пользователей, прежде чем вы сможете отправлять им зашифрованную почту или верифицировать их подписи. У вас есть несколько возможностей получить чей-либо открытый ключ:

- взять ключ на сервере открытых ключей;
- взять ключ из тела почтового сообщения;
- импортировать ключ из файла.

Поскольку открытые ключи представлены просто блоками текста, в равной степени просто добавить их на свою связку, импортировав из файла или скопировав из тела почтового сообщения. Вот пример блока текста, представляющего открытый ключ:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP for Personal Privacy 5.0

mQCNAy+wNIMAAAEANXqEtRa jpmH4GXvN+1MZWAaKVbBEAX6Vu0fBumU+5mpaXmE
4mmUHcBXAF8a6F9Bx3wpmgm3LEzQyOIuf jT90xRv1Tlzh6bg6U7Z9Cd3/lX/u/HY
H04Ft jD6q6uOFCDMWSjxqWVYs+BcZwLyQJ3PwpC9RM6/ki3XGCEHWOiJDhAAUT
tBNNYwtZaW0gRS4gT3RzdGF2bm92tCZNYWtZaW0gRS4gT3RzdGF2bm92IDxtYWtz
aW1Adm9sZ2EubmV0PokAlQMFEEDPUj91xghB1 joiQ4QEBBawEAMHgqakfLELGNIT
wssAqbXbibwJ1UD0xqr jS1Jp9qZyswqP3zUP7wndY+6WfyWQUlulK/Qz9ms41pnb
iLW/QQbklAhKsecAPPPwkoxs5Doc7F30gxiTWSUTgccQ3j6hgBu50FGreohVe+x5
0B9xOnw3rY5WGeV2V0YXmc8zg+VJtCxNYWtZaW0gRS4gT3RzdGF2bm92IDxtYWtz
aW1rYUBnZW9 jaXRpZXMuY29tPokAlQMFEEDPUkAdxghB1 joiQ4QEBRGQD/iSIQ2sd
U7bsOgBek4yUGVaSD1N6GuGodc8sR7B8k1NcgUQOJMtT/vTd05J9QIyWuQ1NxDm
XDKmqg jFVL7o1+fLJG7pL0kot9SMhvMmJee7Is+Nq+yEo1jckc+3BsbFXqDwcIUk
bKSPduRH8ARaFZJR7QRsWAMtMPVGlAAsqNGctC5NYWtZaW0gRS4gT3RzdGF2bm92
IDxtYWtZaW1AaWNjLnR1LWNoZWwuYWMucnU+iQCVaUQM9SQKnGCEHWOiJDhAQET
9wP/YAeEjDmVNFz4T9C3IHnZz4SrStYqVFouXreXMu1di/NoUqc5SOYSgqEZFqD
6blgdq1zBPXviiOp1EmosH2Fml3EoBDbp+mRqbo9S9SVJofrHZoEDmWpWj4iZQf3
XmegYcZjEhWnjsbxfw40BYeRvtFPkMMZiAtzRGQbVULRFi0Kk1ha3NpbSBFLiBP
dHNOYXZub3YgPG1ha3NpbUBpYy5yZWRsaW5lLnJlPokAlQMFEEDPUkEpXghB1 joiQ
4QEBU5ID/j4uV6UHixvZ0xYok7pyoNcnfBgnM2Q7GyBHuHu+3zk/Ro2v+Y/vb7yk
8v7EC7fgrGOHBwxTberM8oApadqlMnOQ562/+uL3p+RqvYxV+0S+VrAvMgkfdvef
ANTdTD5wNkDU6BprRnTFzVK8E7VxIh7d9zu78tcYmVKANCeihRfQctC1NYWtZaW0g
RS4gT3RzdGF2bm92IDxtYWtZaW1AaWMudHVuaXMuDHzLci5zdT6JAJUDBRAZlJBT
cYIQdY6IkOEBBAZ7OA/430on+/HHld94DzFLEngsXPM0HOAPy56gizDJL8v9/LLpC
7qnpb8efbMnji+LLYvrOW5wY1ugJln5dx4Xm3HWHaeKzb3YTA5oGPNNXcxiJ/2FL
iS1tXAV4n/ia6Uz jlijfZQEmtkpgkLgfEe1W6p9eQKyklncCAFEDezthOGjL0bQt
TWFrC2ltIEUuIE90c3Rhdm5vdiA8bWFrC2ltQGJlc2luZXNzLmtpZXZYudWE+iQCW
AwUQM9SQiHGCEHWOiJDhAQGzcgQAu36lFvag9bcplzgxNPJAPAreHDwY jpyvOpOW
pI3iPo+RpK1t/Ekw8OyyBnBiy4tgCv5DmBwtWGLuBSKLYe5BzG6A6ZnV3F7wC5B
NLx0PN6NQcaux9OKxUcUih62lHJ/0r89JuKTMgZydr83fyVACs7yWo5C4Kc2VIGh
Eo4Fl6i0KE1ha3NpbSBFLiBPdHNOYXZub3YgPG1ha3NpbUBpYwJiLnRsdC5ydT6J
AJUDBRAZlJc6cYIQdY6IkOEBAAulBACrsdRw8bVY6ymCDOcPsgnXbDF6DnBhg1NH
+InoL98wG10ERvax7FIumy3NVHtWT7Y6yhkGc7keoEYxMqanxC4ufcmuI5+Flq1
W0rc4vX0rP6gKIFntQv42glzonlfqfFcaYGEbIksicKpFLAcbsFaLL5y7TMLZr5Z
iesFw2Hcc7QuTWFrC2ltIEUuIE90c3Rhdm5vdiA8bWFrC2ltQG1hYmUdG9nbG1h
dHRpLnJlPokAlQMFEEDPUkNdxghB1 joiQ4QEBZ40EAIw5zhHi+EiP1VYLLRB5ReNH
VoaxxmZwvOxvq8aSg8DsYlPYh91VDKp8J7i0JirOHhfNXDuTGcGRwYywfdmDVFFa
OukANuAKiC7+xBtNq6hYKlILkGAKPGGjHjXEaskAKCi88mbIdm4Sk5zMpgGi8WS4
KMDAKYtX7RkKCR1j8+5+
=Ode6
-----END PGP PUBLIC KEY BLOCK-----
```

### Получение открытого ключа с сервера ключей

Если лицо, которому вы собираетесь отправлять зашифрованную почту – достаточно опытный пользователь *PGP*, существуют шансы, что его открытый ключ присутствует на серверах открытых ключей. Это делает весьма удобным для вас получить копию его последнего ключа тогда, когда вам понадобится отправить ему почту, и также освобождает вас от необходимости хранить большое количество открытых ключей на своей связке.

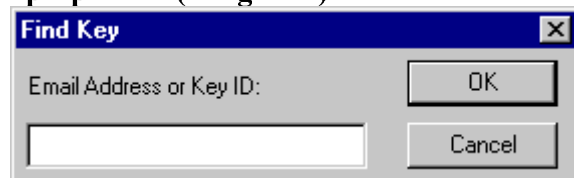
Существует несколько серверов открытых ключей, один из которых поддерживается *PGP, Inc.*, которые позволяют вам получить открытые ключи большинства пользователей *PGP*. Если получатель не предоставил

URL, указывающий на его ключ, вы можете на любом из серверов выполнить поиск по его имени или адресу, поскольку большинство основных серверов связаны таким образом, что однажды попавший в их сеть ключ становится известен всем остальным. Эта версия *PGP*, однако, освобождает вас от необходимости идти столь старомодным путем, предоставляя возможность быстро найти ключ определенного пользователя непосредственно при отправке почты или в любое другое время из окна *PGPkeys*.

#### Как получить чей-либо открытый ключ с сервера

1. Откройте главное окно *PGPkeys*, щелкнув на значке с конвертом и ключом в Области системных индикаторов (System tray) и выбрав пункт **Launch PGPkeys**, или щелкнув на кнопке **Пуск (Start)** и выбрав пункт **PGPkeys** из подменю **PGP** меню **Программы (Programs)**.

1. Выберите **Find New Key** из подменю **Keyserver** меню **Keys**. Появится Диалог поиска ключа (*Find Keys*).



3. Введите адрес или имя пользователя.

Если открытый ключ искомого пользователя найден, от вас требуется указать, хотите ли вы добавить его на свою связку открытых ключей. После того, как вы добавите ключ на связку, он становится виден в окне *PGPkeys*, из которого вы можете исследовать действительность ключа.

#### Получение ключа из тела почтового сообщения

Еще один удобный способ получения чужого открытого ключа – это попросить хозяина отправить его в зашифрованном почтовом сообщении. Если вы пользуетесь почтовым пакетом, поддерживаемым *PGP* с помощью встраиваемых модулей, добавить открытый ключ отправителя можно простым нажатием на кнопку. Например, когда приходит сообщение с блоком текста, содержащим чей-либо открытый ключ, щелкните на кнопку с ключом и конвертом на Панели инструментов почтового пакета, и ключ будет сохранен на вашей связке.

Если вы используете почтовый пакет, не поддерживаемый *PGP* с помощью встраиваемых модулей, вы можете скопировать блок текста, представляющий открытый ключ, в Буфер обмена, а затем, используя команду **Paste** меню **Edit** программы *PGPkeys*, добавить его на связку.

#### Импорт открытого ключа из файла

Другой вариант получения чье-либо открытого ключа – это попросить хозяина сохранить его в файле, из которого вы сможете импортировать ключ или скопировать в Буфер обмена и добавить на свою связку открытых ключей. Для выделения открытого ключа и добавления его на связку существует несколько способов:

- выберите из меню **Keys** программы *PGPkeys* пункт **Import**, затем введите имя файла, содержащего открытый ключ;
- перетащите файл, содержащий открытый ключ, из окна *Проводника (Explorer)* в окно *PGPkeys*;

- откройте текстовый файл, в котором хранится ключ, текстовым редактором, выделите блок текста, содержащий ключ, и выберите **Копировать (Copy)** из меню **Правка (Edit)**. Затем, перейдите в окно **PGPkeys** и выберите **Paste** из меню **Edit**. Ключ станет виден как значок в окне **PGPkeys**.

### Проверка подлинности ключа

Когда вы обмениваетесь ключами с другими пользователями *PGP*, иногда бывает трудно определить, действительно ли ключ принадлежит тому или иному лицу. *PGP* предусматривает ряд предосторожностей, соблюдение которых позволит вам проверить подлинность ключа и удостовериться, что ключ действительно принадлежит номинальному владельцу. *PGP* также предупреждает вас при попытке использовать недействительный ключ и может быть настроена для предупреждения при попытке использования ключа надежного лишь отчасти.

Одно из наиболее уязвимых мест систем шифрования с открытым ключом – возможность того, что злоумышленник предпримет *атаку с активной ретрансляцией* (a “*man-in-the-middle*” attack). Этот тип атаки предполагает подмену чье-либо открытого ключа ключом, сгенерированным самим злоумышленником. Затем, последний может перехватывать всю зашифрованную почту, направляемую его жертве, расшифровывать ее с помощью соответствующего закрытого ключа, снова зашифровывать, используя настоящий открытый ключ жертвы, и переправлять ей, как будто бы ничего не случилось. Фактически, все это может выполнять автоматически хитроумная компьютерная программа, установленная где-либо на пути следования почты и расшифровывающая всю вашу корреспонденцию.

Учитывая такой расклад, вы (и те, с кем вы обмениваетесь электронной почтой) нуждаетесь в способе определения того, действительно ли вы обладаете подлинными копиями открытых ключей друг друга. Лучший способ быть абсолютно уверенным в том, что открытый ключ действительно принадлежит определенному лицу – это получить из рук этого лица дискету с его ключом. Но поскольку вы не всегда находитесь в достаточной близости от своих корреспондентов, обычно обмен ключами производится посредством электронной почты или сервера открытых ключей.

Хотя в некотором смысле это является менее надежным способом защиты ключей от подделки, вы можете определить, принадлежит ли ключ определенному лицу, проверив его цифровой отпечаток, уникальную последовательность чисел, генерируемую при создании ключа. Сравнив отпечаток имеющейся у вас копии чье-либо ключа с отпечатком оригинала, вы можете быть абсолютно уверены в том, что обладаете действительной копией его ключа.

Самый очевидный способ проверки отпечатка – это позвонить хозяину ключа и попросить его продиктовать отпечаток по телефону. Когда вы получаете ключ с сервера открытых ключей, вам не нужно проходить через это, так как вы можете получить информацию об отпечатке, находясь online. Конечно, вы при этом ожидаете, что владелец ключа периодически проверяет копии своих ключей на сервере и убеждается, что их никто не подменил.

После того, как вы абсолютно уверитесь в том, что обладаете подлинной копией чьего-либо открытого ключа, вы можете подписать (сертифицировать) этот ключ. Сертифицируя чей-либо ключ, вы сообщаете миру, что уверены в принадлежности этого ключа его номинальному владельцу. Например, когда вы генерируете новую пару ключей, она автоматически сертифицируется вашей подписью, поскольку разумно предположить, что генерирующее ключи лицо и есть их владелец. Цель сертификации собственных ключей – предотвращение их модификации кем-либо другим, что немедленно сделало бы такую подпись недействительной.

Пользователи *PGP*, находящиеся в доверительных отношениях, часто подписывают ключи друг друга, чтобы придать дополнительную степень уверенности в их подлинности. Например, вы можете попросить своего коллегу сертифицировать ваш ключ и вернуть его вам вместе с подписью, чтобы она была включена в сертификат ключа, отправляемого на сервер. Теперь, когда кто-то третий получает копию вашего ключа с сервера, ему не обязательно проверять ее подлинность самому. Вместо этого он может положиться на подпись лица, которому он доверяет. *PGP* предоставляет средства установления степени доверия к подписи каждого лица, чей ключ находится на вашей связке открытых ключей, и показывает степень доверия, соответствующую каждому из ключей в окне *PGPkeys*. Это значит, что получая ключ, подписанный надежным посредником, вы можете быть в достаточной степени уверены, что он принадлежит номинальному владельцу. Подробно процедуры сертификации ключей и придания степени доверия пользователям описаны в Главе 5.

### Отправка и получение приватной электронной почты

В этой главе объясняется, как шифровать и подписывать почту, отправляемую другим, и расшифровывать и верифицировать почту, получаемую от других.

#### Шифрование почты и наложение подписи

Самый простой и быстрый способ шифровать и подписывать почту – это воспользоваться почтовым пакетом, который поддерживается *PGP* посредством подключаемых модулей. Хотя эти процедуры несколько отличаются в разных пакетах, в любом из них вы выполняете шифрование или наложение подписи нажатием соответствующей кнопки на Панели инструментов почтового пакета. Кроме того, если вы используете пакет, поддерживающий стандарт *PGP/MIME*, вы можете автоматически шифровать и подписывать ваши почтовые сообщения и любые файлы при отправке почты.

Если вы используете почтовый пакет, который не поддерживается посредством встраиваемых модулей, вы можете шифровать и подписывать сообщения, используя Буфер обмена, выбирая соответствующую опцию из меню, вызываемого щелчком на значке с конвертом и ключом в Области системных индикаторов. Для шифрования и подписи файлов, прилагаемых к сообщению, их нужно зашифровать или подписать из окна *Проводника (Explorer)* до присоединения.

#### Шифрование и наложение подписи в поддерживаемых пакетах электронной почты

Шифруя и подписывая почту с помощью пакета, поддерживаемого *PGP* посредством встраиваемых модулей, вы можете использовать один из двух способов, в зависимости от того, каким программным обеспечением пользуется получатель. Если получатель использует почтовый пакет, поддерживающий *PGP/MIME*, вы можете воспользоваться преимуществами этого стандарта, чтобы шифровать и подписывать почтовые сообщения и прилагаемые файлы автоматически во время отправки. Если вы общаетесь с тем, кто использует пакет, не поддерживающий *PGP/MIME*, вы должны выключить опцию *PGP/MIME*, чтобы избавить получателя от проблем, связанных с несовместимостью. Недостаток этого метода в том, что каждый прилагаемый к сообщению файл вам придется шифровать (подписывать) отдельно.

*Примечание:* Если составляемые вами сообщения не отправляются немедленно, а сохраняются некоторое время в очереди, вы должны иметь в виду, что при использовании некоторых почтовых пакетов шифрование будет выполнено только при физической отправке сообщения. До того, как оставлять сообщение в очереди, вам нужно проверить, помещено ли оно туда в уже зашифрованном виде. Если нет, вам стоит рассмотреть возможность выполнения шифрования через Буфер обмена.



Как зашифровать и подписать сообщение, отправляемое с помощью поддерживаемого пакета

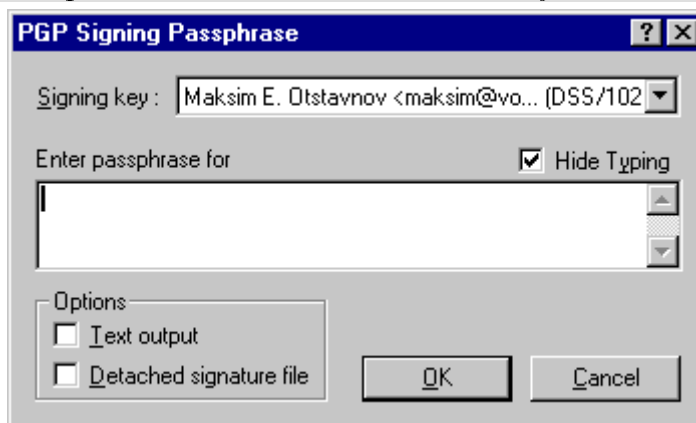
1. Составьте почтовое сообщение с помощью своего почтового пакета, как обычно.
2. Составив сообщение, укажите, хотите ли вы, чтобы оно было зашифровано и/или подписано, щелкнув на кнопке с замком и пером. Если вы переписываетесь с пользователем *PGP*, который применяет почтовый пакет, соответствующий стандарту *PGP/MIME*, вам нужно щелкнуть на кнопке *PGP/MIME*.



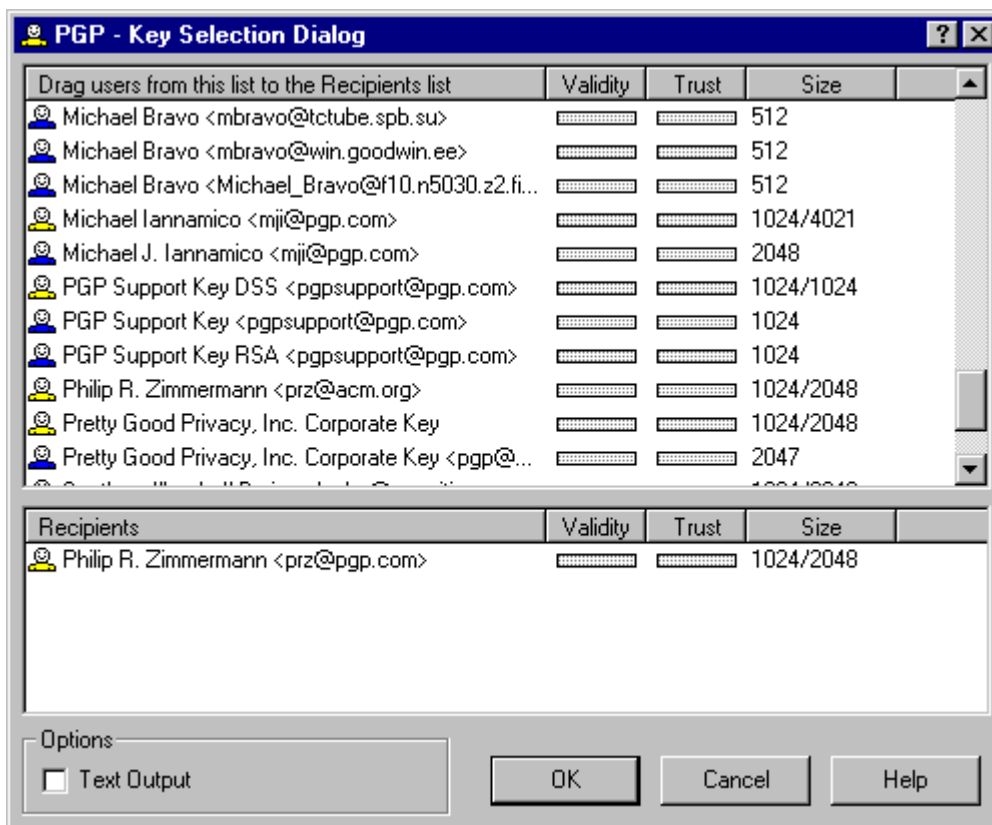
Когда вы щелкаете на одной из этих кнопок, она остается “утопленной”, указывая на операцию, которая будет выполнена.

*Примечание:* Если вы уверены, что собираетесь подписывать и/или шифровать сообщения, а также использовать *PGP/MIME* на регулярной основе, вы можете включить эти операции по умолчанию, выбрав соответствующие установки на страничке *E-Mail* окна диалога *Preferences*.

3. Отправьте сообщение, как обычно. Если вы выбрали опцию наложения подписи, до того, как сообщение будет отправлено, появится *Диалоговое окно пароля (Passphrase)*, требующее от вас ввести пароль.



4. Введите свой пароль и щелкните ОК. Если у вас есть копии открытых ключей всех получателей, будут использованы эти ключи. Если же вы укажете получателя, копии открытого ключа которого на вашей связке нет, появится Диалог выбора ключа (*PGP Key Selection*), в котором вы можете выбрать необходимый ключ.



5. Перетащите открытые ключи тех, кому направляется зашифрованное сообщение в поле *Получатели (Recipients)*. Для перемещения ключа из одного поля в другое вы также можете использовать двойной щелчок мышью на значке ключа.

Полоска *Действительность (Validity)* указывает минимальный уровень уверенности в том, что открытые ключи, помещенные в поле *Получатели (Recipients)*, являются действительными. Это значение вычисляется на основе количества подписей, сертифицирующих каждый ключ и уровень надежности тех, кто его сертифицировал (подробнее об этом см. Главу 5).

*Примечание:* Если вы не используете *PGP/MIME*, вы должны шифровать (подписывать) каждый файл, отправляемый в качестве приложения, из окна *Проводника (Explorer)*.

6. Для отправки сообщения щелкните **ОК**.

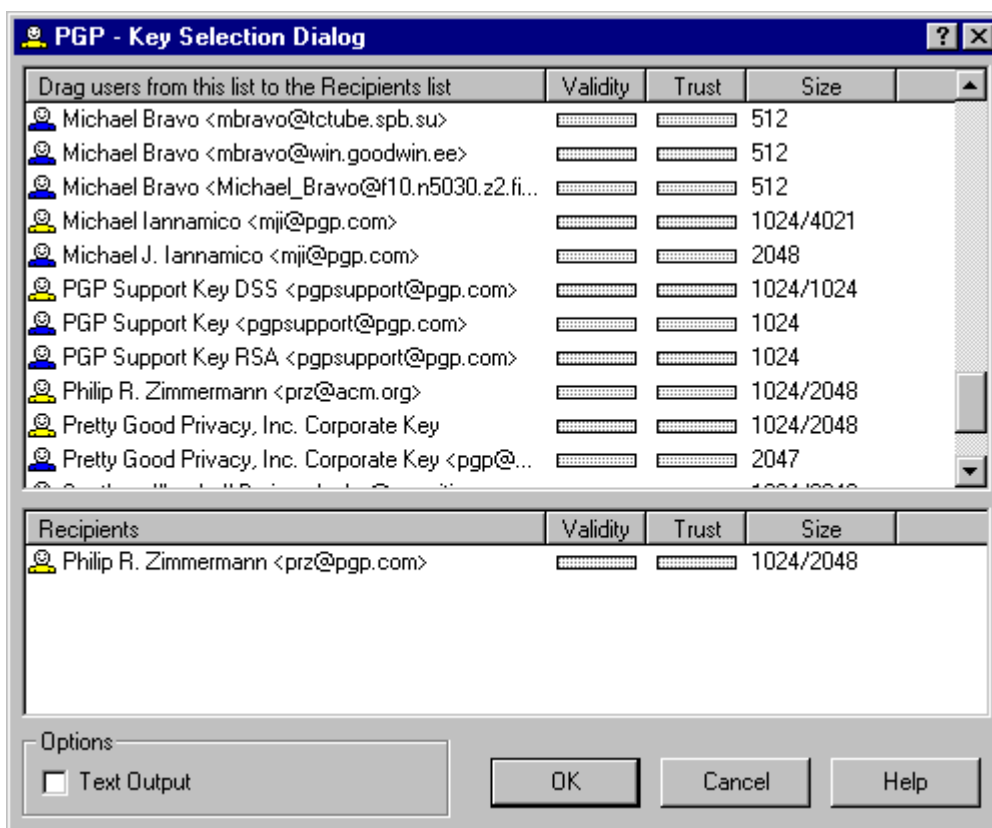
### Шифрование и наложение подписи через Буфер обмена

Если вы используете почтовый пакет, не поддерживаемый *PGP* посредством встроенных модулей, вы должны для шифрования и наложения подписи использовать Буфер обмена. Это осуществляется щелчком на значке с конвертом и ключом в Области системных индикаторов и выбором соответствующего пункта меню. Вы копируете содержимое сообщения в Буфер обмена, шифруете и/или подписываете содержимое последнего и вставляете его в тело почтового сообщения. Если вы прилагаете к сообщению какие-либо файлы, вы должны зашифровать (подписать) их из окна *Проводника (Explorer)* до присоединения.

### Как зашифровать (подписать) содержимое Буфера обмена

Процедура шифрования и/или наложения подписи на содержимое Буфера обмена осуществляется следующим образом:

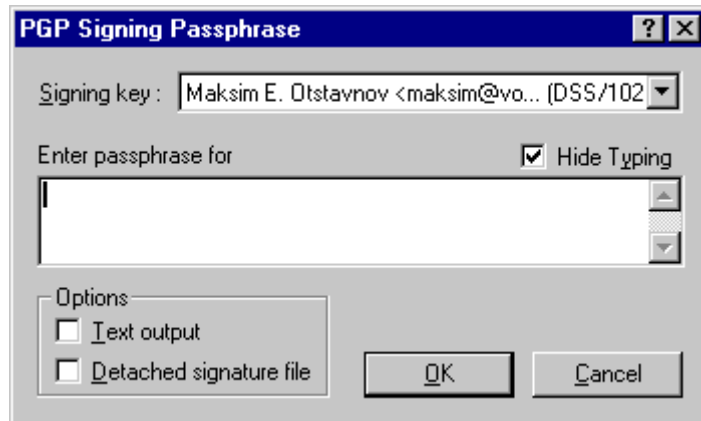
1. Наберите текст сообщения, используя встроенный редактор вашего почтового пакета или свой любимый текстовый процессор.
2. Когда текст набран, пометьте его.
3. Выберите **Копировать (Copy)** из меню **Правка (Edit)**.  
Вы должны знать, что каждый раз, когда вы копируете или вырезаете текст из окна приложения, он временно сохраняется в Буфере обмена.
4. Щелкните на значке с конвертом и ключом в Области системных индикаторов и выберите **Encrypt Clipboard** для шифрования, **Sign Clipboard** – для наложения подписи, или **Encrypt And Sign Clipboard** – для шифрования и наложения подписи на содержимое Буфера обмена.  
Если вы указали, что хотите зашифровать содержимое Буфера обмена, появится окно *Диалогов выбора ключа (Key Selection Dialog)*.



5. Перетащите открытые ключи получателей сообщения в поле *Получатели (Recipients)*.  
Полоска *Действительность (Validity)* указывает минимальный уровень уверенности в том, что открытые ключи, помещенные в поле *Получатели (Recipients)*, являются действительными. Это значение вычисляется на основе количества подписей, сертифицирующих каждый ключ, и уровня надежности тех, кто его сертифицировал (подробнее об этом см. Главу 5).

6. Щелкните **ОК**.

Если вы выбрали опцию наложения подписи, до того, как сообщение будет отправлено, появится *Диалоговое окно пароля (Passphrase)*, требующее от вас ввести пароль вашего закрытого ключа по умолчанию. Если у вас есть другие пары ключей, и вы хотите использовать для подписи одну из них, вы можете нажать для этого кнопку со стрелкой и выбрать нужный ключ.

7. Введите свой пароль и щелкните **ОК**.8. Вернитесь в окно своего почтового пакета и выберите пункт **Вставка (Paste)** меню **Правка (Edit)**. Тем самым вы скопируете зашифрованное (подписанное) сообщение в тело сообщения.

## 9. Отправьте сообщение его получателем.

## Шифрование и наложение подписи из окна Проводника

Если вы собираетесь отправить зашифрованный (подписанный) файл в качестве приложения к сообщению или просто зашифровать файл, чтобы защитить его от несанкционированного доступа, вы можете сделать это из окна *Проводника (Explorer)*.

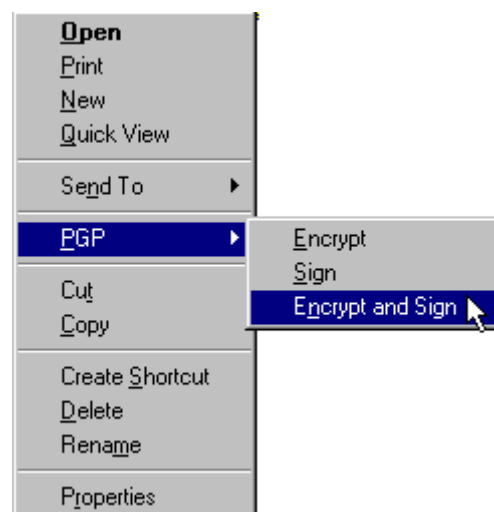
## Как зашифровать и подписать файл из окна Проводника

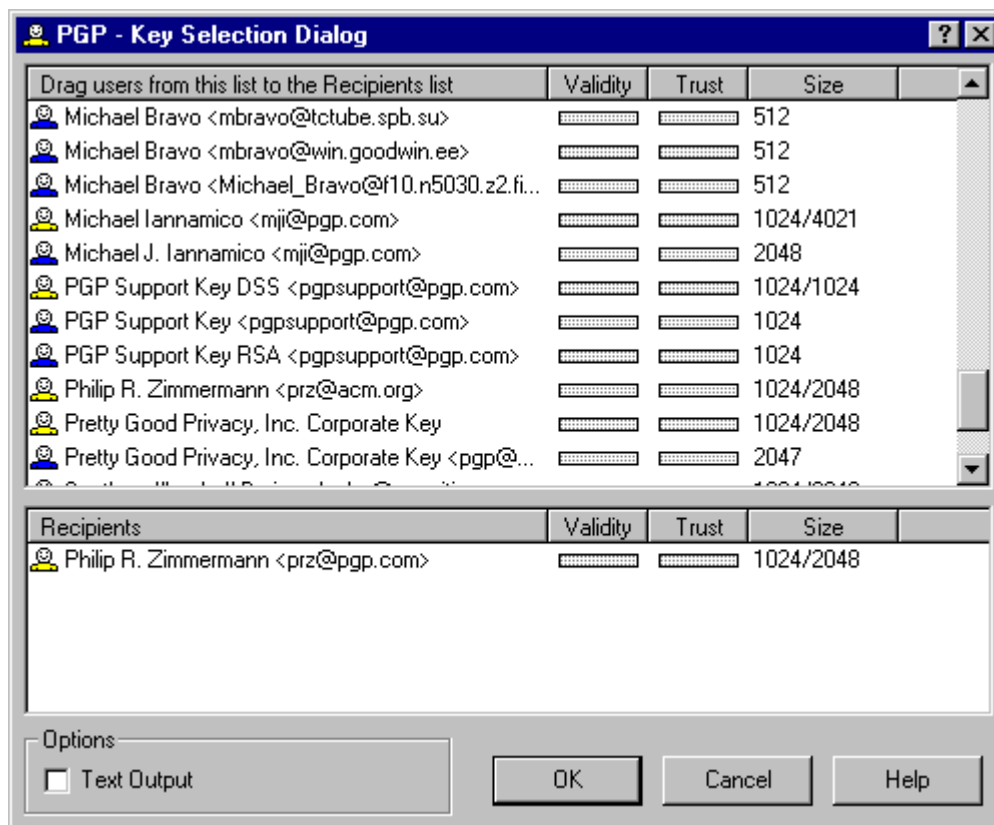
1. Запустите *Проводник (Explorer)* из меню **Пуск (Start)**.

## 2. Пометьте файл или файлы, которые хотите зашифровать (подписать). Вы можете пометить несколько файлов, но шифроваться (подписываться) они будут по отдельности.

3. Выберите необходимую опцию из меню **Файл (File)** или из контекстного меню, вызываемого щелчком правой кнопкой мыши.

При шифровании файла появляется окно *Диалогов выбора ключа (Key Selection Dialog)*, в котором вы выбираете открытые ключи получателей.





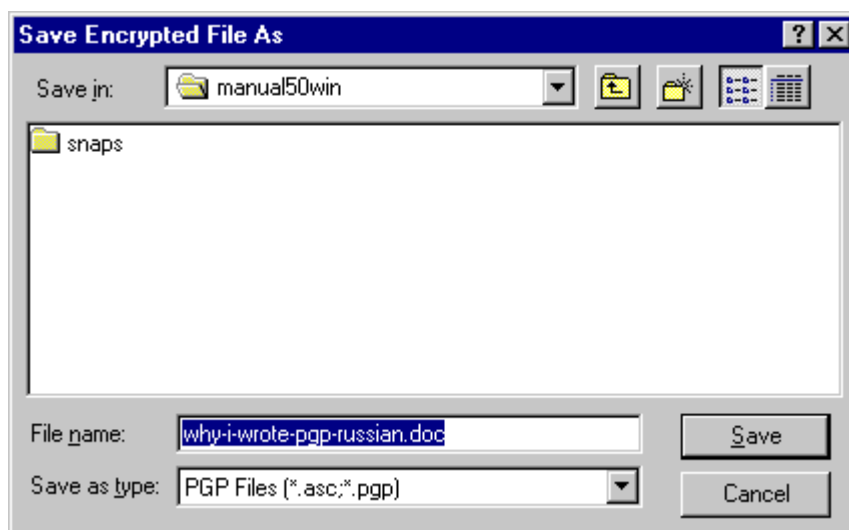
При отправке файлов в качестве приложений к сообщениям при использовании некоторых почтовых пакетов вам может понадобиться отметить поле *Текстовый вывод (Text Output)* для того, чтобы был сгенерирован файл в формате ASCII. Это требуется при использовании некоторых старых почтовых пакетов.

При наложении подписи появится диалоговое окно пароля (*Passphrase*), требующее от вас ввести пароль.

Если вы накладываете на файл подпись и хотите, чтобы подпись была сохранена в отдельном файле, отметьте поле *Отдельный файл подписи (Separate Signature File)*.

Если вы хотите, чтобы был сгенерирован файл в формате ASCII, отметьте поле *Текстовый вывод (Text Output)*. Заметьте, что эта опция увеличивает объем файла приблизительно на 30%.

4. Выберите открытые ключи, перетаскив их в поле *Получатели (Recipients)*.  
Появится Окно диалога выбора выходного файла (Save Encrypted File As).



5. Укажите местоположение и введите имя файла, в котором должен быть сохранен зашифрованный (подписанный) файл. К имени автоматически добавляется расширение “.pgp”, а если была выбрана опция текстового вывода (*Text Output*) – то расширение “.asc”.
6. Чтобы сохранить файл в указанном месте, щелкните **Save**. Если вы взглянете на содержимое папки, в которой сохранили файл, вы увидите, что он символизируется одним из двух значков.



.pgp

зашифрованный со стандартным  
выводом



.asc

зашифрованный с текстовым  
выводом

### Расшифровка и верификация почты

Самый простой и быстрый способ расшифровывать и верифицировать почту – это воспользоваться почтовым пакетом, который поддерживается *PGP* посредством подключаемых модулей. Хотя эти процедуры несколько отличаются в разных пакетах, в любом из них вы выполняете расшифровку или верификацию подписи нажатием соответствующей кнопки на Панели инструментов почтового пакета. Кроме того, если вы используете пакет, поддерживающий стандарт *PGP/MIME*, вы можете автоматически расшифровывать и верифицировать почтовые сообщения и приложенные файлы, щелкая на значках, включенных в тело сообщения.

Если вы используете почтовый пакет, который не поддерживается посредством встраиваемых модулей, вы можете расшифровывать и верифицировать сообщения, используя Буфер обмена и выбирая соответствующую опцию из меню, вызываемого щелчком на значке с конвертом и ключом в Области системных индикаторов. Для расшифровки и верификации файлов, прилагаемых к сообщению, нужно расшифровать или верифицировать их из окна *Проводника (Explorer)*.

## Расшифровка и верификация в поддерживаемых почтовых пакетах

Если вы переписываетесь с пользователями *PGP*, которые шифруют и подписывают свою почту с использованием стандарта *PGP/MIME*, при открытии такого сообщения вы увидите значок с открытым конвертом.

```
X-Sender: mji@mail.pgp.com (Unverified)
X-Mailer: QUALCOMM Windows Eudora Pro Version 3.0.2 b4 (32)
Date: Wed, 21 May 1997 10:02:32 -0700
To: mji@pgp.com
From: Mike Iannamico <mji@pgp.com>
Subject: test
```



Decrypt PGP/MIME Message

В этом случае вы можете расшифровать (верифицировать) сообщение или присоединенный файл, щелкнув два раза на этом значке.

Если вы получаете почту от пользователей *PGP*, которые не используют стандарт *PGP/MIME*, расшифровать (верифицировать) такое сообщение можно, нажав кнопку с изображением открытого конверта на *Панели инструментов* почтового пакета. Если к сообщению приложены зашифрованные (подписанные) файлы, расшифровать (верифицировать) их можно из окна *Проводника (Explorer)*.

## Как расшифровать и верифицировать почту в поддерживаемом почтовом пакете

### 1. Откройте почтовое сообщение, как обычно.

В теле сообщения вы увидите блок непонятной шифровки.

```
-----BEGIN PGP MESSAGE-----
Version: PGP for Personal Privacy 5.0
MessageID: goAFGGxUlgXP12ng98JcVXG+6MUMwWZ5

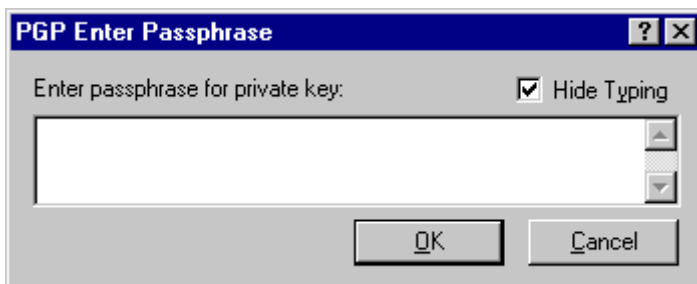
hQcMA3GCEHWOiJDhAQQArOUZgSBy68kmUHcN4+rz9UmDm2o9lJWeJlL68i8UaskX
odJj273Ct/9GDqEmVQjN59tFjVTDqZSSlnpeusvSbo4mBCOaqlncCU90kt+Rev0o
Cct+B3sE1WYR7k7m8dWky4fSXjSaii/4Z7vw031Vr3PuPwAxaMA82yPAdSQy002l
BBZ6f8cK6e+83q4XInY8VpyeEWgMcfsgP642+yWxwsgUQAPH2/qoTN7IApxX6Oej
vn9Ou9V8qdwETuMJI5KA776WYeOFQjeUM+Q3FnA3Hc3nP/5Ub8a8g3IprS1YXWwM
K+Q7iT/qBOirT9K01PIzOq+vgBp9W0g9mCBFGX+Isak4u9x0j/wUw/m94KmmBL3w
J2j4qhUbyqPwSxkhATEbqEe/SwKE2XZSqDb13aWTalNUNInu7i6kcUBFlf++fhjp
3sjxUKA+guc0kiyiCZwWfXa8I8vVH2SCvGjpwyzubHKjtdbaxMjbkKU5jacdEzSt
ximl3YQhy2qAd/7D56x9NBxhCEW+cv+dk1QEtMpsVow/RGe9SGCQ1rcxlinNq0lJ
x//jTWbBnvUkt//4SLT0kBCBP21fPvIHftsqBRvMLkaM5R4VXGTnqZmgIpbL5udh
QWEYPU+8U45NfZed6Z3RRBVD+PJOOf3njauA5FPr+qbpMHb1lVdjrXw7MMFhwoFPS
Pm8zfAp0M9cNIFTBn2C3oFTWW31uVNUg2iLk/615qZ/OxXg4jWHXg/561bY8bZVO
AjIDsS8KCqsXy6oUCsyfVSmRzRvdTmuo4lF2pS8ItuVr4xjrWxxDM+DkoKkaCzV6
O4TTVYPmQBiu0fFqtsgZRsEETyFmQ2hchLf0Ki39i6/xwwJC4OArplCuG6pyn/bN
OGS7cD7FE97PmiWwNE4eMkVIYrTTU7A7mA14gDicPvEEDJY3ptvIR5p04I1BTj9V
0p7HV/1V+8TsgfuiLDY7OZ0DA2ssWNVr36EqVAM5j2KEypda4tZiSDjUT8R3r1Ja
xz2mz65w1W1FRHBzgiHk+mSnKkLyYliyouy5yedlHPerF2EP3EV3FHSBVjQdMCu
KHS CpNs1Sjba/cAk+sZFFbASIfNfFfKjDUWK9xIoPpZ10K+f2Mlzb1HbYIbZfyze
kkaSYpSscTkmGsEfEf4RUeqeODyITEVKVGEeLc5x+nvwczw0/+Mm7P5a6JyDkAp0d
3s+IQw9pdRy/ohKVIVSgHaI/MQMvzRtNj09IzFwUWtKb0VAXWVlFMnxVypXUKXp
kuEo4ku64hKIHYyuy6u3mAoN9gB8e5tL4T9t2Aw6TEFyTSHqZtYXGScfxt3aXTN
XAq4I22s+9axmA5I3RnEQjBrP7Wtrm5yManxx9SCE1uFyQ1G1i00qDy5eFg78csV
T04Hb+w0eoYasTUhSJ/0seBBF1XlIXEuq9fKUBEofHyRCwvShFM+Los/CGk+zVt
EwG164E4NysexHUP4UCxmVepcCs8VLLBAuNblt4i4SzetYzFzZdGMokdoqiv6YH07
USDVwaClmtFznfBbbrzh6DWISpce/3wFrZer41KY9U0YXmjWtRyQw==
=wNSW
-----END PGP MESSAGE-----
```

### 2. Для расшифровки и верификации сообщения, щелкните кнопку с изображением открытого конверта на Панели инструментов почтового



пакета.

При расшифровке появится окно *Диалогов ввода пароля (PGP Enter Passphrase)*, в котором вы должны ввести свой пароль.



3. Введите пароль и щелкните **ОК**.

Зашифрованное сообщение будет расшифровано, а если оно подписано, появится окно, в котором будет указано, успешно ли оно верифицировано.

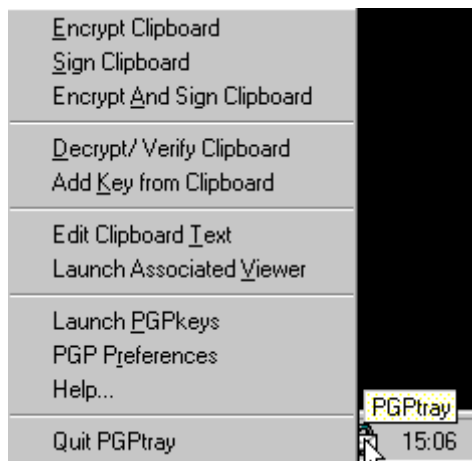
4. На этом шаге вы можете сохранить сообщение в расшифрованном виде или для сохранения безопасности сохранить зашифрованный оригинал.

### Расшифровка и верификация через Буфер обмена

Если вы используете почтовый пакет, не поддерживаемый *PGP* посредством встроенных модулей, вы должны для расшифровки и верификации подписи скопировать содержимое сообщения в Буфер обмена. Если к сообщению прилагаются какие-либо файлы, вы можете расшифровать (верифицировать) их из окна *Проводника (Explorer)*.

### Как расшифровать и верифицировать сообщение через Буфер обмена.

1. Находясь в окне вашего почтового пакета, пометьте зашифрованный (подписанный) текст и скопируйте его в Буфер обмена. В большинстве пакетов это можно сделать, выбрав пункт **Копировать (Copy)** из меню **Правка (Edit)**.
2. Щелкните на значке с конвертом и ключом в Области системных индикаторов. В появившемся меню выберите пункт **Choose Decrypt/Verify Clipboard**.



При расшифровке появится окно *Диалогов ввода пароля (Enter Passphrase)*, в котором нужно ввести пароль.

3. Введите пароль и щелкните **ОК**.

Сообщение будет расшифровано. Если оно подписано, будет сделана попытка верификации подписи, и появится окно с сообщением о том, успешно ли прошла верификация.





- Для просмотра содержимого расшифрованного сообщения выберите из меню **PGP** пункт **Edit Clipboard Text** или **Launch Associated Viewer**. Затем вы можете при желании вставить содержимое буфера обмена обратно в сообщение, из которого вы скопировали шифровку, и сохранить его.

### Расшифровка и верификация из окна Проводника

Если полученная вами почта содержит приложенные файлы, и вы не используете почтовый пакет, поддерживающий стандарт *PGP/MIME*, расшифровывать и верифицировать эти файлы нужно из окна *Проводника (Explorer)*.

### Как расшифровать и верифицировать файл из окна Проводника

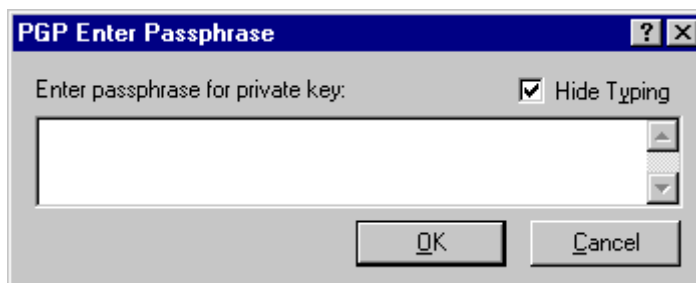
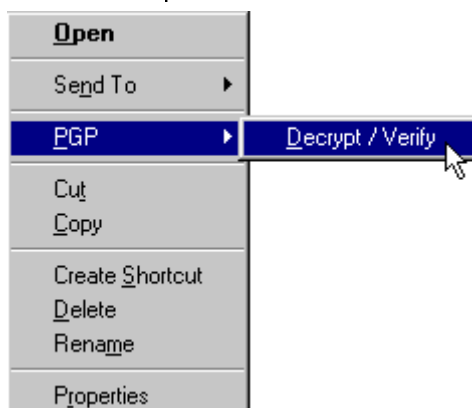
- Запустите *Проводник (Explorer)* из меню **Пуск (Start)**.

- Пометьте файл или файлы, которые хотите расшифровать (верифицировать).

Вы можете пометить несколько файлов, но расшифровываться (верифицироваться) они будут по отдельности.

- Выберите опцию **Decrypt/Verify** из меню **Файл (File)** или из контекстного меню, вызываемого щелчком правой кнопкой мыши.

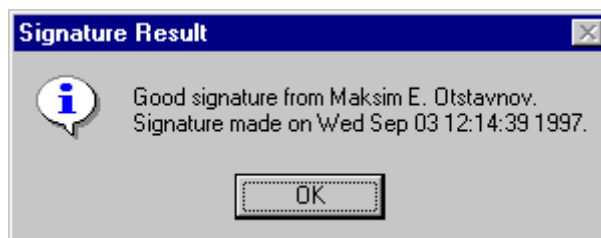
При расшифровке появится *Диалоговое окно пароля (Passphrase)*, требующее от вас ввести пароль.

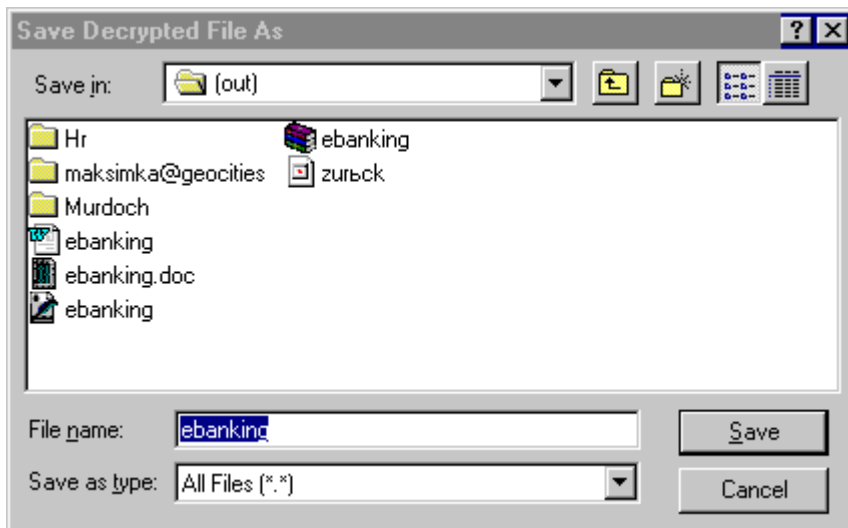


- Введите пароль и щелкните **ОК**.

Если файл подписан, появится окно с информацией о том, успешно ли прошла верификация подписи.

- Щелкните **ОК**. Появится окно диалога выбора выходного файла (*Save Decrypted File As*).





6. Укажите местоположение и введите имя файла, в котором должен быть сохранен расшифрованный файл.  
Если вы явно не укажете имя файла, будет использовано имя исходного файла.
7. Чтобы сохранить файл щелкните **Save**.  
Расшифрованный файл будет сохранен в указанном месте.

## Глава 5

### Управление ключами и установка предпочтений

В этой главе объясняется, как исследовать свойства ключей, хранящихся на ваших связках, и управлять ими. Также описывается установка пользовательских предпочтений для настройки на конкретную среду исполнения.

#### Управление ключами

Ключи, которые вы генерируете, а также открытые ключи, получаемые от других, хранятся на связках, которые, в сущности, представляют собой файлы на жестком или гибком диске. Обычно связка закрытых ключей хранится в файле `secring.skr`, а связка открытых – в `pubring.pkr`. Эти файлы, как правило, располагаются в той же папке, в которую установлена *PGP*. Для символизации файлов со связками ключей используются два особых значка, благодаря которым их можно легко обнаружить при просмотре содержимого папок.



связка закрытых ключей



связка открытых ключей

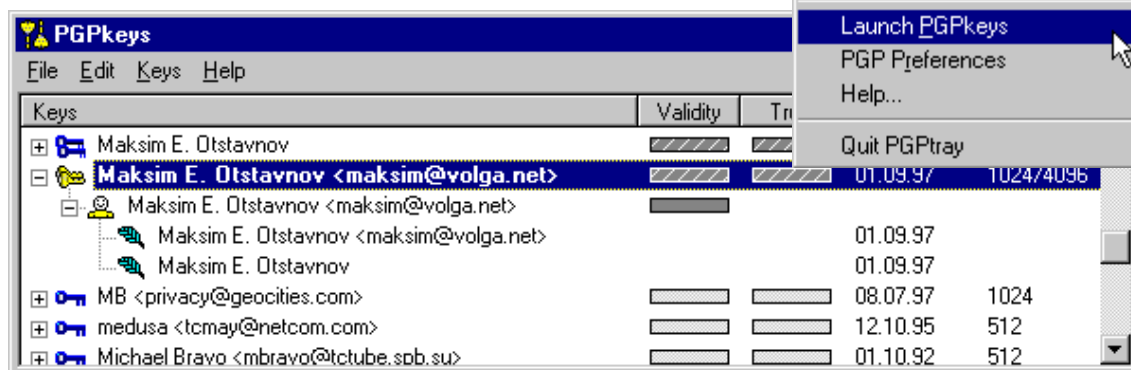
*Примечание:* В случае, если вы пользуетесь более, чем одной парой своих ключей, или вам неудобно хранить связки в обычном месте, вы можете выбрать другие имена и другое их местоположение. Это описано ниже в разделе “Установка предпочтений”.

Временами вам может понадобиться исследовать или изменить атрибуты какого-либо ключа. Например, когда вы получаете чей-либо открытый ключ, вы можете захотеть определить его тип (*RSA* или *DSS/Diffie-Hellman*), проверить его отпечаток или определить действительность на основе сертифицирующих его подписей. Вы можете также захотеть подписать чей-либо открытый ключ, чтобы дать знать, что вы уверены в его действительности, присвоить ключу определенный уровень надежности или изменить пароль доступа к своему закрытому ключу. Все эти функции управления ключами доступны из окна *PGPkeys*.

## Окно PGPkeys

Чтобы открыть окно *PGPkeys*, щелкните мышью на значке с конвертом и ключом в Области системных индикаторов Панели задач.

В окне *PGPkeys* вы увидите пары ключей, сгенерированные вами, а также все открытые ключи других пользователей, которые вы собрали.



Значки с двойным ключом символизируют пары из закрытого и открытого ключей, сгенерированные вами, а одиночные ключи обозначают открытые ключи, полученные вами от других. Если у вас есть ключи разных типов, вы заметите, что *RSA*-ключи символизируются синими значками, а *DSS/DH* – желтыми.

Щелкнув два раза на любом ключе, вы распахнете список, в котором будут отображены имена (и адреса) владельца, каждое из которых символизируется значком с человечком. Щелкнув два раза на этом значке, вы увидите подписи всех тех, кто сертифицировал этот ключ. Каждая из них отображается значком с изображением пера. Если вам не нравятся двойные щелчки как способ перехода от одного уровня информации к другому, просто пометьте интересующие вас ключи и выберите пункт **Expand Selection** из меню **Edit**.

## Определение атрибутов PGPkeys

Вдоль верха главного окна расположены метки (labels), соответствующие атрибутам каждого ключа.

**Keys (Ключи)** – символическое представление ключа, сопровождаемое именем и адресом его владельца.

**Действительность (Validity)** – отображает степень уверенности в том, что ключ принадлежит номинальному владельцу. Действительность ключа вычисляется, исходя из того, кто сертифицировал ключ и насколько вы доверяете речам этих лиц. Открытый ключ, который вы сертифицировали сами, обладает наибольшим уровнем действительности. Это основывается на допущении, что вы подпишите чей-либо ключ лишь тогда, когда будете полностью уверены в том, что он принадлежит номинальному владельцу. Действительность не подписанных лично вами ключей определяется исходя из уровня доверия, присвоенного вами третьим лицам, которые их сертифицировали. Если ключ не сертифицирован никакими подписями,

он рассматривается как недействительный, и надпись, уведомляющая об этом, появляется при любой попытке его использования.








**Надежность (Trust)** – указывает уровень доверия, которое вы присвоили владельцу ключа в смысле его способности быть посредником при сертификации ключей третьих лиц. Это значение используется, когда вы сами не можете определить действительность чье-либо открытого ключа и решаете положиться на суждение третьих лиц, которые его сертифицировали. Когда вы генерируете свою пару ключей, они имплицитно считаются заслуживающими доверия, что символизируется полосками в полях действительности и надежности. Когда вы получаете открытый ключ, который был подписан кем-то, чей открытый ключ уже находится на вашей связке, подлинность определяется, исходя из уровня надежности, который вы присвоили ключу сертифицировавшего новый ключ пользователя. Вы можете указать уровень надежности (*Надежный (Complete)*, *Отчасти надежный (Marginal)* или *Ненадежный (Untrusted)*) в окне диалога *Properties*).







**Создание (Creation)** – показывают дату генерации ключа. Иногда знание даты позволяет сделать некоторые предположения о действительности ключа, основываясь на том, как долго он был в использовании. Если ключ уже используется некоторое время, вероятность того, что его кто-нибудь подменит, становится меньше, поскольку в обращении находится большее число его копий.

**Длина (Size)** – показывает количество бит, составляющих ключ. В общем, чем длиннее ключ, тем меньше вероятность того, что он будет скомпрометирован. Однако, длинные ключи требуют несколько большего времени на шифрование и расшифровку, чем более короткие. Когда вы создаете пару ключей *DSS/DH*, длине компонента *DSS* соответствует одно число, а компоненту *DH* – другое.

### Определение значков PGPkeys

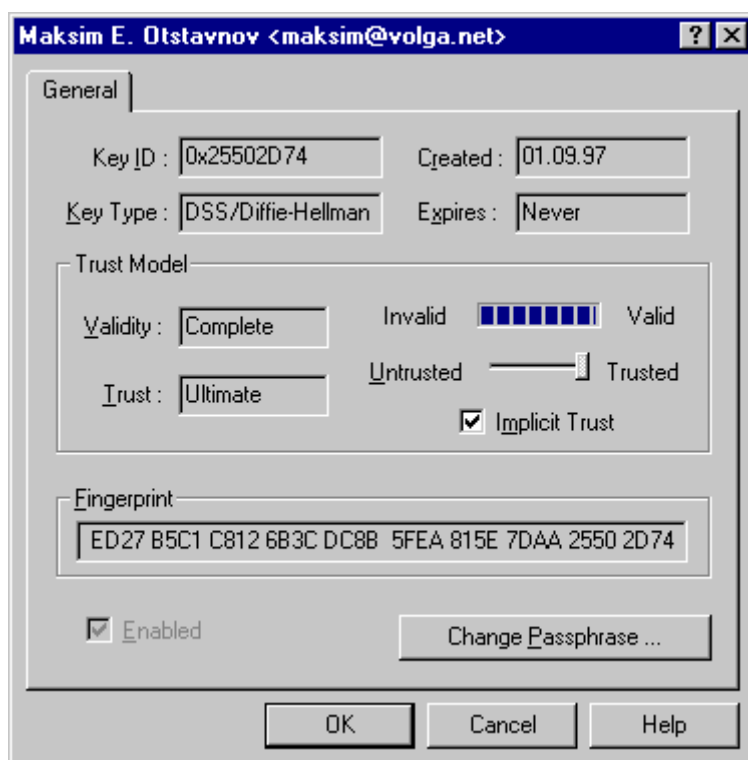
Ниже приведены все значки, используемые в окне *PGPkeys*, и описание того, что они обозначают.

	<b>Пара желтых ключей</b> символизирует вашу пару ключей типа <i>DSS/DH</i> . Пара состоит из закрытого и открытого ключей.
	<b>Одиночный желтый ключ</b> символизирует открытый ключ типа <i>DSS/DH</i> .
	<b>Пара синих ключей</b> символизирует вашу пару ключей типа <i>RSA</i> . Пара состоит из закрытого и открытого ключей.
	<b>Одиночный синий ключ</b> символизирует открытый ключ типа <i>RSA</i> .
	Когда ключ или пара ключей изображены <b>серым цветом</b> , это означает, что их использование временно запрещено. Вы можете запретить использование ключа (и предотвратить таким образом захламенение списка в окне диалога выбора ключа).
	Изображение ключа, перечеркнутое <b>красной линией</b> , означает, что ключ отозван. Пользователи отзывают свои ключи, ставшие недействительными или каким-либо образом скомпрометированными. Изображение ключа, перечеркнутое <b>двумя красными линиями</b> , означает, что ключ неправильный.
	Изображение <b>ключа с часами</b> означает, что срок действия ключа завершился. Срок действия ключа задается при генерации пары.

-  **Улыбающаяся рожица** символизирует владельца ключа и список имен и адресов, связанных с ключом.
- 
-  **Перо** обозначает подпись третьего лица, ручающегося за его подлинность. **Перечеркнутая красной линией** подпись – это отозванная подпись, а **перечеркнутая двумя красными линиями** – недействительная или испорченная.
- 
-  **Пустой прямоугольник** означает недействительный ключ или ненадежного пользователя.
- 
-  **Наполовину заполненный прямоугольник** означает отчасти действительный ключ или отчасти надежного пользователя.
- 
-  **Заполненный прямоугольник** означает действительный ключ или надежного пользователя.
- 
-  **Полосатый прямоугольник** означает имплицитно действительный ключ и имплицитно надежный ключ. Эти значения присваиваются только сгенерированным вами самим парам ключей.

### Исследование свойств ключей

Кроме общих атрибутов, отображаемых в главном окне *PGPkeys*, вы можете исследовать и изменять другие свойства ключей. Чтобы добраться до свойств конкретного ключа, пометьте его и выберите пункт **Key Properties** из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши.



**Идентификатор ключа (Key ID)** – уникальное число, связанное с ключом.

Идентификатор ключа нужен для того, чтобы различать разные ключи, носящие одинаковое имя пользователя и почтовый адрес.

**Создан (Created)** – дата, когда был создан ключ.

**Тип ключа (Key Type)** – тип ключа может быть *RSA* или *DSS/DH*.

**Срок действия (Expires)** – дата, когда истекает срок годности ключа.

Владелец указывает эту дату при генерации новой пары и значение

этого атрибута обычно *никогда (never)*. Однако, некоторые ключи имеют определенный срок действия, если владелец захотел создать их для использования в течение определенного периода времени.

**Модель доверия (Trust Model)** – отображает действительность ключа, основываясь на сертифицирующих его подписях и уровне надежности, приданном тем, кто эти подписи наложил. Вы можете установить уровень надежности, передвигая прямоугольник к соответствующему значению (*Надежный (Complete)*, *Отчасти надежный (Marginal)*, *Ненадежный (Untrusted)*).

**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 у вас копии. Вы также можете проверить подлинность чье-либо ключа, сравнив отпечаток имеющейся у вас копии с отпечатком копии, хранящейся на сервере открытых ключей, предполагая, что владелец периодически проверяет, не была ли эта копия подменена.

**Разрешен (Enabled)** – это поле указывает, разрешено ли использование этого ключа. Временно запрещенный к использованию ключ отображается в главном окне *PGPkeys* серым цветом, и с его помощью невозможно выполнять какие-либо операции *PGP*. Однако, такой ключ остается на вашей связке и как только он вам понадобится, вы сможете снова разрешить его использование. Для того, чтобы разрешить или запретить использование ключа, пометьте или очистите поле *Enable*, или выберите соответствующую опцию (*Enable* – разрешить, *Disable* – запретить) из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши.

**Изменить пароль (Change Passphrase)** – изменить пароль доступа к закрытому ключу. Если вы когда-либо решите, что ваш пароль более не является секретом, известным только вам (например, заметите, что кто-то подглядывал, когда вы его набирали), щелкните на этой кнопке, чтобы ввести новый пароль.

#### Указание пары ключей, используемой по умолчанию

Когда вы подписываете сообщение или ключ, используется ваш ключ по умолчанию. Если вы обладаете более чем одной парой ключей, вам может понадобиться явно обозначить одну пару, которая будет использоваться по умолчанию. Текущая пара по умолчанию выделяется в окне *PGPkeys* жирным шрифтом для того, чтобы ее можно было отличить от остальных пар.

#### Как указать пару по умолчанию

1. Пометьте пару ключей, которую вы хотите использовать по умолчанию.
2. Выберите из меню **Keys** пункт **Set As Default Key**.

Помеченная пара станет выделена жирным шрифтом, что указывает на ее использование по умолчанию.

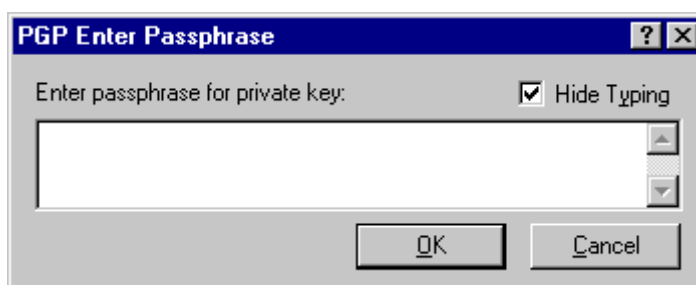
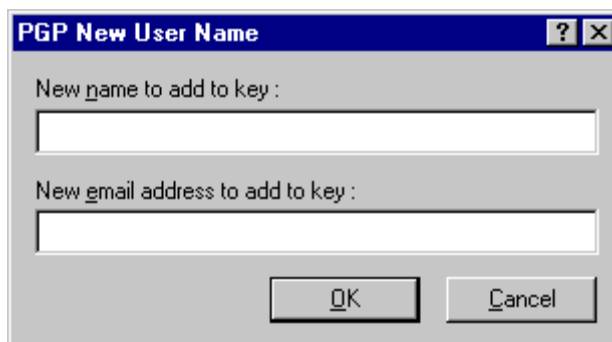
#### Добавление нового имени или адреса

В некоторых случаях вам может понадобиться более чем одно имя или адрес, которые вы захотите связать с одной и той же парой ключей. После того, как

пара ключей сгенерирована, вы можете добавить к ней дополнительные имена или адреса. Добавить новое имя или адрес вы можете только в случае, если обладаете обоими ключами, составляющими пару.

#### Как добавить к существующему ключу новое имя или адрес

1. Выберите пару ключей, к которой вы хотите добавить новое имя или адрес.
2. Выберите из меню **Keys** (или из контекстного меню, доступного при щелчке правой кнопкой мыши) пункт **Add Name**. Появится окно Диалога ввода нового имени (New User Name).
3. Введите новое имя, затем нажатием *Tab* переместите курсор в следующее поле.
4. Введите новый адрес.
5. После ввода имени и адреса щелкните **ОК**. Появится окно Диалога ввода пароля (Enter Passphrase).
6. Введите свой пароль и щелкните **ОК**.



Новое имя будет добавлено в конец списка имен, связанных с ключом. Если вы захотите сделать это имя и адрес первичным идентификатором, пометьте его и выберите пункт **Set As Primary User ID** из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши.

#### Проверка отпечатка ключа

Часто трудно быть уверенным, что ключ принадлежит определенному лицу, если вы не получили этот ключ непосредственно от него на дискете. Такой способ обмена ключами не всегда практичен, особенно для пользователей, живущих на расстоянии многих километров друг от друга, так что вы можете положиться на уникальный отпечаток, связанный с каждым ключом, чтобы убедиться, что ключ действительно принадлежит номинальному владельцу. Для проверки отпечатка ключа существуют разные способы, но наиболее надежно – позвонить владельцу и попросить его прочитать отпечаток по телефону. Крайне маловероятно, что звонок кто-либо перехватит и сумеет симитировать голос вашего собеседника. Вы также можете сравнить отпечаток вашей копии чье-либо открытого ключа с отпечатком копии, хранящейся на сервере.

#### Как проверить отпечаток ключа

1. Пометьте ключ, отпечаток которого вы хотите проверить.
2. Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Key Properties**.



3. Посмотрите на отпечаток (*Fingerprint*) и сравните его с оригиналом.

### Сертификация чужого открытого ключа

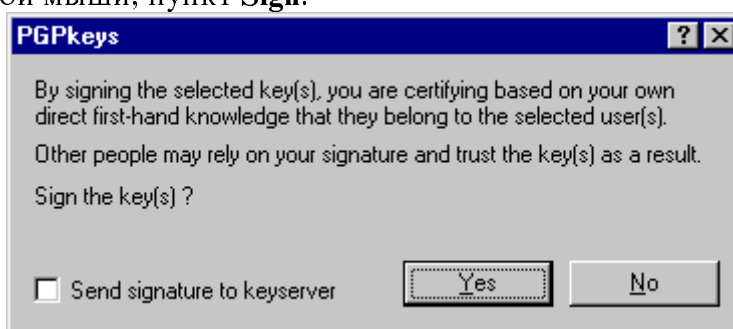
Когда вы генерируете пару ключей, она автоматически подписывается с помощью вашего закрытого<sup>7</sup> ключа. Точно так же, после того, как вы убедились, что открытый ключ принадлежит его номинальному владельцу, вы можете подписать (сертифицировать) этот ключ, указывая, что вы уверены в действительности оною.

### Как подписать чужой открытый ключ

1. Пометьте ключ, который хотите подписать.
2. Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Sign**.

Появится окно предупреждения (*Alert Box*).

3. Щелкните **Yes**, чтобы подтвердить, что вы действительно уверены в том, что



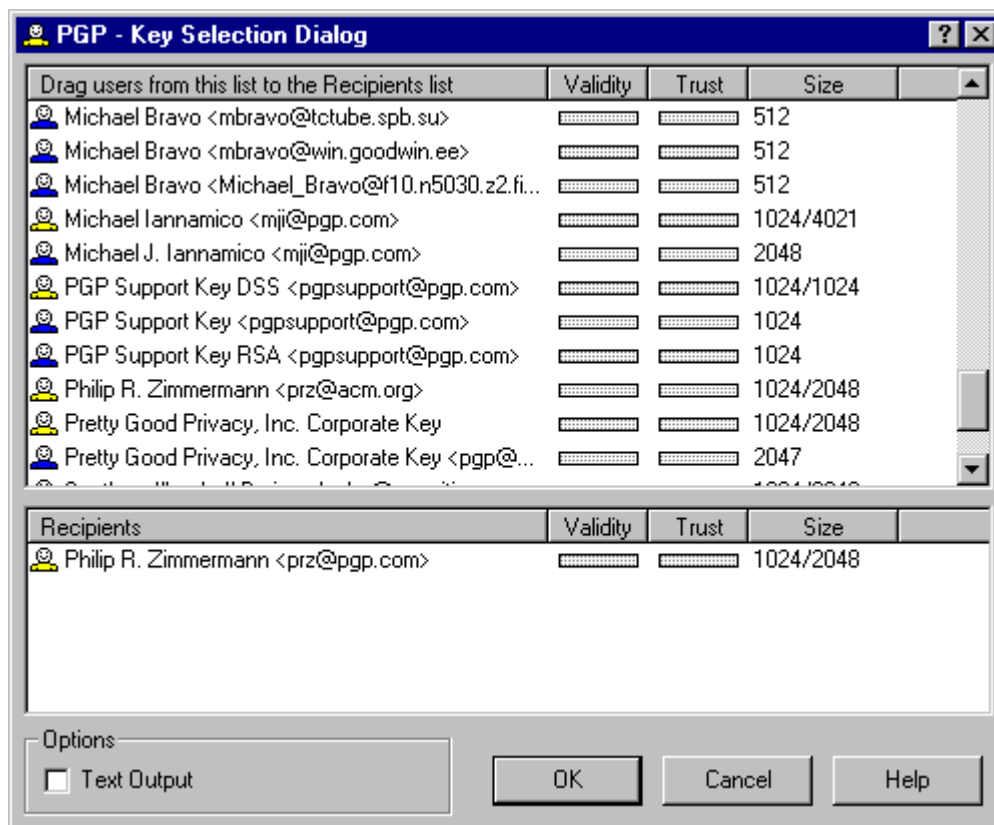
ключ принадлежит номинальному владельцу.

Если вы хотите послать этот ключ со своей подписью на сервер ключей, пометьте поле *Send signature to keyserver*. Копия этого ключа на сервере будет обновлена с тем, чтобы отразить включение вашей подписи. Так как большинство пользователей предпочитают сами решать, чьи подписи должны присутствовать на копии ключа, хранящейся на сервере, неплохо посоветоваться с владельцем ключа до того, как отправлять вновь подписанный ключ на сервер.

Появится окно Диалога ввода пароля (*Enter Passphrase*).

---

<sup>7</sup> В оригинале – ошибочно – "*using your public key*".



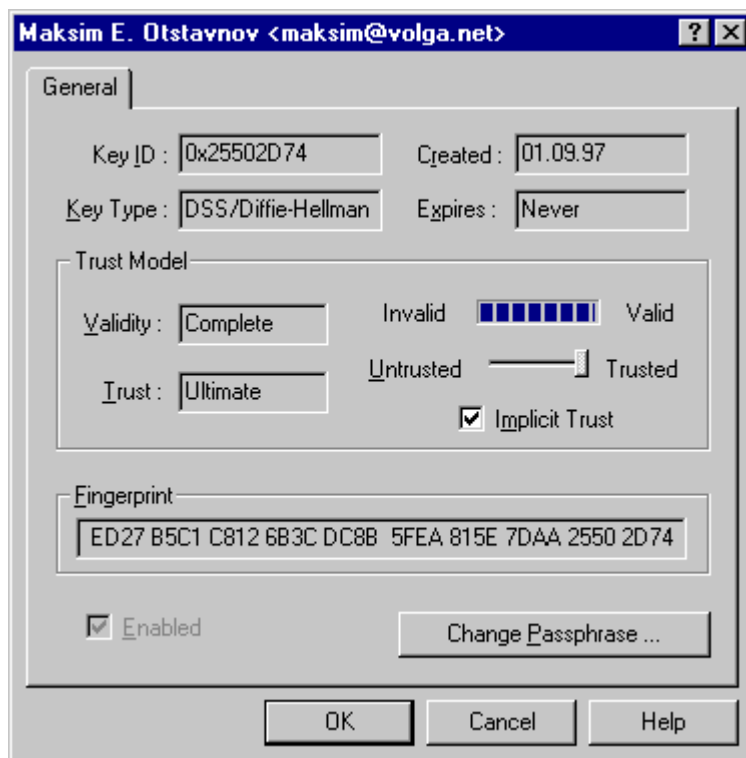
4. Введите свой пароль и щелкните **ОК**. Если у вас есть другая пара ключей, и вы хотите подписать ключ с ее помощью, вы можете нажать на стрелку и выбрать нужный ключ.
5. После того, как вы сертифицировали ключ, в списке сопровождающих его подписей появится строчка со значком пера и вашим именем.

#### Указание уровня доверия

Кроме сертификации принадлежности ключа владельцу, вы можете присвоить его владельцу определенный уровень доверия, указывающий, насколько вы доверяете ему выступать в качестве посредника, ручающегося за целостность ключей, которые вы можете получить в будущем. Это значит, что если вы когда-либо получите от кого-либо ключ, подписанный лицом, которого вы обозначили как заслуживающего доверия, ключ может рассматриваться как действительный, даже если вы не проверяли его подлинность сами.

#### Как присвоить ключу уровень доверия

1. Пометьте ключ, уровень доверия к владельцу которого вы хотите изменить.
2. Выберите из меню **Key** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Key Properties**. Появится окно Диалога свойств ключа (Properties).



3. Используйте движок уровня доверия (*Trust Level*) для установки соответствующего уровня доверия. Вы можете выбрать между уровнями (*Надежный (Complete)*, *Отчасти надежный (Marginal)* или *Ненадежный (Untrusted)*) в окне диалога *Properties*.
4. Для завершения операции щелкните **OK**.

### Запрет и разрешение использования ключей

Иногда вам может понадобиться временно запретить использование ключа. Эта возможность полезна, когда вы хотите сохранить ключ для использования в будущем, но не хотите, чтобы лишние ключи загромождали окно Диалога выбора получателя каждый раз при отправке почты.

#### Как запретить использование ключа

1. Пометьте ключ, использование которого хотите запретить.
2. Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Disable**.

Ключ станет отображаться серым цветом и будет временно запрещен к использованию.

#### Как разрешить использование ключа

1. Пометьте ключ, использование которого хотите разрешить.
2. Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Enable**.

Ключ станет отображаться обычным цветом и будет разрешен к использованию.

### Удаление ключа, подписи или идентификатора пользователя

В какой-то момент вам может понадобиться удалить ключ, сертифицирующую его подпись или идентификатор пользователя, связанный с конкретным ключом.

### Как удалить ключ, подпись или идентификатор пользователя

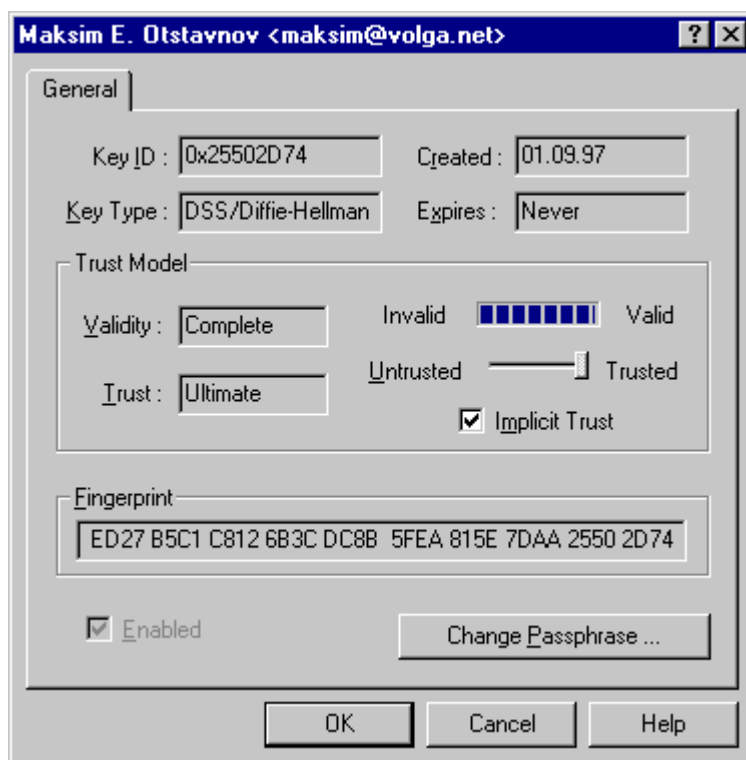
1. Пометьте ключ, подпись или идентификатор пользователя, который хотите удалить.
2. Выберите из меню **Edit** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Delete**.

### Изменение пароля доступа

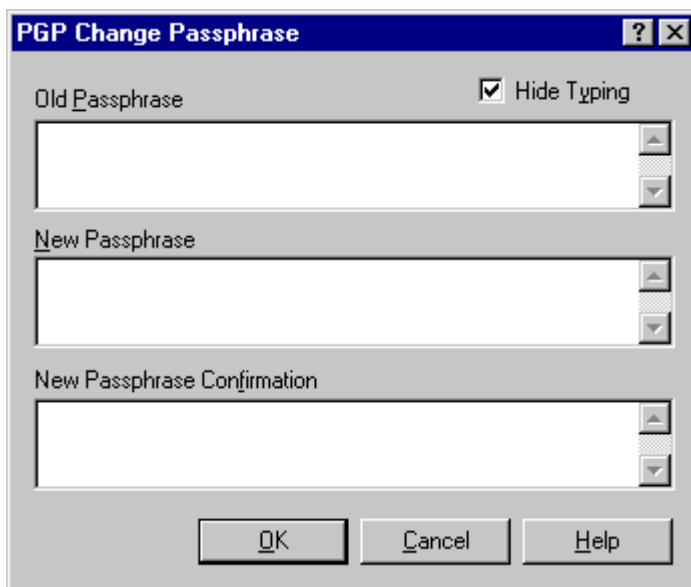
Периодически менять пароль доступа к закрытому ключу – неплохая идея. Если вы хотите изменить пароль, сделать это очень просто.

### Как изменить пароль

1. Пометьте пару ключей, пароль доступа к которой хотите изменить.
2. Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Key Properties**. Появится окно Диалога свойств ключа (Properties).



3. Щелкните на кнопке изменения пароля **Change Passphrase**. Появится окно Диалога смены пароля (Change Passphrase).



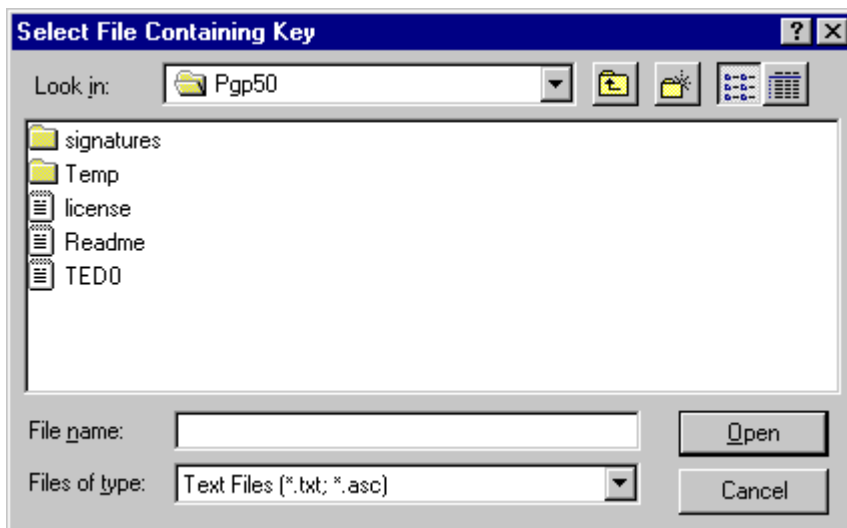
4. Введите свой старый пароль в верхнем поле и нажмите *Tab* для перехода к следующему полю.
5. Введите свой новый пароль в среднем поле и нажмите *Tab* для перехода к нижнему полю.
6. Подтвердите новый пароль, введя его в нижнем поле еще раз.
7. Щелкните **ОК**.

#### Импорт и экспорт ключей

Хотя вы чаще распространяете свой открытый ключ и получаете открытые ключи других посредством сервера открытых ключей, обмениваться ключами можно также импортируя и экспортируя их в виде текстовых файлов. Например, кто-то может передать вам свой открытый ключ на дискете или вы можете захотеть сделать свой ключ доступным через FTP-сервер.

#### Как импортировать ключ из файла

1. Выберите пункт **Import** из меню **Keys**.  
Появится окно Диалога выбора файла, содержащего ключ (Select File Containing Key).

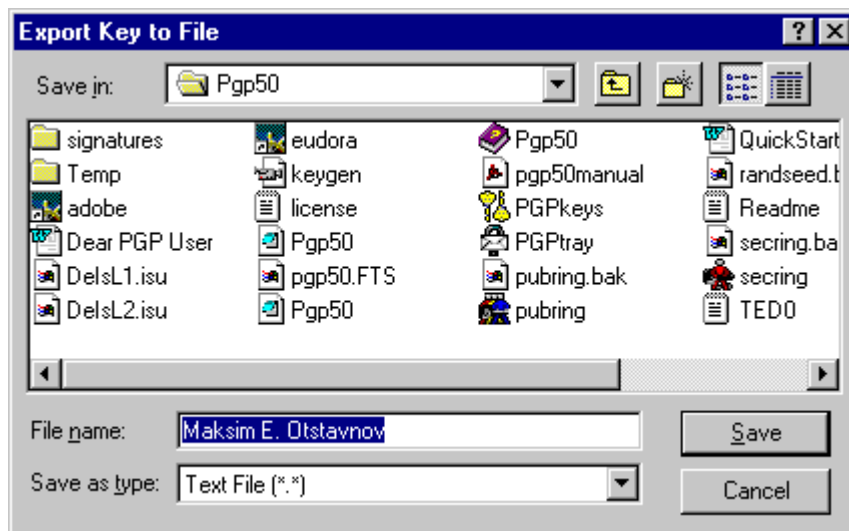


2. Выберите файл, содержащий ключ, который вы хотите импортировать, и щелкните **Open**.

В окне *PGPkeys* появится вновь импортированный ключ, который теперь можно использовать для шифрования данных и верификации подписи его владельца.

#### Как экспортировать ключ в файл

1. Пометьте ключ, который хотите экспортировать в файл.
2. Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Export**.  
Появится окно Диалога выбора файла (Export Key to File).



3. Введите имя файла, в который хотите экспортировать ключ, и щелкните **Save**.

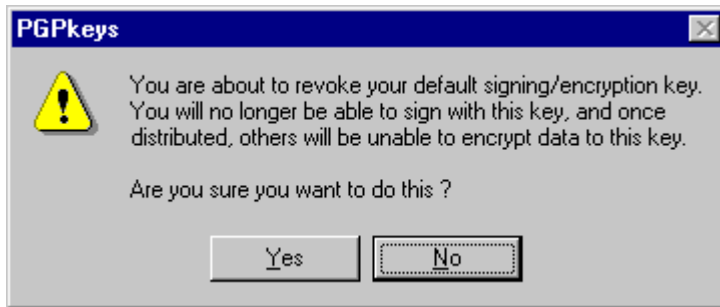
Экспортированный ключ будет помещен в файл с заданным именем и указанным местоположением.

#### Отзыв ключа

Если когда-либо возникнет ситуация, в которой вы не сможете больше доверять своей персональной паре ключей, вы можете выпустить сертификат отзыва ключа, сообщающий всем, что ваш соответствующий открытый ключ не должен более использоваться. Лучший способ распространить сертификат отзыва – это поместить его на сервер открытых ключей.

#### Как отозвать ключ

1. Пометьте пару ключей, которую хотите отозвать.
2. Выберите из меню **“Keys”** “ или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **“Revoke”**.  
Появится сообщение с краткой информацией о последствиях отзыва ключа и вопрос, действительно ли вы хотите его отозвать.



3. Для подтверждения намерения отозвать ключ щелкните **Yes**. Появится окно *Диалогов ввода пароля (Enter Passphrase)*, в котором нужно ввести ваш пароль доступа.



4. Введите пароль и щелкните **OK**. Отозванный ключ символизируется изображением ключа, перечеркнутым красной линией.
5. Отправьте отозванный ключ на сервер, чтобы все знали, что пользоваться им более нельзя.

Может так случиться, что вы вдруг забудете свой пароль. В этом случае вы уже не сможете использовать свой ключ, и у вас даже не будет возможности его отозвать, когда вы создадите новый. В качестве меры предосторожности, вы можете заранее создать сертификат отзыва, сделав копию своей пары, отозвав ее и сохранив отозванный ключ в каком-либо надежном месте. Затем, если вы забудете пароль, вы сможете отправить этот сертификат на сервер открытых ключей. Однако, следует быть очень внимательным при выборе места хранения такого заранее созданного сертификата отзыва. Ведь если до него кто-нибудь доберется, он сможет отозвать ваш ключ и опубликовать вместо него сгенерированный им самим.

### Установка пользовательских предпочтений

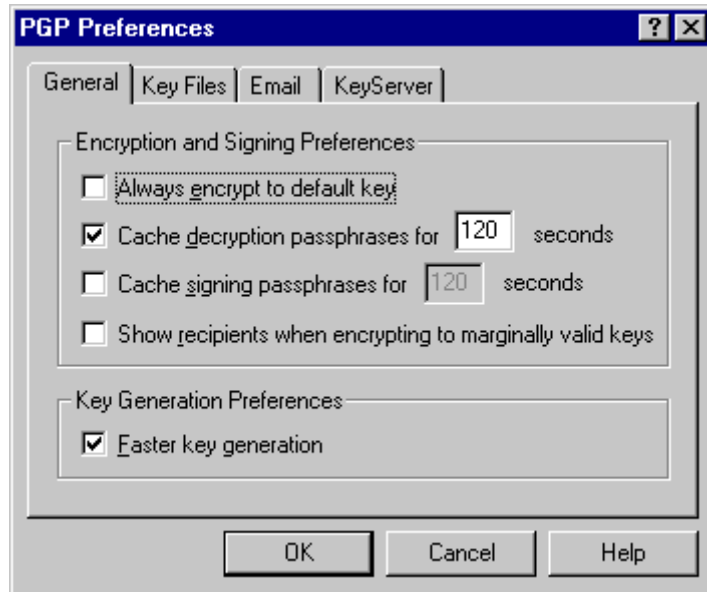
*PGP* сконфигурирована таким образом, чтобы удовлетворять потребностям большинства пользователей, но вам предоставляется возможность изменять некоторые установки, чтобы лучше приспособить программу к вашей конкретной среде исполнения. Эти установки вы можете изменить из окна Диалогов предпочтений (*Preferences*), к которому можно получить доступ следующими способами:

- щелкните значок с ключом и конвертом в Области системных индикаторов, и выберите пункт **Preferences**;
- выберите **Preferences** из меню **Edit** в окне *PGPkeys*.

## Общие предпочтения

Общие предпочтения устанавливаются с помощью вкладки *General* окна **Preferences**.

**Всегда шифровать с помощью ключа по умолчанию (Always Encrypt to Default Key)** – когда установлена эта опция, все сообщения и файлы, шифруемые с помощью открытого ключа получателя, шифруются также и с помощью вашего ключа по умолчанию.



Эту опцию полезно включить, если вы хотите иметь возможность последующей расшифровки содержимого любого зашифрованного сообщения или файла.

**Кэшировать пароль для расшифровки в течение [ ] секунд (Cache Decryption Passphrase for [ ] Seconds)** – этот параметр указывает период времени (в секундах), в течение которого ваш пароль для расшифровки сохраняется в оперативной памяти компьютера. Если вы регулярно читаете по несколько зашифрованных сообщений подряд, вам может понадобиться увеличить значение этого параметра, чтобы не вводить пароль снова и снова при чтении каждого сообщения. Однако, вы должны иметь в виду, что чем дольше пароль сохраняется в памяти, тем больше времени у хитроумной программной закладки, чтобы получить доступ к этой чрезвычайно секретной информации. По умолчанию, этот параметр устанавливается равным 120 сек., чего должно быть достаточно для выполнения большинства функций *PGP* без необходимости вводить пароль слишком часто, но что не слишком долго для возможности перехвата пароля.

**Кэшировать пароль для подписи в течение [ ] секунд (Cache Signing Passphrase for [ ] Seconds)** – этот параметр указывает период времени (в секундах), в течение которого ваш пароль для подписи сохраняется в оперативной памяти компьютера. Если вы регулярно подписываете по несколько сообщений подряд, вам может понадобиться увеличить значение этого параметра, чтобы не вводить пароль снова и снова при наложении подписи на каждое сообщение.

**Указывать получателей при шифровке с помощью отчасти надежных ключей (Show Recipients When Encrypting To Marginally Valid Keys)** – эта опция указывает, что вы будете предупреждены при шифровании с помощью отчасти надежного ключа.

**Быстрая генерация ключа (Faster Key Generation)** – когда установлена эта опция, генерация ключей по новой технологии *DSS/DH* занимает меньше времени. Этот процесс ускоряется за счет использования предварительно сгенерированного набора простых чисел вместо выполнения долгой процедуры генерации длинных простых при генерации каждого ключа. Вы должны знать, что быстрая генерация



ключа реализована лишь для фиксированных длин ключей, приводимых в списке длин, предоставляемом при генерации, и не может быть использована при генерации ключей другой длины. Хотя кажется практически невозможным, что злоумышленнику удастся использовать этот “консервированный” набор простых чисел для взлома вашего ключа, вы можете, отключив эту опцию, ценой затраты дополнительного времени создать пару ключей с максимальным уровнем надежности.

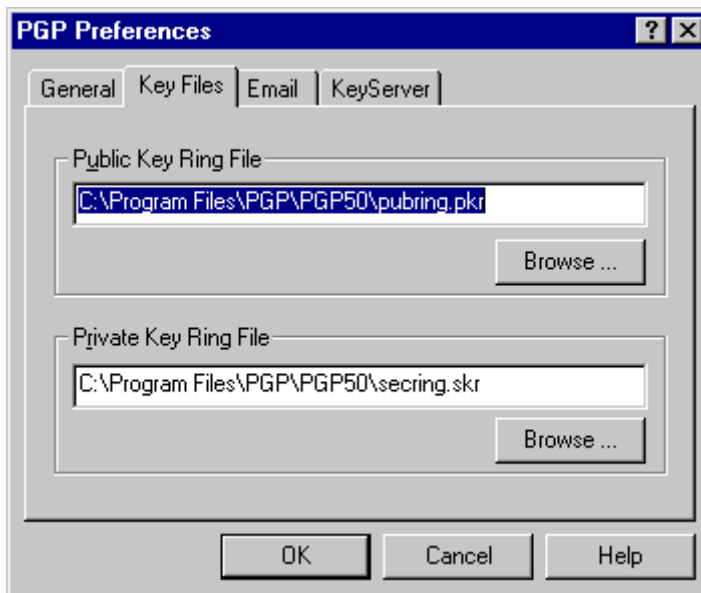
### Предпочтения файлов со связками ключей

Для перехода к вкладке *Предпочтений файлов (Key Files Preferences)*, из которой вы можете изменять местоположение файлов со связками ключей, щелкните на закладке **Key Files**.

**Файл со связкой открытых ключей (Public Key Ring File)** – указывает текущее местоположение и имя файла, в котором *PGP* ожидает найти вашу связку открытых ключей. Если вы

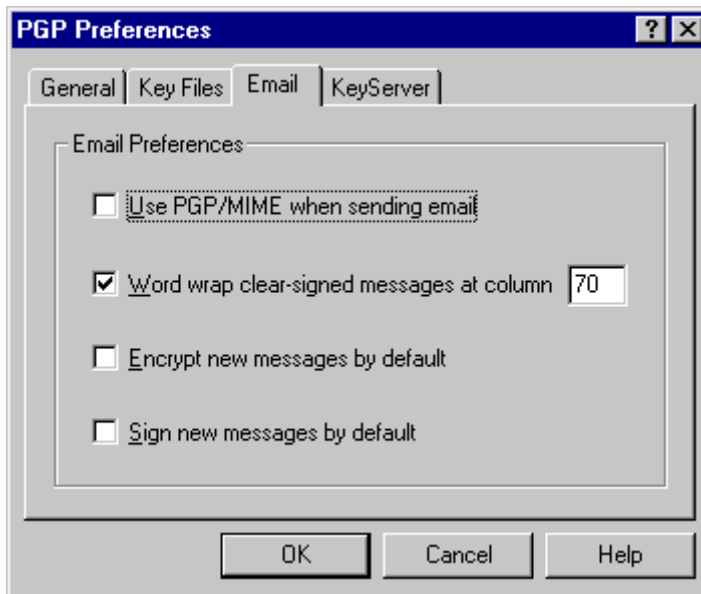
собираетесь хранить открытые ключи в файле с другим именем или в другом месте, укажите его здесь. Вместо того, чтобы явно задавать путь, вы можете использовать кнопку “Browse” для пролистывания доступных дисков и папок.

**Файл со связкой закрытых ключей (Private Key Ring File)** – указывает текущее местоположение и имя файла, в котором *PGP* ожидает найти вашу связку закрытых ключей. Если вы собираетесь хранить закрытые ключи в файле с другим именем или в другом месте, укажите его здесь. Некоторые пользователи предпочитают хранить закрытые ключи на гибком диске, который они вставляют, как ключевую дискету, только на время, пока подписывают или расшифровывают почту.



## Предпочтения работы с почтой

Для перехода к вкладке *Предпочтений работы с почтой (E-mail Preferences)*, из которой вы можете изменять параметры работы с почтой для тех почтовых пакетов, которые поддерживаются посредством встраиваемых модулей, щелкните на закладке **Email**. Обратите внимание, что опция *PGP/MIME* реализована не для всех почтовых пакетов.



### **Использовать PGP/MIME при отправке почты (Use PGP/MIME When Sending e-mail)**

– когда установлена эта опция, вам не требуется каждый раз включать опцию *PGP/MIME* при отправке почты. Например, если вы используете почтовый пакет Eudora, то при включении этой опции, все ваши сообщения и файлы, отправляемые в качестве приложений, будут автоматически шифроваться ключами получателей и подписываться. Эта опция не влияет на другие процедуры, которые вы выполняете над содержимым Буфера обмена и файлами в Проводнике. Она также не должна использоваться, если вы собираетесь отправлять почту получателям, пользующимся почтовыми пакетами, не поддерживающими стандарт *PGP/MIME*.

**Сворачивать текст подписанных текстовых сообщений в позиции [ ] (Word wrap clear-signed messages at column [ ])** – этот параметр указывает позицию, в которой вставляется символ перевода строки для сворачивания текста подписанных текстовых сообщений. Он необходим, поскольку разные почтовые пакеты выполняют сворачивание текста разным способом, а это может разрушить структуру подписанного текстового сообщения и привести к невозможности верификации подписи. По умолчанию, значение этого параметра установлено равным 78, что решает данную проблему для большинства пакетов.

**Шифровать сообщения по умолчанию (Encrypt New Messages by Default)** – делает функцию шифрования исходящей почты в почтовом пакете включенной по умолчанию. Значок с замком будет утоплен, показывая, что функция шифрования включена.

**Подписывать сообщения по умолчанию (Sign New Messages by Default)** -- делает функцию наложения подписи на исходящую почту в почтовом пакете включенной по умолчанию. Значок с пером будет утоплен, показывая, что функция шифрования включена.

### Предпочтения сервера ключей

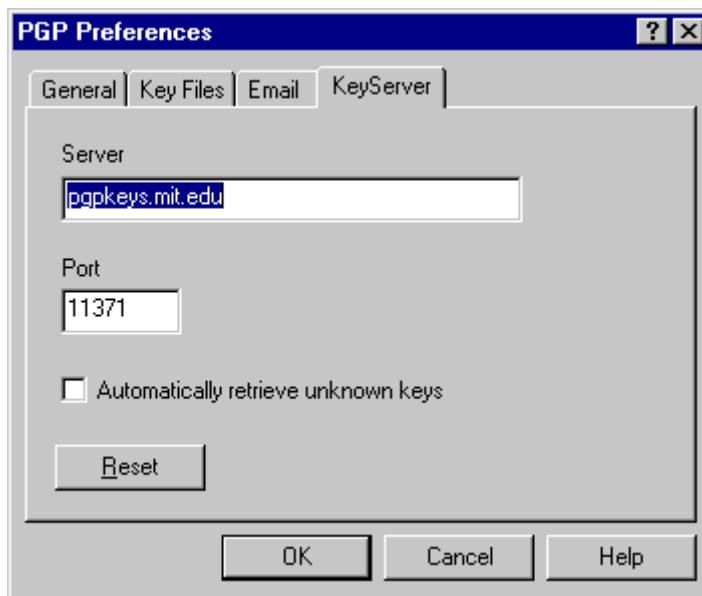
Для перехода к вкладке *Предпочтений сервера ключей* (*Key Server Preferences*), из которой вы можете изменять указывать параметры используемого сервера ключей, щелкните на закладке **Key Server**.

**Сервер (Server)** – указывает URL (Internet-адрес) сервера, который используется *PGP* для отправки и получения открытых ключей. Вам не нужно изменять его, его вы не хотите работать с другим сервером.

**Порт (Port)** – компонент “порт” URL сервера открытых ключей.

**Автоматически запрашивать неизвестные ключи (Automatically Retrieve Unknown Keys)** – когда установлена эта опция, отсутствующий на связке открытый ключ получателя будет запрашиваться с сервера при шифровании или верификации почты.

**Сброс (Reset)** – возвращает полям “Server” и “Port” значения по умолчанию.



## Глава 6

### Особенности модели безопасности и уязвимые места

Эта глава, написанная Филом Зиммерманном, содержит вводную и базовую информацию о криптографии.

*“То, что вы делаете, останется неважным, но очень важно, что вы это делаете”* – Махатма Ганди

#### Зачем я написал PGP

Это личное. Это приватное. И это не касается никого, кроме вас. Возможно, вы планируете политическую кампанию, обсуждаете свои налоговые проблемы, или у вас тайный роман. Возможно, вы переписываетесь с политическим диссидентом из страны с репрессивным режимом. Чего бы это ни касалось, вы не желаете, чтобы ваши частные письма, отправляемые электронной почтой, или конфиденциальные документы читались кем-то еще. Нет ничего дурного в том, чтобы стремиться к приватности. Приватность – такая же американская штука, как и наша Конституция.

Правом на приватность неявно пропитан весь Билль о правах. Но когда писалась Конституция, отцы-основатели не видели необходимости в явном провозглашении права на приватное общение. Это было бы глупо: двести лет назад все общение было приватным. Если в пределах поля слышимости появлялся кто-то еще, вы просто отходили за сарай, и продолжали разговор. Никто не мог подслушать вас без вашего ведома. Право на приватное общение было естественным правом, и не только в философском смысле, но и в смысле законов физики, учитывая уровень тогдашних технологий.

Но с приходом информационной эры, которая началась с изобретения телефона, все изменилось. Теперь мы общаемся в основном с помощью электроники. Это приводит к тому, что наши самые интимные разговоры могут стать достоянием посторонних, а мы об этом даже не узнаем: разговоры по сотовому телефону могут прослушиваться каждым, у кого есть радиоприемник; отправка по Интернет электронной почты ничуть не безопаснее, чем разговоры по сотовому телефону. Последняя, теряя новизну, быстро вытесняет почту бумажную, ее использование становится нормой. Но электронная почта может рутинно и автоматически сканироваться на предмет наличия интересующих кого-либо ключевых слов, в больших объемах и без возможности распознавания – это похоже на ловлю рыбы дрейферной сетью.

Возможно, вы полагаете, что ваша электронная почта не содержит ничего предосудительного, и шифровать ее нет необходимости. Если вы – действительно законопослушный гражданин, которому нечего скрывать, почему вы не пишете все свои письма на открытках? Почему не соглашаетесь регулярно проходить проверку на употребление наркотиков? Почему требуете предъявления ордера, если полиция собирается обыскивать ваш дом? Пытаетесь что-нибудь скрыть? Если вы прячете свои письма в конверты, значит ли это, что вы диверсант, или торговец наркотиками, или, может быть, просто одержимы манией преследования? Так нужно ли законопослушным гражданам шифровать свою электронную почту?

Что, если бы все были уверены, что законопослушные граждане должны писать все свои письма на открытках? Если какой-нибудь нонконформист попытался бы достигнуть приватности, используя для своей почты конверты, это возбудило бы подозрение. Наверное, власти захотели бы открыть его письма, и посмотреть, что же он там прячет. К счастью, мы не живем в таком мире, поскольку большая часть почты отправляется в конвертах. Поэтому никто не может привлечь к себе внимания использованием конверта. Количество обеспечивает некоторую безопасность. Точно так же, чтобы никто не мог привлечь к себе внимания использованием шифрования, было бы неплохо, если бы каждый повседневно использовал шифрование для всей своей электронной почты, сколь бы невинным ни было ее содержание.. Считайте это формой солидарности.

До сих пор, если правительство хотело нарушить приватность рядовых граждан, оно должно было затратить определенное количество средств и усилий для перехвата, отпаривания и чтения бумажной почты. Или, оно должно было прослушивать устные переговоры по телефону, и, возможно, переписывать их, по крайней мере, до того, как стали доступны технологии автоматического распознавания речи. Этот вид трудоемкого мониторинга непрактичен при применении в больших масштабах. Поэтому так делали только в важных случаях, когда такие затраты казались оправданными.

Законопроект S. 266 – внесенный в 1991 г. рамочный законопроект, направленный против преступности – таил в своих недрах беспрецедентные меры. Если бы этот билль принял форму закона, он принудил бы всех производителей оборудования для защищенной коммуникации оставлять в своих продуктах особые “черные ходы”, с тем, чтобы правительство могло читать любую зашифрованную корреспонденцию. Билль гласил: “Конгресс постановляет, что поставщики услуг в области электронной коммуникации и производители оборудования, используемого для оказания услуг в области электронной коммуникации, обязаны обеспечить правительству доступ к незашифрованному содержимому всех передаваемых голосовых, цифровых и других данных в случаях, предусмотренных законом”. Именно этот законопроект побудил меня опубликовать *PGP* в компьютерных сетях для бесплатного распространения. Это случилось незадолго до того, как после решительных протестов гражданских либертарианцев и промышленных групп указанные меры были исключены из законопроекта.

Законопроект 1994 г. “О цифровой телефонии” обязал телефонные компании устанавливать на центральных телефонных узлах точки входа для удаленного подслушивания, создав тем самым новую технологическую инфраструктуру “моментального подключения” для подслушивания, так что федеральным агентам больше не нужно никуда выходить и цеплять зажимы-“крокодилы” к телефонным проводам. Теперь они смогут сидеть у себя в вашингтонской штаб-квартире и вслушиваться в ваши телефонные разговоры. Конечно, закон все еще требует судебного постановления для осуществления подслушивания. Но технологические инфраструктуры могут существовать в течении жизни нескольких поколений, а законы и правила иногда меняются за одну ночь. Раз уж коммуникационную инфраструктуру, оптимизированную для слежки, начали внедрять, любое изменение политических условий может привести к злоупотреблению этим новым видом власти. Политические условия могут измениться при смене правительства или, более неожиданно, вследствие того, что кто-нибудь взорвет правительственное учреждение.

Через год после того, как законопроект 1994 г. “О цифровой телефонии” стал законом, ФБР обнародовало план, согласно которому от всех телефонных компаний требовалось встраивать в свою инфраструктуру возможность одновременного подслушивания 1% всех телефонных разговоров во всех крупных городах США. Это означало бы более чем тысячекратное увеличение количества номеров телефонов, разговоры по которым могут подслушиваться. В предшествующие годы, в США производилось лишь около тысячи санкционированных судом прослушиваний телефонных разговоров в год на всех уровнях, включая федеральный, штатов и местный. Трудно представить, как правительство сможет нанять такое количество судей, которое было бы способно подписывать ордера на прослушивание 1% от всех телефонных разговоров, не говоря уже о найме такого количества федеральных агентов, которое было бы способно сидеть и слушать все эти разговоры в реальном времени. Единственным осуществимым способом обработки таких объемов телефонных переговоров является массовое, по Оруэллу, применение технологий автоматизированного распознавания речи, чтобы просеивать все это в поисках интересующих ключевых слов или голоса определенного человека. Если правительство не обнаружит того, что ищет, в первой однопроцентной выборке, оно перейдет к следующему проценту, и так далее, пока искомое не будет найдено или все телефоны не будут проверены на предмет подрывной активности. ФБР утверждает, что эти возможности понадобятся в будущем. Эти намерения вызвали такое возмущение, что Конгресс отверг план, по крайней мере, на этот раз, в 1995 г. Но уже сам факт, что ФБР посмело просить о таких широких полномочиях, проливает свет на его замыслы. Кроме того, отклонение этого плана не является особо обнадеживающим, если вспомнить, что законопроект “О цифровой телефонии” тоже был отвергнут при первом рассмотрении, в 1993 г. Технологические достижения не оставляют возможности сохранения статус кво в том, что касается приватности. Само статус кво нестабильно. Если мы будем бездействовать, новые технологии предоставят правительству такие возможности для автоматизированной слежки, о которых не мечтал и Сталин. Единственным способом удержать позиции приватности в информационную эру является стойкая криптография.

Для того, чтобы начать применять криптографию, вам необязательно относиться с недоверием к собственному правительству. Ваши деловые разговоры могут подслушиваться конкурентами, организованной преступностью, или зарубежными правительствами. Например, французское правительство известно тем, что использует свою службу информационной разведки для помощи французским корпорациям в достижении большей конкурентоспособности. Забавно, но ограничения, накладываемые правительством США на криптографию, ослабили защиту американских корпораций от иностранных разведок и организованной преступности.

Правительство знает, насколько важную роль суждено сыграть криптографии во взаимоотношениях власти и народа. В апреле 1993 г. администрация Клинтона обнародовала новую инициативу в политике отношения к шифрованию, которая разрабатывалась Агентством национальной безопасности (АНБ) с начала правления Буша. Ядро этой инициативы – разработанное правительством шифровальное устройство под названием “Клиппер”, которое содержит новый секретный алгоритм шифрования, придуманный АНБ. Правительство попыталось убедить частную промышленность встроить его во все выпускаемые продукты для

обеспечения безопасности коммуникаций, такие как защищенные телефоны, защищенные факсы и т.п. Компания АТ&Т установила “Клиппер” в свои защищенные голосовые продукты. Но дело в том, что в каждый кристалл “Клиппер” во время его производства загружается уникальный ключ шифрования, и правительство получает копию этого ключа, отправляемую в хранилище. Беспокоиться, впрочем, не стоит, ведь правительство обещает использовать этот ключ для доступа к вашим сообщениям только “в случаях, установленных законом”. Конечно, чтобы сделать Клиппер эффективным, следующим логическим шагом должно стать запрещение других форм криптографии.

Вначале правительство заверяло, что использование “Клиппера” будет добровольным, и никого не будут заставлять применять его вместо других типов криптографии. Но реакция общества против “Клиппера” была упорной, гораздо более упорной, чем ожидало правительство. Компьютерная промышленность единодушно объявила о своей оппозиции использованию “Клиппера”. Тогда директор ФБР Луис Фрей, отвечая на вопросы во время пресс-конференции в 1994 г., сказал, что если “Клиппер” не найдет общественной поддержки, и возможности ФБР в подслушивании сообщений будут блокированы криптографией, не находящейся под правительственным контролем, его ведомство будет вынуждено искать законодательной поддержки. Позже, по горячим следам трагедии в Оклахома-Сити, г-н Фрей свидетельствовал перед Законодательным комитетом Сената, что правительство должно ограничить публичный доступ к стойкой криптографии (хотя никто так и не высказал предположения, что динамитчики использовали криптографию).

Информационный Центр Электронной Приватности, пользуясь гарантиями Закона об информации, получил доступ к ряду приоткрывающих замыслы спецслужб документов. В “докладной записке” под названием “Шифрование: угрозы, применения и возможные решения”, отправленном ФБР, АНБ и Департаментом юстиции в адрес Совета по национальной безопасности в феврале 1993 г., утверждается, что “технические решения будут работать только в том случае, если они встраиваются во все шифровальные продукты. Для обеспечения этого необходимо законодательное принуждение к использованию утвержденных правительством шифровальных продуктов или к соблюдению установленных правительством критериев”.

За правительством тянется “хвост”, который не позволяет поверить, что оно никогда не прибегнет к подавлению наших гражданских свобод. Программа ФБР под названием COINTELPRO была направлена на преследование групп, не согласных с политикой правительства. Оно шпионило за участниками антивоенного движения и движения за гражданские права. Оно подслушивало телефонные разговоры Мартина Лютера Кинга. Никсон располагал целым списком своих врагов. А после этого случился уотергейтский скандал. Конгресс теперь, похоже, готов к принятию законов, ограничивающих наши гражданские свободы в Интернет. Никогда еще в последнее столетие недоверие к правительству не было так широко распространено по всему политическому спектру, как сегодня.

Если мы собираемся сопротивляться тревожной тенденции к запрещению криптографии, одно из действий, которые мы можем предпринять – это по возможности более широкое использование криптографии сейчас, пока это еще легально. Чем более популярным станет использование стойкой

криптографии, тем труднее будет правительству ее запретить. А значит, использование *PGP* идет во благо сохранению демократии.

Если приватность ставится вне закона, то лишь те, кто стоит вне закона, обладают приватностью. Разведывательные службы имеют доступ к хорошим криптографическим технологиям, его также имеют гангстеры и торговцы наркотиками. Но обычным гражданам и самодеятельным политическим организациям по большей части не была доступна криптография с открытыми ключами “военной степени” стойкости. До сих пор не была.

*PGP* отдает власть над приватностью народа в руки самого народа. И в этом есть общественная необходимость. Вот почему я написал эту программу.

### Основы криптографии

Для начала, немного элементарной терминологии. Предположим, вы желаете отправить сообщение своей коллеге (назовем ее Алис), и вы хотите, чтобы никто, кроме Алис, не смог его прочитать. Как показано на Рис.1, вы можете зашифровать (или закодировать), то есть преобразовать сообщение безнадежно сложным образом, зная, что никто, кроме вас и Алис, не сможет его прочитать. Вы применяете для шифрования криптографический ключ, а Алис должна использовать тот же ключ для его расшифровки (или раскодирования). По крайней мере, так это выглядит при применении обычной криптографии с “секретным ключом”.

Один и тот же ключ используется как для зашифровки, так и для расшифровки сообщения. Это означает, что этот ключ должен быть сначала передан по надежному каналу, с тем, чтобы обе стороны знали его до того, как передавать зашифрованное сообщение по ненадежному каналу. Но если у вас есть надежный канал, которым вы можете воспользоваться для обмена ключами, спрашивается, зачем вам вообще нужна криптография?

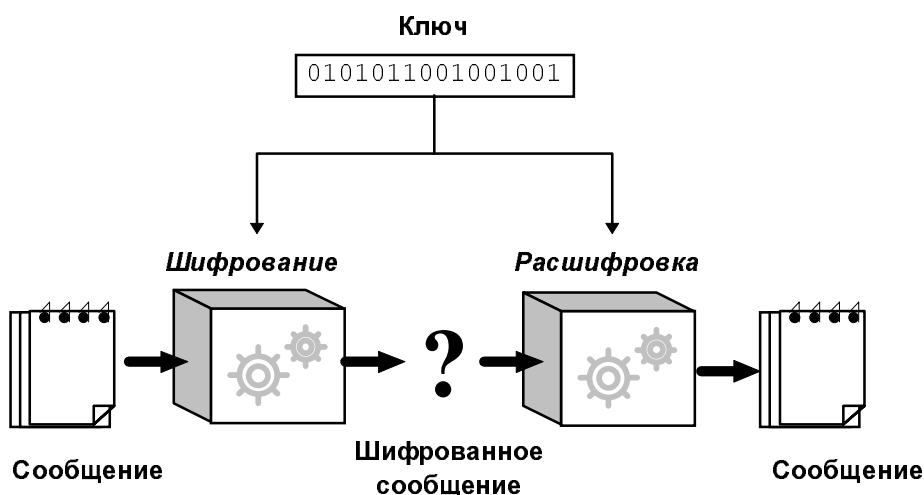


Рис. 1

Как работает криптография с открытым ключом

Как показано на Рис. 2, при использовании криптографии с открытым ключом каждый обладает парой дополняющих друг друга ключей: открытым



и закрытым. Каждый из ключей, входящих в пару, подходит для расшифровки сообщения, зашифрованного с применением другого ключа из той же пары. Зная открытый ключ, закрытый вычислить невозможно. Открытый ключ может быть опубликован и широко распространен по сетям коммуникаций.

Такой протокол обеспечивает приватность без необходимости обладания надежным каналом, которого требует обычная криптография с секретным ключом.

Кто угодно может использовать открытый ключ получателя для того, чтобы зашифровать отправляемое тому сообщение. Получатель затем использует соответствующий закрытый ключ для его расшифровки. Никто, кроме получателя, не может расшифровать сообщение, так как никто больше не имеет доступа к его закрытому ключу. Даже тот, кто зашифровал сообщение с помощью открытого ключа, не сможет его расшифровать.

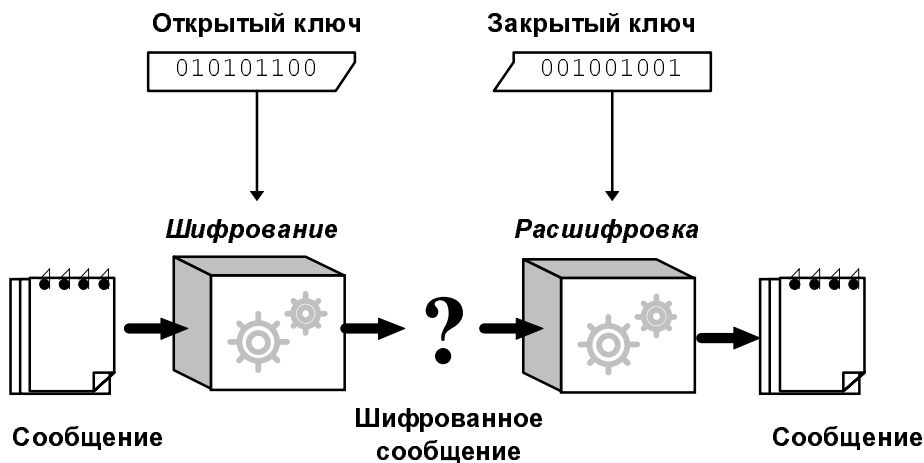


Рис. 2

### Как шифруются ваши файлы и сообщения

Поскольку алгоритм шифрования с открытым ключом значительно медленнее алгоритма обычного шифрования, использующего один ключ, шифрование лучше всего выполнять, используя процесс, показанный на Рис. 3.

Для шифрования сообщения используется качественный и быстрый алгоритм обычного шифрования с секретным ключом. В оригинальной, незашифрованной форме это сообщение называется "открытым текстом". В ходе процесса, невидимого пользователю, для обычного шифрования открытого текста используется временный случайный ключ, сгенерированный специально для этого "сеанса". Затем данный случайный ключ шифруется с помощью открытого ключа получателя. Этот, зашифрованный с использованием открытого ключа "сеансовый ключ", отправляется получателю вместе с зашифрованным текстом ("шифровкой").

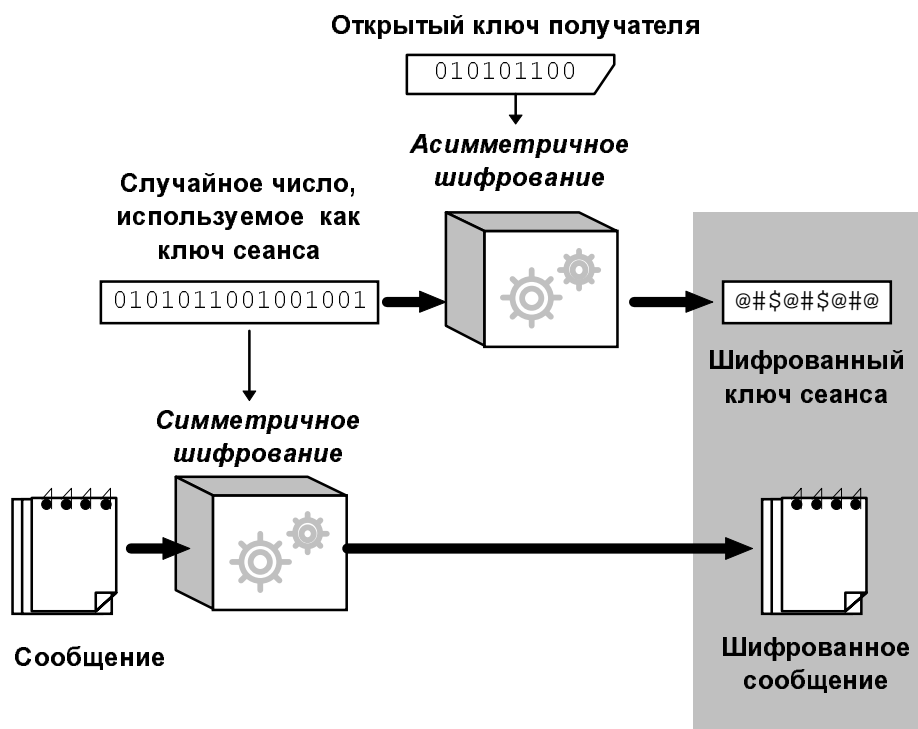


Рис. 3

### Симметричные алгоритмы PGP

*PGP* предоставляет выбор из ряда различных алгоритмов с секретным ключом, используемых для шифрования тела сообщения. Под алгоритмом с секретным ключом мы понимаем обычный, или симметричный, блочный шифр, который использует для шифрования и расшифровки один и тот же ключ. *PGP* предоставляет три симметричных блочных шифра, включая *CAST*, *тройной DES* и *IDEA*. Эти алгоритмы не являются “домашними поделками”; все они разработаны командами криптографов с выдающейся репутацией.

Для интересующихся криптографией: все три шифра оперируют 64-битными блоками открытого текста и шифровки. *CAST* и *IDEA* работают со 128-битным ключом, а *тройной DES* - с ключом длиной 168 бит. Как и Стандарт шифрования данных (*DES*), любой из этих шифров может использоваться в режимах CFB и CBC. *PGP* использует их в режиме CFB с размером блока 64 бит.

Алгоритм *CAST* я включил в *PGP*, потому что он является многообещающим в качестве хорошего блочного шифра с 128-битной длиной ключа, потому что он очень быстрый, и потому что он может быть использован бесплатно. Его название состоит из инициалов разработчиков, Карлисла Адамса и Стаффорда Тавареса из Northern Telecom (Nortel). Nortel подал патентную заявку на *CAST*, но разработчики сделали письменное заявление о том, что *CAST* может использоваться всеми на бесплатной основе. Специалистами с хорошей репутацией в области криптографии *CAST* признан исключительно хорошо построенным алгоритмом. Он основан на очень формальном подходе, с использованием ряда математически доказуемых положений. Это позволяет предположить, что для взлома его 128-битного ключа требуется исчерпывающий перебор вариантов. Существуют сильные аргументы в

пользу того, что *CAST* полностью иммунен как к линейному, так и к дифференциальному криптоанализу (двум самым мощным из опубликованных схем криптоанализа, обе из которых оказались достаточно эффективными для взлома *DES*). Хотя *CAST* слишком молод для того, чтобы иметь долгий послужной список, его формальный дизайн и отличная репутация разработчиков несомненно привлекут внимание других членов академического криптографического сообщества. У меня складывается то же предварительное ощущение доверия к *CAST*, которое ранее я испытывал к *IDEA*, шифру использованному мною в более ранних версиях *PGP*. В то время *IDEA* также был слишком молод для того, чтобы иметь хороший послужной список, но он достойно выдержал все испытания.

Блочный шифр *IDEA* (Международный алгоритм шифрования данных) основан на понятии “смещения операций, принадлежащих различным алгебраическим группам”. Он был разработан в ЕТН в Цюрихе Джеймсом Л. Мэсси и Ксуэйджа Лаем, и опубликован в 1990 г. В ранних статьях этот алгоритм упоминается как IPES (Предложенный улучшенный алгоритм шифрования), но позднее они изменили название на *IDEA*. До сих пор *IDEA* оказывался в большей степени устойчивым к криптографическим атакам, чем другие шифры, такие, как *FEAL*, *REDOC-II*, *LOKI*, *Snefru* и *Khafre*. *IDEA* более устойчив, чем *DES*, к очень успешной криптографической атаке Бихама и Шамира, использующей дифференциальный криптоанализ, а также к атакам с применением линейного криптоанализа. Поскольку этот шифр продолжает быть мишенью для атак со стороны наиболее выдающихся представителей мира криптоанализа, уверенность в стойкости *IDEA* растет со временем. К сожалению, самым серьезным препятствием к принятию *IDEA* в качестве стандарта является то, что патентом на этот алгоритм обладает Ascom Systec, и он, в отличие от *DES* и *CAST*, не является доступным для всех на бесплатной основе.

В репертуар блочных шифров *PGP* включает в качестве страховки *тройной DES*, использующий три ключа. Алгоритм *DES* был разработан в IBM в середине 1970-х гг. При хорошем дизайне, 56-битный ключ является по сегодняшним стандартам слишком коротким. *Тройной DES* очень стоек, и изучался многие годы, так что ставка на его использование может оказаться более верной, чем использование таких шифров, как *CAST* и *DES*. *Тройной DES* – это *DES*, примененный к одному и тому же блоку данных три раза с тремя разными ключами, причем второй раз *DES* запускается в режиме расшифровки. Хотя *тройной DES* много медленнее, чем *CAST* и *IDEA*, скорость обычно не является критичной для применения в электронной почте. *Тройной DES* обладает ключом длиной 168 бит, но, эффективная приведенная длина ключа, вероятно, составляет 112 бит при атаке, когда атакующий располагает невероятно большим ресурсом для хранения данных. Согласно статье, представленной Мишелем Винером на Crypto96, любой хотя бы отдаленно правдоподобный объем запоминающего устройства позволит провести атаку, требующую столько же времени, сколько взлом 129-битного ключа. *Тройной DES* не защищен патентами.

Открытые ключи, генерируемые *PGP* версий 5.0 или более ранних, содержат информацию, которая сообщает отправителю, какие из блочных шифров поддерживаются программным обеспечением получателя, так что программное обеспечение отправителя знает, какие из шифров могут быть использованы. С открытыми ключами *DSS/DH* могут использоваться блочные шифры *CAST*, *IDEA* и *тройной DES*, причем *CAST* является

выбором по умолчанию. С открытыми ключами *RSA* в настоящее время может использоваться только *IDEA*, так как ранние версии *PGP* поддерживают лишь *RSA* и *IDEA*.

### Сжатие данных

Обычно *PGP* сжимает данные до того, как зашифровать их, так как сжимать их после шифрования слишком поздно: зашифрованные данные несжимаемы. Сжатие данных экономит время передачи данных по модему, дисковое пространство и, что более важно, усиливает криптографическую безопасность. Большинство приемов криптоанализа используют для взлома шифра избыточность исходного открытого текста. Сжатие данных снижает избыточность, значительно увеличивая, таким образом, устойчивость к криптоанализу. На сжатие исходного текста требуется дополнительное время, но с точки зрения безопасности это оправдано.

Файлы, слишком короткие для сжатия, или просто плохо сжимаемые, не сжимаются *PGP*. Вдобавок, *PGP* распознает файлы, создаваемые наиболее популярными программами сжатия, например *PKZIP*, и не пытается сжимать уже сжатые файлы.

Для интересующихся техническими подробностями: в программе использованы свободно распространяемые подпрограммы сжатия *ZIP*, написанные Жаном-Лу Гэйи, Марком Адлером и Ричардом Б. Уэлсом. Эти алгоритмы сжатия *ZIP* функционально эквивалентны использованным фирмой *PKWare* в *PKZIP 2.x*. Программы сжатия *ZIP* использованы, потому что они характеризуются хорошим коэффициентом сжатия, и потому что они быстрые.

### О случайных числах, используемых в качестве сеансовых ключей

В *PGP* для генерации временных сеансовых ключей использован криптографически стойкий генератор псевдослучайных чисел. Если файл с исходным для генерации этих чисел числом не существует, он автоматически генерируется с использованием строго случайных событий, в качестве источника которых используются параметры нажатий клавиш и движений мыши.

Этот генератор записывает файл с исходным числом каждый раз при его использовании, смешивая его содержимое с данными, получаемыми из значения даты и других строго случайных источников. В качестве средства генерации случайных чисел использован алгоритм обычного шифрования. Этот файл содержит как исходный материал для генерации случайных чисел, так и исходный материал для ключа, используемого для генерации следующего случайного числа.

Этот файл с исходным случайным числом должен предохраняться от несанкционированного доступа для снижения риска того, что атакующему станет доступен ваш следующий или предыдущий сеансовый ключ. Хотя атакующему будет крайне сложно извлечь какую-либо пользу от захвата этого файла, криптографически очищаемого до и после каждого использования, благоразумным будет попытаться предохранить его от попадания в чужие руки. Если это возможно, сделайте этот файл доступным для чтения только себе. Если же это невозможно, не позволяйте другим бесконтрольно копировать данные с вашего компьютера.

### Как осуществляется расшифровка

Как показано на Рис. 4, процесс расшифровки обратен по отношению к шифрованию. Закрытый ключ получателя используется для восстановления временного сеансового ключа, который, в свою очередь, используется при запуске быстрого обычного алгоритма с секретным ключом для расшифровки основного тела сообщения.

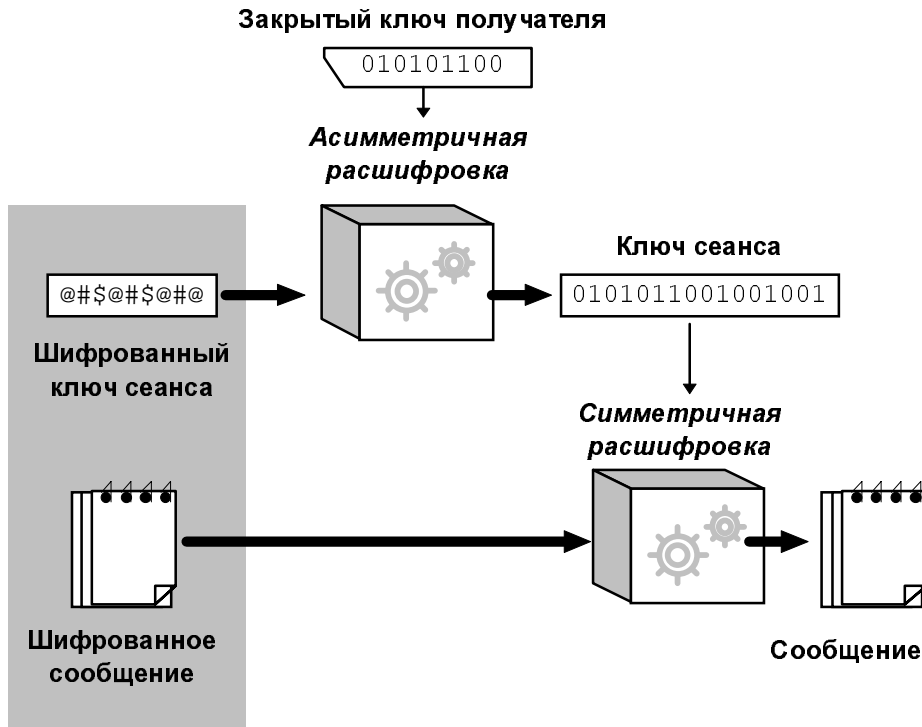


Рис. 4

### Как осуществляется электронная подпись

*PGP* накладывает цифровую подпись для обеспечения аутентификации сообщения. Закрытый ключ отправителя используется для зашифровки дайджеста сообщения, таким образом “подписывая” сообщение. Дайджест сообщения – это 160- или 128-битная криптографически стойкая односторонняя хэш-функция. В чем-то она похожа на “контрольную сумму”, или код проверки ошибок CRC, который компактно представляет сообщение и используется для проверки сообщения на наличие изменений. В отличие от CRC, дайджест сообщения формируется таким образом, что злоумышленник не может сгенерировать поддельное сообщение с аналогичным дайджестом. Дайджест сообщения передается в зашифрованном закрытым ключом отправителя виде, составляя цифровую подпись сообщения.

На Рис. 5 показано, как генерируется цифровая подпись.

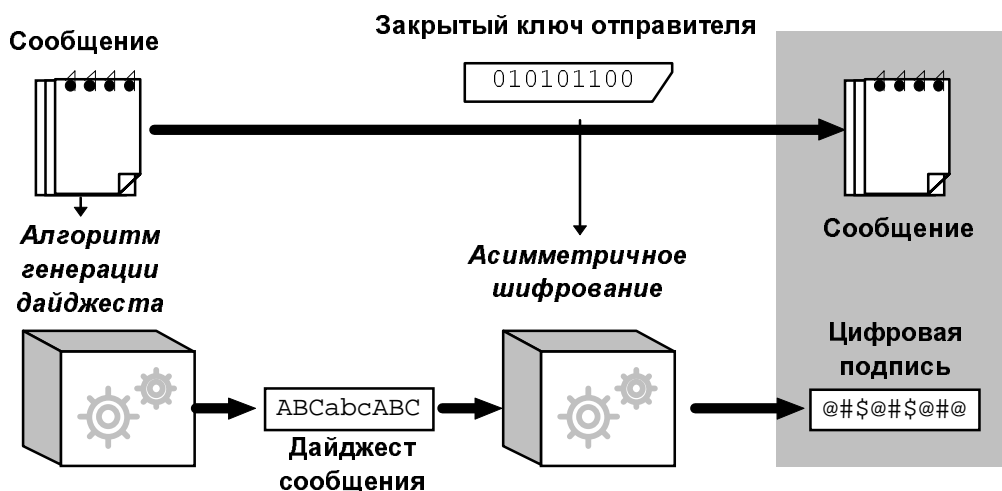


Рис. 5

Получатель (или кто-либо другой) может проверить правильность цифровой подписи, используя открытый ключ отправителя для расшифровки дайджеста сообщения. Это доказывает, что тот, кто указан в качестве отправителя сообщения, является его создателем, и что сообщение не было впоследствии изменено другим человеком, так как только отправитель владеет своим закрытым ключом, использованным для формирования цифровой подписи. Подделка цифровой подписи невозможна, и отправитель не может впоследствии отрицать ее подлинность.

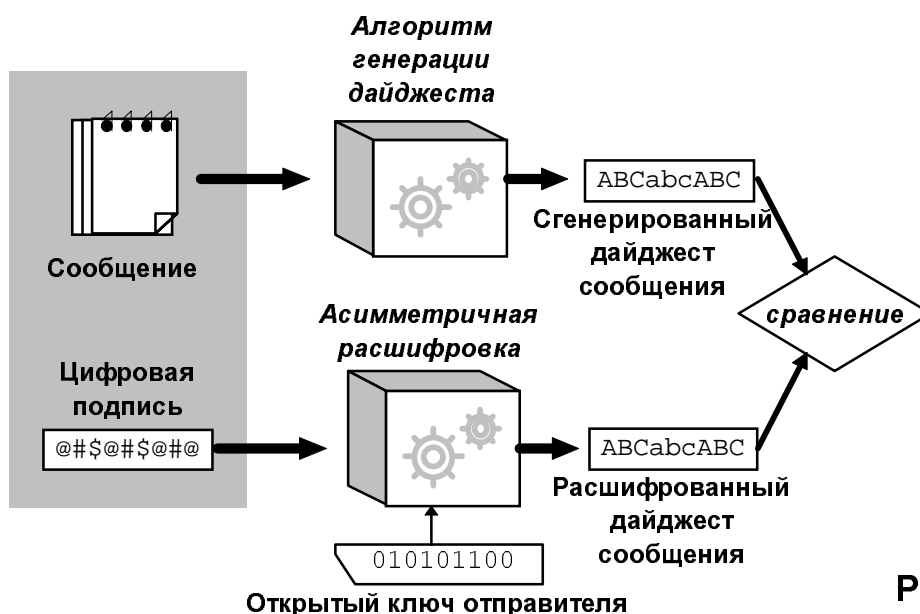


Рис. 6

### О дайджесте сообщения

*Дайджест сообщения* – это компактная (160- или 128-битная) “выжимка” вашего сообщения, или контрольная сумма файла. Ее можно также сравнить с отпечатком вашего пальца на сообщении или файле. Дайджест сообщения “представляет” ваше сообщение таким образом, что если сообщение подвергнется какому-либо изменению, ему будет соответствовать другой дайджест. Это позволяет обнаружить любое изменение, внесенное в сообщение злоумышленником. Дайджест сообщения вычисляется с

использованием криптографически стойкой односторонней хэш-функции сообщения. Для атакующего должно быть вычислительно невозможным изобрести подложное сообщение, которому соответствовал бы идентичный дайджест. В этом отношении, дайджест сообщения гораздо лучше контрольной суммы, потому что сгенерировать другое сообщение, дающее ту же контрольную сумму, достаточно просто. Но, как и из контрольной суммы, из дайджеста сообщения невозможно восстановить само сообщение.

Используемый теперь (начиная с версии 5.0 и выше) в *PGP* алгоритм получения дайджеста сообщения называется *SHA* (Алгоритм защищенного хеширования), он разработан в АНБ для Национального института стандартов и технологий (NIST). *SHA* является 160-битным алгоритмом хеширования. Некоторые относятся ко всему, исходящему от АНБ, с подозрением, поскольку АНБ занимается перехватом коммуникации и взломом шифров. Но следует иметь в виду, что АНБ не заинтересовано в подделке подписей, и что правительство только выиграет от внедрения стандарта цифровой подписи, которую невозможно подделать, поскольку это не позволит кому-либо отрицать подлинность своей подписи. Это несет очевидные преимущества для поддержания законности и сбора разведывательных данных. Кроме того, *SHA* был опубликован в открытой литературе. Он внимательно изучен большинством криптографов во всем мире, которые специализируются на хэш-функциях. Они единодушно заявляют об исключительно хорошей проработанности *SHA*. Во всех новых версиях *PGP* в качестве алгоритма генерации дайджестов сообщений используется *SHA*, а для наложения цифровой подписи – новые ключи *DSS*, соответствующие Стандарту цифровой подписи NIST. Из соображений совместимости, новые версии *PGP* продолжают поддерживать алгоритм *MD5* в сочетании с *RSA*, поскольку такой была технология подписи в прежних версиях *PGP*.

Использовавшийся в ранних версиях *PGP* для создания дайджестов сообщений алгоритм *MD5*, предоставленный в общее пользование *RSA Data Security, Inc.*, является 128-битным хеш-алгоритмом. Он был почти взломан в 1996 г. немецким криптографом Хансом Доббертином. Хотя к настоящему времени *MD5* и не взломан окончательно, в нем были обнаружены настолько серьезные слабые места, что никто не должен продолжать использовать его для генерации цифровой подписи. Дальнейшие разработки в этой области могут окончательно взломать его, позволив, таким образом, подделывать подписи. Если вы не хотите однажды увидеть свою цифровую подпись *PGP* на каком-либо подложном документе, примите совет перейти к новым ключам *DSS* в качестве основного метода наложения цифровой подписи, так как *DSS* использует в качестве алгоритма защищенного хеширования *SHA*.

### Как защищать открытые ключи от подмены

В криптосистемах с открытыми ключами вам не нужно защищать открытые ключи от несанкционированного доступа. Наоборот, чем шире они распространяются, тем лучше. Однако важно защитить открытые ключи от подделки, чтобы быть уверенным в том, что ключ действительно принадлежит тому, чье имя он несет. Процедуры защиты описаны в главе 3 “Защита ваших ключей”. Давайте сначала взглянем на потенциальную опасность такой подмены, а затем опишем, как ее избежать при использовании *PGP*.

Предположим, вы хотите отправить приватное сообщение Алис. Вы загружаете открытый ключ Алис с какой-нибудь электронной доски объявлений (BBS). Вы шифруете свое письмо Алис ее открытым ключом и отправляете его через систему электронной почты той же BBS.

К несчастью, незаметно для вас или Алис, другой пользователь, по имени Виктор, проникает на BBS и генерирует открытый ключ, несущий идентификатор пользователя Алис. Он тайно подменяет своим фальшивым ключом настоящий открытый ключ Алис. Вы неосторожно используете этот фальшивый ключ, принадлежащий Виктору, вместо открытого ключа Алис. Все выглядит нормально, потому что фальшивый ключ несет идентификатор пользователя Алис. Теперь Виктор может расшифровать сообщение, предназначенное Алис, поскольку обладает секретным ключом из фальшивой пары. Он даже может затем снова зашифровать расшифрованное им сообщение настоящим ключом Алис и отправить ей, так что никто ничего не заметит. Более того, он даже сможет потом накладывать от имени Алис подпись, которая будет казаться подлинной, так как все будут использовать для ее верификации фальшивый ключ.

Единственный способ предотвратить такую неприятность – это исключить возможность подделки открытых ключей. Если вы получили открытый ключ Алис непосредственно от нее, проблем не возникает. Но это может быть затруднительным, если Алис находится на расстоянии тысячи миль, или по другим причинам с ней невозможно встретиться лично.

Возможно, открытый ключ Алис может передать вам ваш общий друг Генри, которому вы оба доверяете, и который знает, что обладает подлинным ключом Алис. Генри может подписать открытый ключ Алис, ручаясь, таким образом, за его целостность. Для подписи он должен использовать всей собственный закрытый ключ.

Эта процедура создает подписанный сертификат открытого ключа, который подтверждает, что ключ Алис не был подделан. Конечно, для того, чтобы вы могли проверить правильность подписи Генри, необходимо, чтобы у вас была заведомо правильная копия его открытого ключа. Возможно, Генри может также передать Алис подписанную копию вашего ключа. Генри, таким образом, будет служить “посредником” между вами и Алис.

Этот подписанный сертификат открытого ключа Алис или Генри могут загрузить на BBS, откуда вы можете его позднее скопировать. Так как вы в состоянии проверить подпись Генри с помощью его открытого ключа, вы можете быть уверены, что это – действительно ключ Алис. Никакой злодей не сможет обмануть вас, заставив поверить, что изготовленный им фальшивый ключ принадлежит Алис, поскольку никто не может подделать подпись Генри.

Пользующееся широким доверием лицо может даже специализироваться на “посредничестве” между пользователями, заверяя своей подписью сертификаты их открытых ключей. Это пользующееся доверием лицо может считаться “доверенным сертифициктором”. Любому публичному ключу, заверенному подписью уполномоченного сертифициктора, можно доверять в том смысле, что он принадлежит тому, чье имя он несет. Все пользователи, желающие участвовать в реализации такой сети распределенного доверия, должны обладать заведомо верной копией ключа уполномоченного сертифициктора с тем, чтобы подпись последнего могла быть проверена. В некоторых случаях, доверенный сертифициктор может также поддерживать



сервер ключей, обеспечивая пользователям сети возможность искать открытые ключи с помощью запросов к серверу ключей, однако необязательно, чтобы тот, кто поддерживает сервер ключей, был также и тем, кто их сертифицирует.

Единый уполномоченный сертифициатор особенно подходит для больших централизованно управляемых организаций, правительственных или корпоративных. Некоторые организационные среды используют иерархии доверенных сертифициаторов.

Для более децентрализованных сред более подходящим, чем создание централизованного доверенного сертифициатора, вероятно, будет предоставление всем пользователям возможности действовать в качестве “посредников”.

Одним из наиболее привлекательных свойств *PGP* остается то, что она в равной мере успешно может работать как в централизованной среде с уполномоченным сертифициатором, так и в децентрализованной среде, в которой индивидуумы свободно обмениваются своими ключами.

Задача защиты открытых ключей от подделки как таковая составляет единственную серьезную проблему практического приложения криптографии с открытыми ключами. Она является “ахиллесовой пятой” этой технологии, и сложность программного обеспечения в основном связана с решением именно этой задачи.

Вам следует использовать чей-либо открытый ключ только после того, как вы убедитесь в том, что это настоящий ключ, а не подделка, что он принадлежит именно тому лицу, чье имя несет. Вы можете быть уверены в этом только если получили сертификат открытого ключа непосредственно от его хозяина, или если он подписан кем-либо, кому вы доверяете, и заведомо правильная копия ключа которого у вас уже есть. Идентификатор пользователя ключа должен нести полное имя владельца, а не только его первое имя.

Как бы велико ни было искушение, вы никогда не должны полагаться на случайность и доверять подлинности ключа, взятого с BBS, если он не подписан кем-нибудь, кому вы доверяете. Несертифицированный открытый ключ может оказаться подделкой, выполненной кем угодно, включая администратора этой BBS.

Если вас просят подписать сертификат чьего бы то ни было открытого ключа, убедитесь, что он действительно принадлежит лицу, чье имя он несет. Ведь ваша подпись на чужом ключе – это ручательство с вашей стороны за то, что ключ принадлежит его владельцу. Те, кто вам доверяют, примут к использованию этот ключ, потому что он несет вашу подпись. Полагаться на слухи чрезвычайно неосмотрительно – не подписывайте открытых ключей, если вы не уверены в том, что они действительно принадлежат их хозяевам. По возможности, вы должны подписывать их, только если вы получили их непосредственно от хозяев.

Для того, чтобы подписать открытый ключ, вы должны быть уверены в его принадлежности хозяину в гораздо большей степени, чем если просто собираетесь использовать его для шифрования сообщения. Подписи на сертификате, сделанной надежным посредником, обычно достаточно для того, чтобы использовать сертифицированный ключ для шифрования. Однако, чтобы подписать чей-либо ключ, вы должны обладать независимым

знанием из первых рук о том, кому принадлежит этот ключ. Можно позвонить владельцу ключа и продиктовать ему отпечаток ключа – удостоверившись при этом, что вы разговариваете именно с ним.

Имейте в виду, что ваша подпись на сертификате открытого ключа представляет собой ручательство за целостность ключа и принадлежности его действительному владельцу, а отнюдь не за самого владельца. Вы ничем не рискуете, подписывая открытый ключ социопата, если уверены в том, что этот ключ действительно ему принадлежит. Другие примут этот ключ, проверив вашу подпись на нем (если они, конечно, вам доверяют), но из этого не будет следовать доверия к его обладателю. Быть уверенным в ключе – совсем не то же самое, что верить его владельцу.

Совсем неплохо иметь под рукой свой собственный открытый ключ, сертифицированный подписями различных “посредников”, имея в виду, что большинство корреспондентов доверяет хотя бы одному из тех, кто ручается за целостность вашего ключа. Вы можете опубликовать свой открытый ключ вместе с набором удостоверяющих подписей на различных BBS. Если вы подписали чей-либо ключ, верните сертификат владельцу с тем, чтобы он смог присоединить вашу подпись к набору подписей других лиц, также ручающихся за его целостность.

*PGP* сама следит за тем, какие из открытых ключей на вашей связке надлежащим образом сертифицированы подписями посредников, которым вы доверяете. Все что вам остается – это указать, кому вы доверяете как посредникам, и сертифицировать их ключи своей собственной подписью. *PGP* затем будет автоматически переносить эту степень доверия на все ключи, сертифицированные подписями указанных вами посредников. И, конечно, вы можете непосредственно сертифицировать ключи сами.

Обеспечьте невозможность подделки вашей связки открытых ключей. Проверка сертификата вновь подписываемого ключа в конечном итоге зависит от целостности тех зацепленных на эту связку открытых ключей, которым вы уже доверяете. Сохраняйте физический контроль за своей связкой открытых ключей, храня ее по возможности на своем персональном компьютере, а не на удаленной системе с разделяемым доступом, так же как вы поступаете и со своим закрытым ключом. Это следует делать для предохранения связки ключей от подделки, а не от раскрытия. Сохраняйте надежные копии связки открытых ключей и свой закрытый ключ на защищенном от записи носителе.

Так как ваш собственный открытый ключ используется в качестве последней инстанции для прямой или косвенной сертификации всех остальных открытых ключей, хранящихся на вашей связке, он является самым важным ключом для защиты от подделки. Нелишним будет сохранить его копию на отдельном защищенном от записи флоппи-диске.

Вообще, использование *PGP* предполагает, что вы сохраняете физический контроль над своим компьютером, связками ключей, а также исполняемой копией самой *PGP*. Если злоумышленник может модифицировать данные на ваших дисках, тогда, теоретически, он может модифицировать саму программу с тем, чтобы она более не могла распознавать подделку ключей.

Один из несколько более сложных способов защитить всю связку открытых ключей целиком – это подписать всю связку своим закрытым ключом. Выполнить это можно, создав отделенную цифровую подпись этой связки.

Как PGP следит за тем, какие ключи действительны?

До чтения этого раздела вам нужно прочитать предыдущий, где рассказывается о том, как защищать открытые ключи от подделки.

*PGP* следит за тем, какие из ключей, находящихся на вашей открытой связке, надлежащим образом сертифицированы посредниками, которым вы доверяете. Все что вам остается – это указать, кому вы доверяете как посредникам, и сертифицировать их ключи своей собственной подписью. *PGP* затем будет автоматически переносить эту степень доверия на все ключи, сертифицированные подписями указанных вами посредников. И, конечно, вы можете непосредственно сертифицировать ключи сами.

Для определения степени полезности открытого ключа *PGP* использует два различных критерия – не перепутайте их: 1) Принадлежит ли ключ действительно тому, чье имя он несет? Иными словами, сертифицирован ли он кем-нибудь, чьей подписи вы доверяете? 2) Принадлежит ли он тому, кому вы доверяете сертифицировать другие ключи?

Ответ на первый вопрос *PGP* может вычислить. На второй вопрос вы должны дать *PGP* явный ответ. После того, как вы ответите на второй вопрос, *PGP* может вычислить ответ на первый вопрос для ключей, сертифицированных посредником, которому вы доверяете.

Ключи, сертифицированные посредниками, которым вы доверяете, *PGP* считает действительными. Ключи, принадлежащие этим посредникам, сами должны быть сертифицированы вами или другими посредниками, которым вы доверяете.

*PGP* также учитывает, что вы можете испытывать разную степень доверия к людям, в смысле их способности быть посредниками. Степень вашего доверия к способности владельца ключа выступать в качестве посредника отражает вашу оценку не только его персональной порядочности, но и его компетентности в понимании механизма управления ключами и склонности руководствоваться здравым рассудком при принятии решения о сертификации ключа третьего лица. Вы можете обозначить лицо, как пользующееся полным доверием, ограниченным доверием или не пользующееся доверием. Эта информация об испытываемой вами степени доверия хранится на связке вместе с соответствующими ключами, но при экспорте ключа из связки она не переносится, так как ваше личное мнение о степени, в которой можно доверять владельцу ключа, считается конфиденциальным.

Когда *PGP* оценивает действительность открытого ключа, она проверяет уровень доверия, приданный вами всем подписям, которыми он сертифицирован. Она вычисляет взвешенное значение действительности, т.е. две подписи лиц, пользующихся ограниченным доверием, рассматриваются так же, как подпись одного лица, пользующегося полным доверием. Скептицизм *PGP* может регулироваться – например, вы можете настроить ее таким образом, чтобы она требовала наличия двух подписей лиц, пользующихся полным доверием или трех – лиц, пользующихся ограниченным доверием для того, чтобы считать ключ действительным<sup>8</sup>.

Ваш собственный ключ является для *PGP* “аксиоматически” действительным и не требует для подтверждения никаких сертификатов. *PGP* распознает

---

<sup>8</sup> К сожалению, версия 5.0 для **Windows** не предоставляет такой возможности.

ваши собственные открытые ключи по наличию соответствующих закрытых ключей на связке закрытых ключей. *PGP* предполагает, что вы доверяете себе в достаточной степени, чтобы сертифицировать ключи других лиц.

По прошествии некоторого времени, вы соберете ключи людей, которым вы доверяете как посредникам. Остальные также выберут тех, кому они доверяют в этом качестве. И каждый, в свою очередь, постепенно соберет такую коллекцию сертифицирующих его открытый ключ подписей, что сможет ожидать от любого получателя доверия по крайней мере к одной или двум из этих подписей. Это приведет к возникновению широкой и устойчивой к сбоям сети доверия, по которой будут распространяться открытые ключи.

Этот уникальный самодеятельный подход контрастирует со стандартными схемами управления открытыми ключами, разработанными правительством и другими монолитными организациями, например, с *Internet Privacy Enhanced Mail (PEM)*, основанным на централизованном контроле и принудительно централизованном доверии. Стандартная схема предполагает иерархию уполномоченных сертифицикторов, которая диктует вам, кому вы должны верить. Децентрализованный вероятностный метод определения действительности ключей, реализованный *PGP*, позволяет вам самим решать, кому вы доверяете, ставя вас самих на вершину своей собственной пирамиды сертификации. *PGP* – для тех людей, которые предпочитают сами укладывать свои парашюты.

Хотя здесь подчеркивается децентрализованный, рассчитанный на самодеятельность подход, это не значит, что *PGP* не может использоваться в более иерархических и централизованных схемах управления открытыми ключами. Например, пользователи-большие корпорации, вероятно, предпочтут иметь специальную должность или лицо, которое подписывает ключи всех сотрудников. *PGP* поддерживает и этот централизованный сценарий в качестве вырожденного случая своей обобщенной модели распределенного доверия.

### Как защищать закрытые ключи от раскрытия

Свой закрытый ключ и пароль следует сохранять очень тщательно. Если же закрытый ключ окажется скомпрометированным, следует быстро оповестить об этом все заинтересованные стороны, пока кто-нибудь не использовал его для фальшивой подписи от вашего имени. Например, украденный ключ может быть использован для создания фальшивых сертификатов открытых ключей, что создаст проблемы для массы людей, особенно если ваша подпись пользуется широким доверием. И, разумеется, компрометация вашего ключа может привести к тому, что все зашифрованные сообщения, адресованные вам, смогут быть расшифрованы.

Защиту закрытого ключа следует начать с того, что вы должны всегда сохранять над ним физический контроль. Держать его на домашнем персональном компьютере или на переносном компьютере, который вы носите с собой, приемлемо. Если вы вынуждены использовать служебный компьютер, над которым вы не всегда сохраняете физический контроль, держите связки закрытых и открытых ключей на защищенном от записи флоппи-диске, и забирайте его с собой, когда выходите из офиса. Хранить закрытый ключ на удаленной системе с разделенным доступом (например, на UNIX-системе с удаленным доступом) не годится. Кто-нибудь может

перехватить сеанс связи, захватить ваш пароль и затем получить доступ к самому закрытому ключу, хранящемуся на этой системе. Закрытый ключ может храниться только на машине, находящейся под вашим физическим контролем. Для получения дополнительной информации см. Главу 5.

Не храните пароль на том же компьютере, где хранится ваш закрытый ключ. Сохранение закрытого ключа и пароля на одном компьютере похоже на хранение банкоматной карточки и бумажки с записанным на ней PIN в одном и том же бумажнике. Вы не должны позволить постороннему добраться до диска, содержащего и пароль, и файл с закрытым ключом. Более безопасным будет просто запомнить пароль, и не держать его нигде, кроме собственной головы. Если вы все-таки чувствуете необходимость записать пароль, предохраняйте эту запись очень тщательно, возможно, более тщательно, чем сам закрытый ключ.

Вы также должны сделать резервную копию своего закрытого ключа – если у вас есть лишь одна его копия, и вы ее потеряете, это сделает бесполезным все копии вашего открытого ключа, распространенные по всему миру.

Децентрализованный неинституциональный подход к управлению ключами, поддерживаемый *PGP*, имеет свои преимущества, но его использование означает также, что мы не можем полагаться на единый централизованный список скомпрометированных ключей. Это делает более сложной задачу ограничения ущерба от компрометации закрытого ключа. Вам просто нужно сообщить миру о факте компрометации, и надеяться, что об этом услышит каждый.

Если случится худшее, и будут скомпрометированы как ваш закрытый ключ, так и пароль (надеемся, что вы об этом каким-то образом узнаете), вам необходимо будет сгенерировать сертификат о “компрометации ключа”. Этот тип сертификата используется для предупреждения других о том, что ваш открытый ключ не должен больше использоваться. В *PGP* для создания такого сертификата используется команда *Revoke* (Отозвать) из меню *PGPkeys*. Затем вы должны каким-то образом отправить этот сертификат всем на свете, или по крайней мере своим друзьям, друзьям своих друзей и т.д. Их копия программы *PGP* присоединит этот сертификат к связке открытых ключей, что воспрепятствует случайному использованию скомпрометированного ключа в будущем. Затем вы можете сгенерировать новую пару из открытого и закрытого ключей и опубликовать новый открытый ключ. Новый открытый ключ и сертификат компрометации старого ключа могут быть разосланы в одном сообщении.

Что, если вы потеряете свой закрытый ключ?

Обычно для создания сертификата отзыва закрытого ключа, подписанного этим самым ключом, можно использовать команду **Revoke (Отозвать)** из меню **PGPkeys**.

А что если вы потеряли свой закрытый ключ, или ваш закрытый ключ оказался разрушенным? Вы не можете отозвать его сами, так как для этого вам потребовался бы тот самый закрытый ключ, которого у вас уже нет. Вам придется попросить каждое лицо, которое подписывало сертификат с вашим открытым ключом, отозвать свою подпись. Тогда каждый, кто попытается использовать ваш ключ, основываясь на доверии к одному из этих посредников, будет знать, что использовать ваш открытый ключ больше нельзя.

### Осторожно: шарлатанские снадобья

При оценке пакета криптографического программного обеспечения всегда остается вопрос: “Почему вы должны доверять этому продукту?” Он остается даже в случае, когда вы сами изучили исходный текст программ – ведь не каждый обладает криптографическим опытом, чтобы оценить уровень безопасности. И даже если вы опытный криптограф, от вас могут ускользнуть неочевидные слабые места в алгоритмах.

Когда в начале семидесятых я учился в колледже, я изобрел схему шифрования, которая казалась мне блестящей. Для создания шифровки к открытому тексту добавлялась простая последовательность псевдослучайных чисел. Казалось бы, это должно противостоять любому частотному анализу шифровки и сделать ее нераскрываемой даже правительственными разведывательными службами с их огромными ресурсами. Я так гордился своим достижением!

Годами позже, я обнаружил ту же самую схему в нескольких текстах введения в криптографию и учебниках. Как мило: о ней думали и другие криптографы. К несчастью, эта схема приводилась как задание для простой домашней работы на применение элементарных приемов криптоанализа для тривиального ее взлома. Вот и все о моей блестящей схеме.

Из этого унижительного опыта я узнал, как просто впасть в ложное чувство безопасности при разработке алгоритма шифрования. Большинство людей просто не представляет, как немыслимо сложно придумать алгоритм шифрования, который выдержит продолжительную и целеустремленную атаку со стороны хорошо оснащенного противника. Многие разработчики обычного программного обеспечения используют столь же наивные схемы шифрования (а иногда – и ту же самую схему), а некоторые из этих схем оказываются внедренными в коммерческие программные пакеты шифрования и продаются за немалые деньги ничего не подозревающим пользователям.

Это похоже на продажу автомобильных ремней безопасности, которые выглядят прочными, но не выдерживают даже несильного рывка. Полагаться на них будет более опасным, чем обходиться вовсе без ремней безопасности. Никто не подозревает, что они слабы, пока не случится настоящая авария. Если вы полагаетесь на слабое криптографическое обеспечение, вы можете, сами не подозревая о том, подставить под удар секретную информацию. Если бы у вас не было никакого криптографического обеспечения, наверное, вы бы этого не сделали. Возможно, вам не удастся даже узнать, что ваши данные скомпрометированы.

Некоторые коммерческие пакеты используют Федеральный стандарт шифрования данных (*DES*), действительно неплохой алгоритм обычного шифрования, рекомендованный правительством для коммерческого использования (но не для защиты правительственной секретной информации – достаточно странно...). Существует несколько “режимов использования” *DES*, некоторые из которых лучше, чем другие. Правительство не рекомендует использовать для шифрования сообщений самый слабый из них, *ECB* (“электронная кодовая книга”), а рекомендует более стойкие, но и более сложные режимы “шифрования с обратной связью” (*CFB*) и “цепочки шифрованных блоков” (*CBC*).

К несчастью, большинство коммерческих пакетов шифрования, которые я видел, используют режим *ECB*. Когда я разговаривал с авторами некоторых из этих программ, они говорили, что никогда не слышали о режимах *CBC* и *CFB* и не знают ничего об уязвимости *ECB*. Сам факт того, что они не изучили криптографию даже до такой степени, чтобы знать об этих элементарных понятиях<sup>9</sup>, не является оправданием. К тому же, они иногда реализуют управление ключами *DES* ненадлежащим или небезопасным образом. А кроме того, их программы часто предусматривают использование другого алгоритма, более быстрого по сравнению с *DES*. Авторы программ часто полагают, что их собственные алгоритмы не менее безопасны, чем *DES*, но после расспросов я нередко обнаруживал, что это лишь вариации на тему той моей “блестящей” схемы студенческих годов. А некоторые авторы отказываются сообщать, как работают их собственные схемы шифрования, лишь уверяя, что это блестящие схемы, и что им можно доверять. Я не сомневаюсь, что они действительно верят в то, что их алгоритмы замечательные, но как в этом можно убедиться, не видя самих алгоритмов?

Впрочем, стоит отметить, что в большинстве случаев эти ужасающе слабые программы написаны все же не в компаниях, специализирующихся на криптографических технологиях.

Даже действительно хорошие криптографические пакеты, использующие *DES* в правильных режимах, создают проблемы. Стандартный *DES* использует 56-битные ключи, слишком короткие по сегодняшним стандартам, поскольку они могут быть взломаны специальными высокоскоростными компьютерами путем исчерпывающего перебора ключей. *DES* уже заканчивает свой жизненный путь, и с ним – все основанные на нем программы<sup>10</sup>.

Существует компания под названием *AccessData* (87 East 600 South, Orem, Utah 84058, тел. 1-800-658-5199), которая продает за \$185 пакет, взламывающий криптографические схемы, встроенные в *WordPerfect*, *Lotus 1-2-3*, *MS Excel*, *Symphony*, *Quattro Pro*, *Paradox*, *MS Word* и *PKZIP*. Эта программа не просто подбирает пароли – она выполняет настоящий криптоанализ. Люди покупают ее, когда забывают пароли от собственных файлов. Правоохранительные службы также приобретают ее, чтобы иметь возможность читать такие файлы, когда они встречаются на изъятых носителях. Я говорил с Эриком Томсоном, автором этой программы, и он сообщил, что его программе требуются для взлома лишь доли секунды, и он вставил циклы задержки, чтобы покупателям не показалось, что это слишком просто.

В области средств защищенной телефонии ваш выбор невелик. Самым серьезным является устройство *STU-III* (Защищенный телефонный аппарат),

---

<sup>9</sup> При использовании режима *ECB* одинаковым блокам открытого текста соответствуют одинаковые блоки шифровки, что, в случае, если криптоаналитик располагает значительным количеством шифрованного материала, может существенно облегчить его работу. Остальные режимы использования *DES* предполагают ту или иную форму зависимости блока шифровки не только от соответствующего ему блока открытого текста и ключа, но и от других блоков открытого текста.

<sup>10</sup> Пока эта книга переводилась, алгоритм *DES* был взломан совместными усилиями участников конкурса, объявленного *RSA, Inc.*

продаваемый Motorola и AT&T по \$2000-\$3000, и используемый правительством для передачи секретной информации. Он использует стойкую криптографию, но для его покупки нужно особое правительственное разрешение. Доступна и его коммерческая версия, которая ослаблена для удобства АНБ, а также экспортная версия, ослабленная в еще большей степени. Затем, существует устройство Surity 3600, продаваемое AT&T по \$1200, в котором для шифрования используется хваленая правительственная микросхема “Клиппер”, а копии ключей помещены в правительственное хранилище для удобства подслушивающих. Кроме того, существуют и аналоговые (не цифровые) голосовые скремблеры, которые можно найти в любом каталоге для шпионов-любителей, и которые, в криптографическом аспекте, являются на самом деле бесполезными игрушками. Однако они продаются в качестве “продуктов для безопасной коммуникации” покупателям, которые не видели ничего лучшего.

В некотором отношении, криптография похожа на фармацевтику: целостность является решающим фактором. Испорченный пенициллин выглядит так же, как свежий пенициллин. Если неправильно работает ваш пакет электронных таблиц, вы это увидите; но как вы можете распознать слабость своего криптографического пакета? Шифровка, выполненная с помощью слабого алгоритма шифрования, выглядит так же, как шифровка, выполненная с помощью стойкого алгоритма. В этой области как нигде масса шарлатанских снадобий. Куча лекарств, ни от чего не помогающих. В отличие от торговцев “патентованными средствами” прошлого, их изготовители обычно даже не подозревают, что продают знахарское зелье. Они могут быть неплохими программистами, но часто не удосуживаются прочитать ни единого учебника по криптографии. Но они полагают, что могут писать хорошие криптографические программы. Почему бы нет? Ведь на первый взгляд это так просто. И программы вроде бы неплохо работают.

Каждый, кто думает, что изобрел непробиваемую схему шифрования – или невероятно редкий гений, или просто наивен и неопытен. К несчастью, мне приходилось иметь дело с такими горе-криптографами, которые хотели “улучшить” PGP, добавив алгоритм шифрования собственного производства.

Я вспоминаю разговор с Брайеном Сноу, высокопоставленным криптографом из АНБ. Он говорил, что никогда не стал бы доверять алгоритму шифрования, изобретенному тем, кто предварительно бы не “съел собаку”, потратив массу времени на ломку шифров. Это звучало вполне убедительно. Я заметил, что практически никто в кругах коммерческих криптографов не удовлетворяет этому требованию. “Да,” – ответил он с самодовольной улыбкой: “И это так упрощает нашу работу в АНБ”. Отрезвляющая мысль. Ведь и я не удовлетворяю этому требованию.

Правительство также занималось торговлей шарлатанскими снадобьями. После Второй мировой войны США продавали немецкую шифровальную машину *Энигма* правительствам стран Третьего мира. Однако, последним при этом не сообщалось, что во время войны союзники взломали шифр *Энигмы* (факт, многие годы остававшийся засекреченным). Даже сейчас многие UNIX-системы во всем мире используют шифр *Энигмы* для шифрования файлов, отчасти потому, что правительство создало юридические препятствия к использованию лучших алгоритмов. Оно даже пыталось помешать первой публикации алгоритма *RSA* в 1977 г. Кроме того, в течение многих лет правительство противостояло почти всем попыткам



коммерческих фирм создать по-настоящему безопасные телефоны для массового использования.

Главной задачей Агентства национальной безопасности США является сбор разведывательных данных, в основном, путем тайного подслушивания частных коммуникаций между людьми (это описано в книге Джеймса Бэмфорда “Палата загадок”). АНБ затрачивает массу усилий и ресурсов на взлом шифров. Если народ не может получить хорошие криптографические средства для самозащиты, задача АНБ намного упрощается. АНБ также отвечает за экспертизу и рекомендацию алгоритмов шифрования. Ряд критиков усматривает в этом конфликт интересов, подобно тому, как если бы козлу поручили сторожить огород. В 1980-ые годы АНБ проталкивало разработанный им алгоритм обычного шифрования, (COMSEC), , но не сообщало о том, как он работает, так как он был засекречен. В АНБ хотели, чтобы другие поверили им и начали его использование. Но любой криптограф подтвердит, что хорошо продуманный алгоритм шифрования не должен оставаться засекреченным, чтобы быть безопасным: необходимо лишь обеспечить секретность ключей. Как можно судить, безопасен ли секретный алгоритм АНБ? АНБ не так трудно придумать алгоритм, который только оно может сломать, если никто больше не может его изучить. И в микросхему “Клиппер” АНБ засунуло *SKIPJACK*, еще один разработанный этим ведомством секретный шифр. Не подсовывают ли они снова шарлатанское снадобье?

Качество коммерческого криптографического программного обеспечения в США подрывается тремя факторами.

- Первым из них является практически повсеместная некомпетентность разработчиков коммерческого криптографического программного обеспечения (впрочем, с публикацией *PGP* это начало меняться). Каждый программист воображает себя криптографом, что ведет к распространению исключительно плохого криптообеспечения.
- Второй – жесткое и систематическое подавление хороших коммерческих технологий шифрования со стороны АНБ посредством установления юридических ограничений и экономического давления. Частично, это давление производится путем строгих ограничений на экспорт, что, в свою очередь, благодаря законам рынка программного обеспечения, ведет к подавлению криптографического программного обеспечения для внутреннего применения.
- Еще одним важным методом подавления служит передача всех патентных прав на алгоритмы шифрования с открытым ключом единственной компании, что приводит к замыканию проблемы предотвращения распространения этой технологии на одну фирму (хотя этот криптопатентный картель уже распался осенью 1995 г.).

Итоговым эффектом действия этих факторов стало то, что до публикации *PGP* в США практически не было доступно достаточно безопасное программное обеспечение для шифрования общего назначения.

В безопасности *PGP* я не так уверен, как был уверен в своей “блестящей” схеме времен пребывания в колледже. Если бы это было не так, это было бы плохим знаком. Но я не думаю, что *PGP* содержит серьезные слабые места (хотя, я почти уверен, что ошибки в ней есть). Я выбрал лучшие алгоритмы из опубликованных в литературе гражданскими учеными-криптологами. Почти каждый из алгоритмов был подвергнут тщательному изучению со

стороны коллег. Я знаком со многими ведущими криптографами мира, и с некоторыми из них обсуждал многие использованные в *PGP* алгоритмы и протоколы. *PGP* хорошо изучена, и находится в использовании многие годы. К тому же, я не работаю на АНБ. Но вам совсем не обязательно полагаться на мое слово в вопросе криптографического совершенства *PGP*, так как исходные тексты программ доступны для экспертизы.

И еще один пункт, касающийся моей преданности криптографическому качеству *PGP*. С тех пор, как в 1991 г. я разработал и опубликовал для бесплатного использования *PGP*, три года я был объектом уголовного расследования, предпринятого Таможенной службой США из-за распространения *PGP* за рубеж, с риском уголовного наказания и многих лет тюремного заключения. Кстати, правительство не беспокоилось из-за другого криптографического программного обеспечения – только *PGP* заставило его выйти из себя – не говорит ли это о стойкости *PGP*? Я заслужил свою репутацию именно криптографической целостностью своего продукта. Я не предаю свою приверженность нашему праву на приватность, за которое я рисковал своей свободой. Я не позволю продукту, связанному с моим именем, содержать скрытые “черные ходы”.

### Уязвимые места

Ни одна система защиты данных не является неуязвимой. *PGP* можно обойти целым рядом способов. Защищая данные, вы должны задать себе вопрос: является ли информация, которую вы пытаетесь защитить, более ценной для атакующего, чем стоимость атаки? Ответ на этот вопрос приведет вас к тому, чтобы защититься от дешевых способов атаки и не беспокоиться о возможности более дорогой атаки.

Нижеследующее обсуждение местами может показаться маниакальным, но такой подход уместен при обсуждении уязвимых мест.

*Если все персональные компьютеры мира (260 миллионов штук) заставить работать с единственным сообщением, зашифрованным PGP, расшифровка такого сообщения в среднем потребует времени, в 12 миллионов раз превышающего возраст Вселенной.*

Уильям Кроуэлл, заместитель директора Агентства национальной безопасности, 20 марта 1997 г.

### Скомпрометированные пароль и закрытый ключ

Наверное, самую простую атаку можно осуществить, если вы оставите где-нибудь записанный пароль, защищающий ваш закрытый ключ. Если кто-нибудь получит его, а затем получит доступ к файлу с вашим закрытым ключом, он сможет читать адресованные вам зашифрованные сообщения и ставить от вашего имени цифровую подпись.

Вот некоторые рекомендации по защите пароля:

1. Не используйте очевидные фразы, которые легко угадать, например, имена своих детей или супруги.
2. Используйте в пароле пробелы и комбинации цифр и букв. Если ваш пароль будет состоять из одного слова, его очень просто отгадать, заставив компьютер перебрать все слова в словаре. Именно поэтому фраза в качестве пароля гораздо лучше, чем слово. Более изощренный злоумышленник может

заставить свой компьютер в поисках пароля перебрать словарь известных цитат.

3. Используйте творческий подход. Придумайте фразу, которую легко запомнить, но трудно угадать: такая фраза может быть составлена из бессмысленных выражений или очень редких литературных цитат.

### Подделка открытых ключей

Самое уязвимое место – это возможность подделки открытых ключей. Вероятно, это самое серьезное слабое место любой криптосистемы с открытыми ключами, в частности, потому, что большинство новичков не в состоянии немедленно обнаружить такую подделку. О том, почему это важно, и какие против этого следует предпринимать контрмеры, подробно написано выше, в разделе “Как защитить открытые ключи от подделки”.

Вкратце: когда вы используете чей-то открытый ключ, удостоверьтесь, что он не был подделан. Целостности нового чужого открытого ключа следует доверять только если он получен непосредственно от его владельца или подписан кем-то, кому вы доверяете. Обеспечьте невозможность подделки открытых ключей на вашей связке. Сохраняйте физический контроль как над связкой открытых ключей, так и над своим закрытым ключом, при возможности сохраняйте их на своем персональном компьютере, а не на удаленной системе с разделением доступа. Сохраняйте резервную копию обеих связок.

### Не до конца удаленные файлы

Еще одна потенциальная проблема безопасности связана со способом, которым большинство операционных систем удаляет файлы. Когда вы шифруете файл и затем удаляете файл с исходным открытым текстом, операционная система не стирает данные физически. Она просто помечает соответствующие блоки на диске, как свободные, допуская тем самым повторное использование этого пространства. Это похоже на то, как если бы ненужные секретные документы выбрасывались в мусорную корзину вместо того, чтобы отправить их в шреддер. Блоки диска все еще сохраняют исходные секретные данные, которые вы хотели стереть, и лишь со временем будут заняты новыми данными. Если злоумышленник прочтает эти блоки данных вскоре после того, как они помечены как свободные, он сможет восстановить ваш исходный открытый текст.

Это может произойти и случайно: если из-за какого-нибудь сбоя будут уничтожены или испорчены другие файлы, для их восстановления запустят программу восстановления, а она восстановит также и некоторые из ранее стертых файлов. Может случиться так, что среди последних окажутся и ваши конфиденциальные файлы, которые вы намеревались уничтожить без следа, но они могут попасться на глаза тому, кто восстанавливает поврежденный диск. Даже когда вы создаете исходное сообщение с использованием текстового редактора или Word-процессора, программа может оставить множество промежуточных временных файлов, просто потому, что она так работает. Эти временные файлы обычно удаляются редактором при его закрытии, но фрагменты вашего секретного текста остаются где-то на диске.

Единственный способ предотвратить восстановление открытого текста – это каким-либо образом обеспечить перезапись места, занимаемого удаленными

файлами. Если вы не уверены, что все блоки, занимаемые на диске удаленными файлами, будут вскоре использованы, нужно предпринять активные шаги для перезаписи места, занятого исходным открытым текстом и временными файлами, создаваемыми Word-процессором. Это можно осуществить, используя любую утилиту, которая способна перезаписать все неиспользованные блоки на диске. Такими возможностями, к примеру, обладают Norton Utilities for MS-DOS.

### Вирусы и закладки

Другая атака может быть предпринята с помощью специально разработанного компьютерного вируса или червя, который инфицирует *PGP* или операционную систему. Такой гипотетический вирус может перехватывать пароль, закрытый ключ или расшифрованное сообщение, а затем тайно сохранять их в файле или передавать по сети своему создателю. Вирус также может модифицировать *PGP* таким образом, чтобы она перестала надлежащим образом проверять подписи. Такая атака обойдется дешевле, чем криптоаналитическая.

Защита от подобных нападений подпадает под категорию общих мер защиты от вирусных инфекций. Существует ряд коммерчески доступных антивирусных программ с неплохими возможностями, а также набор гигиенических процедур, следование которым серьезно снижает риск заражения вирусами. Общие вопросы мер борьбы с вирусами и червями находятся за пределами темы настоящего документа. *PGP* не содержит никакой защиты от вирусов, и ее использование предполагает, что ваш персональный компьютер является надежной средой. Если такой вирус или червь действительно появится, будем надеяться, что сообщение об этом достигнет ушей каждого.

Другая аналогичная атака заключается в том, чтобы создать хитрую имитацию *PGP*, которая в работе выглядела бы точно так же, но делала не то, что предполагается. Например, она может обходить верификацию подписей, делая возможным принятие фальшивых сертификатов ключей.

Вы должны попытаться получить свою копию *PGP* непосредственно от *PGP, Inc.*

Существуют также возможности проверить, не подделана ли *PGP*, с помощью цифровых подписей. Вы можете использовать другую заведомо целостную версию *PGP* для верификации цифровых подписей на двоичных файлах подозрительной версии. Это не поможет, если вирусом инфицирована сама операционная система, или если первоначальная версия *PGP* модифицирована таким образом, чтобы уничтожить в ней способность проверять подписи. Такая проверка также предполагает, что у вас есть заслуживающая доверия копия открытого ключа, который можно использовать для верификации подписей на исполняемых модулях *PGP*.

### Файлы подкачки (виртуальная память)

*PGP* первоначально разрабатывалась для *MS-DOS*, достаточно примитивной, по сегодняшним стандартам, операционной системы. С ее переносом в другие, более сложные операционные системы, такие как *MS Windows* или *MacOS*, возникло еще одно уязвимое место. Оно связано с тем,

что в этих более хитрых операционных системах используется технология под названием “виртуальная память”.

Виртуальная память позволяет вам запускать на своем компьютере огромные программы, размер которых больше, чем объем установленных на машине полупроводниковых микросхем памяти. Это удобно, поскольку с тех пор, как графический интерфейс стал нормой, программы занимают все больше и больше места, а пользователи норовят запускать по несколько больших приложений одновременно. Операционная система сохраняет фрагменты программного обеспечения, которые в настоящий момент не используются, на жестком диске. Это значит, что операционная система может записать некоторые данные, о которых вы думаете, что они хранятся только в оперативной памяти, на диск без вашего ведома. Например, такие данные, как ключи, пароли, расшифрованные сообщения. *PGP* не оставляет подобного рода секретные данные в памяти дольше, чем это необходимо, однако остается возможность того, что операционная система успеет сбросить их на диск.

Данные на диск записываются в особую временную область, известную как файл подкачки. По мере того, как они становятся нужны, они считываются обратно в память. Таким образом, в каждый отдельный момент в физической памяти находится лишь часть ваших программ и данных. Вся эта работа по подкачке остается невидимой для пользователя, который лишь слышит, как щелкает дисковод. *MS Windows* перекачивает фрагменты памяти, называемые страницами, используя алгоритм замещения *LRU* (Наиболее давно использованных страниц). Это означает, что первыми окажутся сброшены на диск страницы, доступ к которым осуществлялся наиболее давно. Такой подход предполагает, что в большинстве случаев риск того, что секретные данные окажутся сброшенными на диск, неощутимо мал, поскольку *PGP* не оставляет их в памяти надолго. Но мы не можем дать никаких гарантий.

К этому файлу подкачки может получить доступ каждый, кому физически доступен ваш компьютер. Если вас беспокоит эта проблема, возможно, вам удастся ее решить, установив специальное программное обеспечение, стирающее данные в файле подкачки. Другим возможным средством является отключение механизма виртуальной памяти в операционной системе. Это позволяют сделать и *MS Windows*, и *MacOS*. Отключение виртуальной памяти означает, что вам потребуется больше физически установленных микросхем оперативной памяти, для того, чтобы в нее вошло все.

### Нарушение режима физической безопасности

Нарушение режима физического доступа может позволить постороннему захватить ваши файлы с исходным текстом или отпечатанные сообщения. Seriously настроенный противник может выполнить это посредством ограбления, роясь в мусоре, спровоцировав необоснованный обыск и изъятие, с помощью шантажа или инфильтрации в ряды ваших сотрудников. Применение некоторых из этих методов особенно подходит против самостоятельных политических организаций, использующих в основном труд неоплачиваемых добровольцев.

Не стоит впадать в ложное чувство безопасности только потому, что у вас есть криптографическое средство. Приемы криптографии защищают данные

только пока те зашифрованы, и не могут воспрепятствовать нарушению режима физической безопасности, при котором скопрометированными могут оказаться исходные тексты, письменная или звуковая информация.

Этот вид атаки также дешевле, чем криптоаналитическая атака на *PGP*.

### Радиоатака

Хорошо оснащенным противником может быть предпринята атака еще одного вида, предполагающая удаленный перехват электромагнитного излучения, испускаемого вашим компьютером. Эта дорогая и часто трудоемкая атака, вероятно, также является более дешевой, чем криптоанализ. Соответствующим образом оборудованный фургон может припарковаться рядом с вашим офисом и издали перехватывать нажатия клавиш и сообщения, отображаемые на мониторе. Это скопрометирует все ваши пароли, сообщения и т.п. Такая атака может быть предотвращена соответствующим экранированием всего компьютерного оборудования и сетевых кабелей с тем, чтобы они не испускали излучения. Технология такого экранирования известна под названием *Tempest* и используется рядом правительственных служб и фирм, выполняющих оборонные заказы. Существуют поставщики оборудования, которые продают *Tempest*.

### Защита от фальшивых дат подписей

Несколько менее очевидным слабым местом *PGP* является возможность того, что нечестный пользователь создаст электронную подпись на сообщении или сертификате ключа, снабженную фальшивой датой. Если вы пользуетесь *PGP* от случая к случаю, вы можете пропустить этот раздел и не погружаться в дебри сложных протоколов криптографии с открытыми ключами.

Ничто не мешает нечестному пользователю изменить системную дату и время на своем компьютере и создать сертификат своего открытого ключа или подпись, содержащие другую дату. Он может создать видимость того, что подписал что-то раньше или позже того времени, когда он это действительно сделал, или что его пара ключей была создана раньше или позже. Из этого могут проистекать различные юридические или финансовые выгоды, например, за счет создания некоего оправдания, позволяющего ему затем отрицать свою подпись.

Я полагаю, что проблема фальшивой даты на электронной подписи не более серьезна, чем проблема фальшивой даты, стоящей рядом с подписью ручкой. Никого не волнует, что кто угодно может поставить любую дату рядом со своей подписью на договоре. Иногда, “некорректная” дата рядом с подписью не предполагает никакого мошенничества: возможно, она означает время, с которого подписывающий признает этот документ, или время, с которого он хочет, чтобы его подпись вступила в силу.

В ситуациях, когда вопрос доверия к тому, что подпись выполнена именно в определенное время, является критичным, люди могут просто обратиться к нотариусу, чтобы он засвидетельствовал момент подписи и заверил это своей печатью. Аналогично, при использовании цифровой подписи для заверения даты подписи документа можно обратиться к пользующейся доверием третьей стороне, чтобы она сертифицировала эту подпись своей. Никакого экзотического или чрезмерно формализованного протокола для этого не

требуется. Подписи свидетелей издавна используются как юридическое доказательство того, что документ был подписан в определенное время.

Пользующийся доверием уполномоченный сертифициатор или нотариус может создавать достойные доверия подписи с заведомо корректной датой. Такой подход не требует централизованной сертификации. Возможно, эту роль может выполнять любой пользующийся доверием посредник или незаинтересованная сторона, точно так же, как действуют сегодня обычные нотариусы. Когда нотариус заверяет своей подписью подпись другого лица, он создает заверенный сертификат другого заверенного сертификата, который может служить подтверждением подписи точно так же, как подпись обычного нотариуса служит подтверждением подписи, выполненной от руки. Нотариус может вести собственный реестр, добавляя в него отделенные сертификаты с цифровыми подписями (не копируя в него сами подписанные документы). Этот реестр можно сделать общедоступным. Дата на подписи нотариуса должна пользоваться доверием, и она может являться более веским доказательством и юридически быть более значимой, чем дата на сертифицируемой подписи.

Эта тема хорошо проанализирована Деннинг в ее статье 1983 г. в *IEEE Computer* (см. список рекомендованной вводной литературы ниже). Последующие версии *PGP*, вероятно, будут предусматривать возможность простого управления нотаризованными сертификатами подписей с достойными доверия датами.

#### Утечка данных в многопользовательских системах

*PGP* была разработана для использования на однопользовательском персональном компьютере, находящимся под физическим контролем пользователя. Если вы запускаете *PGP* дома на своем собственном PC, ваши зашифрованные файлы находятся в безопасности, пока никто не ворвался в ваш дом, не украл компьютер и не заставил вас открыть ему свой пароль (или не отгадал пароль, если он слишком прост).

*PGP* не предназначена для защиты исходных открытых данных в скомпрометированной системе. Она также не может предотвратить использование злоумышленником изощренных способов доступа к закрытому ключу во время его использования. Вы должны просто знать о существовании этих опасностей при использовании *PGP* в многопользовательской среде и соответствующим образом изменить свои ожидания и свое поведение. Возможно ваши обстоятельства таковы, что вы должны рассмотреть возможность использования *PGP* только на изолированной однопользовательской машине, находящейся под вашим непосредственным физическим контролем.

#### Анализ активности

Даже если атакующий не сможет прочитать содержимое вашей зашифрованной корреспонденции, он может извлечь по крайней мере некоторую полезную информацию, наблюдая, откуда приходят, и куда уходят сообщения, отмечая их размер и время дня, когда они отправляются. Это похоже на то, как если бы злоумышленник смог взглянуть на счет за междугородные телефонные переговоры, чтобы узнать, кому вы звонили, когда, и сколько времени разговаривали, даже если содержание телефонных разговоров остается ему неизвестно. Это называется “анализом активности”.

Решение этой проблемы требует введения специальных коммуникационных протоколов, разработанных для повышения сопротивления анализу активности в вашей коммуникационной среде. Возможно, при этом потребуются применение ряда криптографических приемов.

### Криптоанализ

Возможно, кто-то, обладающий суперкомпьютерными ресурсами (например, правительственная разведывательная служба) предпримет дорогостоящую и чудовищную криптоаналитическую атаку. Возможно, ему удастся сломать ваш ключ *RSA*, используя новые засекреченные знания в области разложения чисел на множители. Но гражданские ученые интенсивно и безуспешно атакуют этот алгоритм с 1978 г.

Возможно, правительство обладает каким-либо секретным методом взлома обычного шифра *IDEA*, использованного в *PGP*. Это – самый страшный кошмар для криптографа. Но абсолютных гарантий безопасности в практическом приложении криптографии не бывает.

И все же, осторожный оптимизм кажется оправданным. Разработчики алгоритма *IDEA* – одни из самых сильных криптографов Европы. Он подвергался интенсивной проверке на безопасность и экспертировался лучшими гражданскими криптографами мира. В том, что касается устойчивости к дифференциальному криптоанализу, он, вероятно, лучше *DES*.

Кроме этого, даже если этот алгоритм обладает какими-то до сих пор не замеченными слабыми местами, опасность сильно уменьшается из-за того, что *PGP* сжимает открытый текст до шифрования. Стоимость необходимых для взлома вычислений скорее всего будет больше ценности любого сообщения.

Если обстоятельства, в которых вы находитесь, оправдывают предположения о том, что вы можете подвергнуться столь чудовищной атаке, возможно, вам следует обратиться к консультанту по вопросам безопасности данных для выработки особого подхода, соответствующего вашим чрезвычайным требованиям.

В общем, без надежной криптографической защиты ваших данных, от противника не требуется практически никаких усилий для перехвата ваших сообщений, и он может делать это на повседневной основе, особенно если они передаются по модему или электронной почтой. Если вы используете *PGP* и соблюдаете разумные меры предосторожности, злоумышленнику потребуется затратить намного больше усилий и средств для нарушения вашей приватности.

Если вы защищаете себя от простейших атак, и чувствуете, что на вашу приватность не собирается посягать целеустремленный и обладающий огромными ресурсами противник, вы, вероятно, будете защищены *PGP*. *PGP* дает вам Почти Полную Приватность.

### Рекомендованная вводная литература

- Bacard Andre, "Computer Privacy Handbook," Peachpit Press, 1995
- Garfinkel Simson, "Pretty Good Privacy," O'Reilly & Associates, 1995
- Schneier Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition," John Wiley & Sons, 1996



Schneier Bruce, "E-mail Security," John Wiley & Sons, 1995  
Stallings William, "Protect Your Privacy," Prentice Hall, 1994

### Другая литература

Lai Xuejia, "On the Design and Security of Block Ciphers," Institute for Signal and Information Processing, ETH-Zentrum, Zurich, Switzerland, 1992  
Lai Xuejia, Massey James L., Murphy Sean" Markov Ciphers and Differential Cryptanalysis," Advances in Cryptology—EUROCRYPT'91  
Rivest Ronald, "The MD5 Message Digest Algorithm," MIT Laboratory for Computer Science, 1991  
Wallich Paul, "Electronic Envelopes," Scientific American, Feb. 1993, page 30.  
Zimmermann Philip, "A Proposed Standard Format for RSA Cryptosystems," Advances in Computer Security, Vol. III, edited by Rein Turn, Artech House, 1988

### Словарь терминов

**ASCII-текст (ASCII-Armored Text):** Двоичная информация, закодированная с использованием только стандартных печатаемых 7-битных символов, входящих в набор ASCII. В таком виде информация пригодна для передачи по любым сетевым каналам. Программа *PGP* использует для кодирования и декодирования ASCII-текста формат Radix-64 и по умолчанию придает именам файлов, содержащих ASCII-текст, расширение ".asc".

**Аутентификация (Authentication):** Проверка происхождения документа посредством верификации цифровой подписи, или проверка целостности открытого ключа путем сличения его уникального отпечатка с отпечатком оригинала.

**Сертифицировать (Certify):** Подписать чей-либо открытый ключ.

**Уполномоченный сертифициатор (Certifying Authority):** Пользующееся доверием лицо (или лица), которому дано право сертифицировать ключи и вносить их в общую базу данных.

**Расшифровка (Decryption):** Метод преобразования зашифрованной информации в понятную форму. Для расшифровки используется закрытый ключ получателя.

**Цифровая подпись (Digital Signature):** См. подпись.

**Шифрование (Encryption):** Метод преобразования информации в формат, непонятный никому, кроме адресата, который должен расшифровать сообщение для того, чтобы его прочитать.

**Посредник (Introducer):** Лицо или организация, которой позволено ручаться за аутентичность открытых ключей. Вы назначаете посредников, придавая их открытым ключам определенную степень доверия.

**Ключ (Key):** Цифровой код, используемый для шифрования, расшифровки, наложения подписи и верификации. Ключи генерируются парами и хранятся на связках.

**Депонирование ключей (Key Escrow):** Практика передачи пользователями копий своих закрытых ключей третьей стороне. При такой практике третья сторона получает доступ к содержанию зашифрованной коммуникации.

**Отпечаток (Key Fingerprint):** Строка из цифр и букв, уникальным образом идентифицирующая открытый ключ. Вы можете, например, позвонить по телефону владельцу открытого ключа, и попросить его продиктовать отпечаток своего ключа с тем, чтобы вы смогли сравнить его с

отпечатком своей копии его ключа. Если отпечатки не совпадают, вы узнаете, что ваша копия – подделка.

**Идентификатор ключа (Key ID):** Читаемая строка, однозначно идентифицирующая пару ключей. Две пары ключей могут обладать одинаковыми идентификаторами пользователя, но идентификаторы ключа у них будут разными.

**Пара ключей (Key Pair):** Открытый ключ и дополняющий его закрытый ключ. В криптосистеме с открытыми ключами, такой, как *PGP*, каждый пользователь имеет по крайней мере одну пару ключей.

**Связка (Keyring):** Набор ключей. Каждый пользователь обладает связками двух типов: связкой закрытых ключей и связкой открытых ключей.

**Дайджест сообщения (Message Digest):** Компактный “дистиллят” сообщения или контрольная сумма файла. Он является функцией вашего сообщения: будь оно изменено, его дайджест был бы другим.

**Пароль (Passphrase):** Последовательность нажатия клавиш, вводимая для получения исключительного доступа к вашему закрытому ключу, который используется при наложении подписи на сообщения и файлы, а также при расшифровке сообщений и файлов, вам адресованных.

**Открытый текст (Plaintext):** Обычный, читаемый, не зашифрованный и не подписанный текст.

**Закрытый ключ (Private Key):** Секретная половина пары ключей, используемая для наложения подписи и расшифровки информации. Закрытый ключ каждого пользователя должен храниться в тайне и быть известен только ему.

**Связка закрытых ключей (Private Keyring):** Набор из одного или нескольких закрытых ключей, принадлежащих владельцу связки.

**Открытый ключ (Public Key):** Тот ключ из пары, который используется для шифрования информации и верификации подписи. Открытый ключ пользователя может свободно распространяться среди других участников системы и передаваться посторонним. Обладание открытым ключом пользователя не позволяет вычислить соответствующий закрытый ключ.

**Связка открытых ключей (Public Keyring):** Набор открытых ключей. Ваша связка открытых ключей включает ваш собственный открытый ключ.

**Криптография с открытым ключом (Public-Key Cryptography):** Криптографическая технология, при которой используется пара из открытого и закрытого ключей, и не требующая безопасности используемого канала связи.

**Подписать (Sign):** Наложить подпись.

**Подпись (Signature):** Цифровой код, создаваемый с помощью закрытого ключа. Подпись позволяет аутентифицировать информацию в процессе верификации подписи. Когда вы подписываете сообщение или файл, программа *PGP* использует ваш закрытый ключ для генерации цифрового кода, который однозначно зависит как от содержания сообщения, так и от вашего закрытого ключа. Чтобы проверить вашу подпись, любой может использовать ваш открытый ключ.

**Текст (Text):** Обычный печатаемый 7-битный текст в коде ASCII.

**Надежный (Trusted):** Открытый ключ называется надежным, если его сертифицировали вы или кто-то, кого вы назначили представителем.

**Идентификатор пользователя (User ID):** Фраза, идентифицирующая пару ключей. В качестве идентификатора пользователя обычно используется полное имя владельца и его адрес электронной почты. Идентификатор

пользователя помогает пользователям (владельцу пары и другим участникам системы) идентифицировать принадлежность пары.

**Верификация (Verification):** Сравнение подписи, созданной с помощью закрытого ключа, и расшифрованной с помощью открытого, с дайджестом сообщения. Верификация доказывает, что информация была действительно послана номинальным отправителем, и что сообщение не претерпело после наложения подписи никаких изменений.

## Дополнение Ресурсы PGP, доступные в Internet

Международный релиз PGP 5.0 распространяется бесплатно. Информация о способах его получения (а также о способах получения настоящего перевода документации в электронном виде) представлена на страницах *Русского Альбома PGP* (по-русски) и на *The International PGP Homepage* (по-английски и на других языках).

### PGP, Inc.'s Homepage



<http://www.pgp.com>

### The International PGP Homepage



<http://www.pgpi.com>

### Русский Альбом PGP



<http://www.geocities.com/SoHo/Studios/1059/pgp-ru.html>

### MIT's PGP Homepage



<http://web.mit.edu/network/pgp.html>

### PGP.net

<http://www.pgp.net>