Эссе на тему:

«PGP. Распределение ключей. Web of Trust»

Выполнил студент 012 группы Лукьянченко Дмитрий.

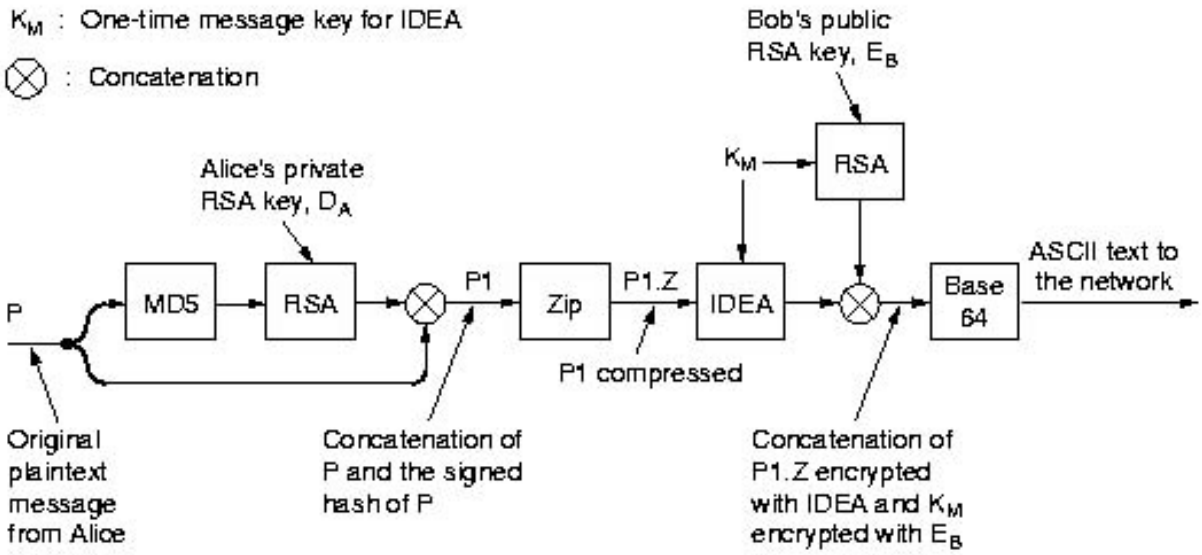
Криптозащита электронной почты.

К настоящему времени разработано множество криптографических алгоритмов и протоколов кодирования. Среди алгоритмов симметричной криптографии (здесь используется один ключ, по которому в соответствии с алгоритмом закодируется и раскодируется информация), можно выделить RC4, RC5, CAST, DES, AES и т.д. Что касается асимметричного кодирования (здесь используются два ключа: открытый - отвечает за кодирование информации и раздается всем желающим, и секретный, который раскодирует защищенную информацию), то тут в основном используются алгоритмы RSA, Diffie-Hellman и El-Gamal, при этом длина ключей кодирования обычно составляет 2048 бит. На основе алгоритма RSA в начале 90-х годов американцем Филом Циммерманном разработана программа PGP (Pretty Good Privacy). Это полный пакет безопасности, который включает средства конфиденциальности, установления подлинности, электронной подписи, сжатия и все это в удобной для использования форме. Благодаря этому, а также что это разработка далекого от государственных структур человека, качественная, работает как на платформе Unix, так и MS-DOS/Windows, Macintosh и распространяется бесплатно, этот она получила очень широкое распространение.

Циммерман был обвинен в нарушении ряда законов США о шифровании. Это позволило ему выдвинуть лозунг "Если конфиденциальность - вне закона, то она доступна только тем, кто вне закона".

PGP.

PGP использует алгоритмы шифрования RSA, IDEA и MD5. PGP поддерживает компрессию, передаваемых данных, их секретность, электронную подпись и средства управления доступа к ключам. Схема работы PGP показана на рис1. На этом рисунке - D_A ,



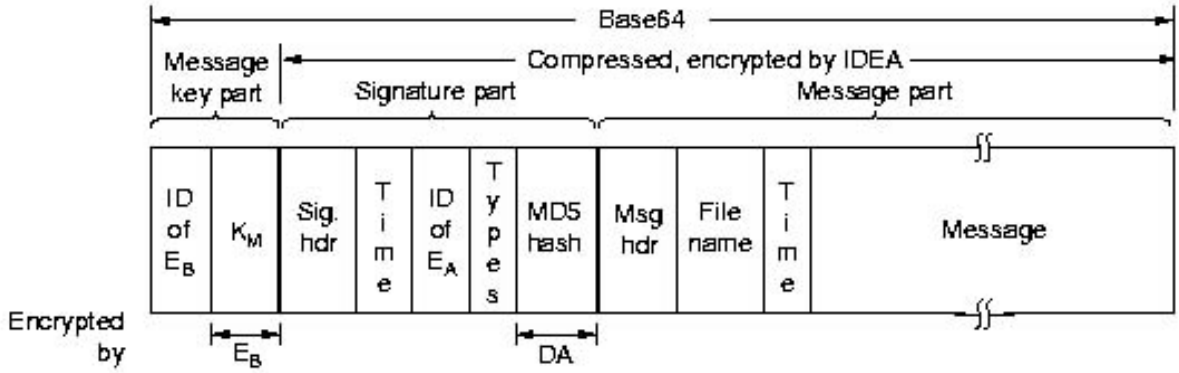
D_B личные (закрытые) ключи A и B соответственно, а E_A , E_B - их открытые ключи.

Отметим, что секретный ключ для IDEA строится автоматически по ходу работы PGP на стороне A и называется ключом сессии - K_M, который затем шифруется алгоритмом RSA с открытым ключом пользователя B. Так же следует обратить внимание на то, что медленный алгоритм RSA используется для шифрования коротких фрагментов текста: 128 бит MD5 и 128 бит IDEA ключа.

PGP поддерживает три длины ключей:

- Обычный - 314 бит (может быть раскрыт за счет больших затрат);
- Коммерческий - 512 бит (может быть раскрыт специализированными организациями, названия которых, как правило, состоит из трех букв);
- Военный - 1024 бита (не может быть раскрыт пока ни кем на земле).

Структурная схема PGP:



Распределение ключей. Web of Trust.

Каждый пользователь PGP может самостоятельно сгенерировать свой ключ. Каждый пользователь может присвоить ключу любое имя и любой e-mail-адрес. Всё это открывает широкий простор для жульничества и атак по методу "человек в середине". Дабы убедиться, что конкретный ключ действительно принадлежит предполагаемому владельцу, нужно как-то это проверить. Это нетрудно, если вы лично знакомы с человеком, в противном же случае может оказаться весьма затруднительным. Основной из механизмов, предлагаемых PGP для решения этой проблемы - это *цифровые сертификаты ключей* и модель отношений доверия *Web of Trust*.

О сертификатах ключей.

Сертификат открытого ключа PGP — это форма удостоверения, несущая идентификацию пользователя (т.е. объективный способ его опознавания), и связанная с определённым открытым ключом с помощью подтверждающей подписи третьей стороны — подписи поручителя. На сегодняшний день не существует устоявшегося определения подтверждающей подписи. Такая подпись на сертификате ключа может иметь примерно следующее значение: *"Я поручаюсь в том, что подписанный мною ключ действительно принадлежит лицу, указанному в сведениях (идентификации) сертификата"*. Такое значение, к сожалению, нельзя считать достаточным и полным: например, кому из всех живущих на Западе людей с именем Joe Smith принадлежит конкретный ключ с таким именем в сертификате, каков источник уверенности поручителя, что ключ принадлежит данному Джо Смиту, подтверждает ли поручитель, что Джо Смит является истинным владельцем указанного в сертификате почтового ящика smith@matrix.com?

Поэтому более точное значение подтверждающей подписи звучит так: *"Я поручаюсь, основываясь на своей личной непосредственной убеждённости и объективных подтверждающих свидетельствах, в том, что подписанный мною открытый ключ и связанный с ним закрытый ключ действительно принадлежат лицу, чьё имя, e-mail и*

другие идентификационные сведения указаны в сертификате ключа". Чтобы дать такую подтверждающую подпись, поручитель обязан удостовериться в следующем (в приведённой последовательности): ключ индивидуален и уникален. Для этого владелец ключа должен сообщить его цифровой отпечаток; указанный в сертификате ключа человек (имя, фото) является тем, за кого себя выдаёт. Обычно с этой целью проверяют персональные документы государственного образца или иное надёжное удостоверение личности с фотографией; владелец открытого ключа обладает соответствующим закрытым ключом. Если он может расшифровать зашифрованный данным открытым ключом текст и сгенерировать цифровую подпись, сверяемую данным открытым ключом, значит он владеет и соответствующим закрытым ключом; в сертификате указаны принадлежащие владельцу ключа контактные координаты. Он должен доказать, что имеет полный доступ к этим координатам для получения и отправки сообщений.

Но даже если поручитель заверил своей подписью сертификат и ключ, подразумевая именно такое значение своей подтвеждающей подписи, всё равно ряд вопросов остаются открытыми: каким документом владелец ключа удостоверил свою личность, надёжен ли этот документ, было ли удостоверение личности подлинным, не был ли закрытый ключ скомпрометирован и похищен? Эти вопросы вплотную подводят нас к критерию доверия в среде асимметричных криптосистем и к распределённой модели доверия PGP *Web of Trust*.

Распределённость против централизованности.

Модели доверия в криптосистемах с открытым ключом делятся на два крупных вида: централизованные и распределённые. В централизованных, или иерархических, моделях все пользователи системы полагаются на доверие к одному корневому источнику, подтверждающему достоверность всех открытых ключей. Такая модель обычно применяется в корпоративной среде (где единый источник доверия обязателен) и в системах удостоверяющих центров на базе стандарта X.509, хотя бывают и исключения, например, удостоверяющий центр Thawte Consulting, реализующий, как схему с единым сервером-хранителем ключей, так и PGP, распределённую модель, также называемую сетью доверия.

В такой системе нет единого источника сертификации, напротив, каждый пользователь самостоятельно решает, кому он доверяет, а кому не доверяет в удостоверении других открытых ключей, создавая тем самым личную сеть поручителей. Такой подход обеспечивает гибкость и устойчивость системы к любому злонамеренному воздействию: можно повлиять на один узел распределённой системы, но тысячи других узлов сохранят полную надёжность. В качестве наглядного примера приведу выдержку из статьи Брюса Шнайера, опубликованной в мартовском выпуске его журнала-рассылки CRYPTO-GRAM:

"...Предположим, у меня есть несколько пачек денег, каждая из которых помещена в индивидуальную систему защиты. Системы защиты характеризуются стоимостью их взлома. 100-долларовая пачка денег, защищённая 200-долларовой системой, хранится надёжно, поскольку пытаться её украсть экономически невыгодно. 100-долларовая пачка, находящаяся в 50-долларовой системе, недостаточно защищена, ибо взломщик получит выгоду в 50 долларов от кражи, что делает попытку взлома оправданной.

Вот мой пример. Есть десять 100-долларовых пачек, каждая хранится в индивидуальной 200-долларовой системе защиты. Все они в безопасности. И есть ещё десять 100-долларовых пачек, которые хранятся в 50-долларовых системах. Они защищены ненадёжно.

Положение как-то нужно изменить. Можно, например, заменить все самостоятельные системы защиты одной централизованной системой. Эта новая система гораздо лучше и надёжней обыкновенных: её взлом обойдётся в 500 долларов.

К сожалению, новая дорогая система не обеспечит лучшей сохранности денег. При старых системах можно было похитить десять пачек с издержками в 50 долларов на пачку (вы помните, другие десять пачек похищать экономически нецелесообразно); суммарный доход взломщика составит 500 долларов. С новой системой мы имеем двадцать 100-долларовых пачек, защищённых единой 500-долларовой системой. Взломщик теперь имеет куда больший стимул взломать эту более надёжную систему, ведь он сможет украсть 2000 долларов, затратив всего 500 долларов на взлом, в итоге извлекая из операции 1500 долларов прибыли.

Это и есть проблема централизации. Если индивидуальные системы безопасности объединены в одну общую систему, желание и стимул взломать её обычно оказываются гораздо выше. Несмотря на то, что централизованная система может быть намного надёжней каждой самостоятельной системы в отдельности, общая защищённость может стать даже ниже, если централизованную систему взломать легче, чем ВСЕ индивидуальные системы вместе взятые."

Зачем плести сеть?

Общая проблема всей асимметричной криптографии — сложность проверки аутентичности открытых ключей. Непросто с достаточной точностью определить, что конкретный открытый ключ является подлинным и принадлежит предполагаемому владельцу, и ещё труднее это в среде PGP, где нет единого источника сертификации ключей, как в условиях инфраструктур PKI (Personal Key Infrastructure). С другой стороны, распределённая природа модели доверия PGP имеет и свои преимущества.

Рассмотрим простой пример. (Пример приведен дословно, т.к. требуются точные данные о ключах PGP).

К пользователю “B” (Владиславу Миллеру) приходит подписанное письмо от пользователя “A” (Олафа Колкмана из европейской организации RIPE = Reseaux IP Europeenne). Чтобы сверить цифровую подпись пользователю “B” нужен открытый ключ “A”. Для его получения удобнее воспользоваться интерфейсом депозитария, введя в строку запроса email-адрес отправителя письма. Но откуда уверенность, что в результатах поиска “B” получит открытый ключ именно этого человека, а не качественную фальшивку, которой также заверено и письмо (тем более, что один из ключей в результатах был аннулирован)? Злоумышленник мог создать собственный ключ, указав в сертификате идентификацию реального человека, а потом загрузить этот поддельный ключ на сервер.

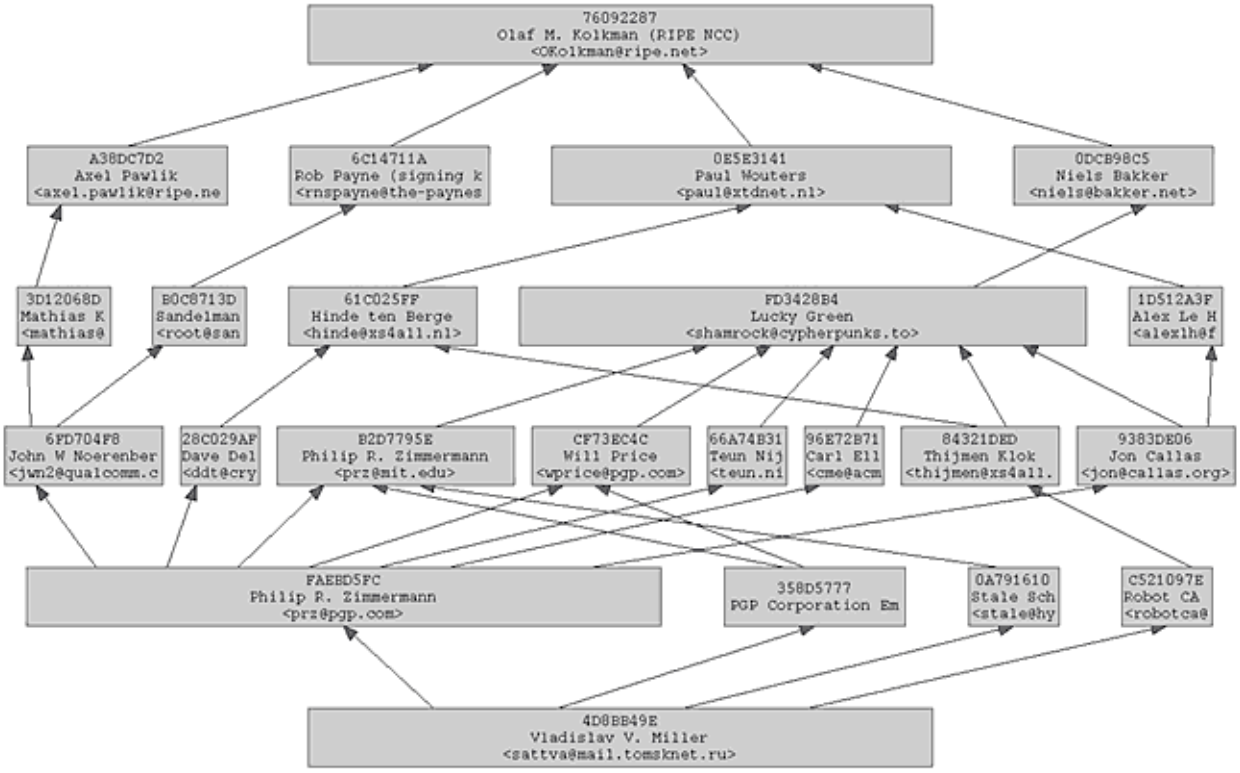
Значит, “B” придётся каким-то образом удостовериться в подлинности ключа “A”. Есть несколько способов сделать это:

- В RIPE “B” выясняет, в каком государстве проживает “A”, берет официальный телефонный справочник этой страны и звонит по его номеру. По телефону “A” называет “B” цифровой отпечаток своего ключа, который “B” сверяет с находящейся у него копией.
- “B” приезжает в гости к “A”, “A” предъявляет удостоверение личности, отпечаток своего открытого ключа и доказывает, что обладает соответствующим закрытым.
- “B” находит другого человека, который может подтвердить (поручиться), что находящийся у “B” открытый ключ действительно принадлежит “A”.

Первый способ применим, только если “B” знаком голос владельца ключа. В ином случае кто угодно на том конце может заявить, что он “A”. Второй способ слишком затратен и непрактичен — ради одной только аутентификации ключа “B” не станет ездить по зарубежьям. А вот третий вариант наиболее удобен, поскольку всю процедуру можно совершить электронно, не покидая собственного дома.

Для этой цели существует специальный инструмент, называемый визуализатор цепочек сертификации. В него “B” вводит ID своего ключа, от которого желает проследить путь поручительств (0x4D8BB49E), и ID подозрительного ключа,

достоверность которого нужно оценить (0x76092287). Система обрабатывает запрос и выдаёт следующую схему:



В прямоугольнике в основании схемы указан открытый ключ “B”, вверху — подозрительный ключ “A”. Направление стрелки от одного ключа к другому указывает на то, что второй ключ подписан первым, владелец которого выступает поручителем другого.

У “B” (Владислав Миллер) есть подлинная копия служебного ключа PGP Corporation (0x358D5777), которым компания подписывает открытые ключи своих сотрудников. По этой схеме “B” может определить, что названным ключом был заверен ключ Уилла Прайса (0xCF73EC4C), вице-президента по разработкам PGP Corporation, следовательно, у “B” есть все основания доверять его подлинности. Уилл Прайс, в свою очередь, является поручителем за достоверность ключа Лаки Грина (0xFD3428B4), а тот подверждает подлинность ключа Нилса Баккера (0x0DCB98C5). Нилс Баккер подписал ключ Олафа Колкмана (“A”), по-видимому, имея достаточные основания быть уверенным в подлинности его ключа. Даже если “B” не доверяет подтверждающей подписи Нилса Баккера, есть ещё по меньшей мере три несовмещённых цепочки сертификации, поручительствующие за подлинность ключа Колкмана. В качестве промежуточных звеньев цепочек много людей, которым “B” в полной мере доверяет, считая их абсолютно компетентными в проверке надёжности ключей; кроме того, ключ “A” (Колкмана) от ключа “B” отделяет всего четыре степени разделения, иными словами, четыре звена поручителей, что совсем немного в сравнении со среднестатистическими шестью. Поэтому (по личному убеждению “B”) вероятность того, чтобы полученный мною ключ “A” оказался поддельным, крайне мала.

Всё же в ходе анализа схемы может возникнуть вопрос, насколько “B” может быть уверен в надёжности того или иного звена цепочки сертификации, особенно, если приходится полагаться на небольшое количество несовмещённых цепочек. Для сбора дополнительных сведений о любом ключе можно использовать другой инструмент — запрос в статистику Сети доверия, что позволяет по индексу MSD (mean strong set distance, средняя удалённость от прочного набора) составить представление о положении ключа в

системе Сети доверия, по количеству и составу поручителей примерно оценить компетентность его владельца и "вес" издаваемых им подписей.

Приведённая здесь схема довольно сложна и богата на несовмещённые цепочки сертификации. Несовмещёнными цепочками называются такие, которые не имеют общих звеньев поручителей (как видно из схемы, во второй степени разделения несовмещённых цепочек аж восемь, а в последней — четыре). Чем больше таких параллельных путей поручительств, тем меньше вероятность, что подозрительный ключ недостоверен: маловероятно, чтобы сразу несколько человек в таком случае поручились за его подлинность.

Чтобы иметь возможность находить такие комплексные цепочки, очень важно, чтобы пользователи проверяли подлинность ключей своих корреспондентов, заверяли их подписями и обновляли на сервере. В конечном итоге это будет благом для всех. Такие взаимные поручительства образуют своего рода сеть, именно поэтому модель доверия PGP называется Web of Trust — Сеть доверия.

Понятие доверия

Всякий открытый ключ на своей связке вы можете наделить некоторой степенью доверия в сертификации других ключей. Это значит, что если к вам в руки попадёт ключ Б, подписанный ключом А, подтверждающей подписи которого вы всецело доверяете, ключ Б будет расценен изначально достоверным, избавляя вас от необходимости проверять его подлинность самостоятельно.

Чтобы наделить чужой ключ той или иной степенью доверия (ключ уже должен быть расценен программой как подлинный), подумайте, какого доверия заслуживает его владелец, порядочный и честный ли это человек, насколько он компетентен в работе с PGP, достаточное ли имеет понимание механизмов и уязвимостей асимметричной криптографии. Помочь в этом деле может анализ ключа в Сети доверия: сколько и какие ключи заверил этот человек, раздаёт ли он подписи направо и налево, кто сертифицировал его ключ, много ли перекрёстных подписей и какого их качество. Интегральным показателем этих критериев становится ранг ключа в Сети доверия, основанный на индексе MSD. Всем этим процедура наделения доверием существенно отличается от сертификации ключа, когда вы должны оценить только его взаимосвязь с предполагаемым владельцем, но не личностные качества владельца ключа.

Рассматривая схему несовмещённых цепочек, пытаясь определить подлинность подозрительного ключа, обязательно убедитесь, что в составе промежуточных звеньев есть хотя бы несколько человек, которым вы доверяете в сертификации ключей. Если цепочка сертификации не содержит доверенных поручителей, вы не должны полагаться на неё как на оценочный критерий.

Анатомия Сети доверия.

Чем больше взаимных перекрёстных сертифицирующих подписей будет аккумулировано в Сети доверия, тем короче начнут становиться цепочки сертификации, и тем выше станет общая убеждённость в подлинности всякого ключа. Ключи, надёжно связанные множеством коротких удостоверяющих цепочек, называются прочным набором. Количество этих ключей в настоящее время составляет примерно 25 тысяч, и именно они образуют стержень и ядро всей Сети доверия, или связного набора — ключей, имеющих хотя бы одну цепочку сертификации от прочного набора. Связный набор исчерпывается примерно 70 тысячами ключей, при этом в названные 70 тысяч входят 25 тысяч ключей прочного набора. Ключи из связного набора, не входящие в прочный набор, называют периферийным набором (порядка 45 тысяч).

Разумеется “вселенная” ключей PGP не исчерпывается связным набором, границы которого обозначают границы Большой Сети доверия. На общественных серверах Интернета хранится около двух миллионов открытых ключей, которые образуют

"Большую связку". Большинство из них не имеет сертифицирующих подписей; некоторые имеют подписи, но не от ключей, входящих в Большую Сеть доверия. Такие небольшие группы взаимоподписанных ключей и ключи, не имеющие подтверждающих подписей, называются изолированным набором. Они не учитываются в статистике Сети доверия, и определить их подлинность по приведённому выше методу анализа цепочек сертификации невозможно. Если же любой владелец ключа из связного набора проверит надёжность одного из изолированных ключей и подпишет его, подтверждающая подпись окажется связующим звеном, ведущим к сердцу прочного набора, и эта группа изолированных ключей тут же вольётся в Большую Сеть доверия.

Keyserver (Сервер ключей).

Серверы, или депозитарии, ключей OpenPGP, — это открытые базы данных, простые хранилища сертификатов. Дабы упростить своим потенциальным корреспондентам задачу нахождения вашего открытого ключа, вы можете загрузить его на сервер. Аналогично, когда у вас возникнет потребность отправить человеку зашифрованное письмо, просто воспользуйтесь формой поиска для нахождения его открытого ключа в базе.

Кроме загрузки и поиска ключей, к вашим услугам сводная статистика сети доверия PGP Web of Trust, а также базирующиеся на ней специальные механизмы отслеживания путей сертификации ключей и оценки "авторитетности" и "веса" любого ключа в системе Web of Trust. Механизм отслеживания пути сертификации позволяет установить цепочку подписаний от ключа А к ключу Б, выявляя все промежуточные звенья поручителей. Это один из вспомогательных методов определения подлинности и достоверности конкретного ключа. Анализ и оценка положения ключа в системе Web of Trust также позволяет определить, как давно ключ циркулирует в Интернете, насколько весомой можно считать его сертифицирующую подпись и т.д.

Источники информации:

- http://www.pgpru.com (“PGP в России”);
- http://www.dpost.ru/main.php?pg=crypto (Деловая почта Оптимальное решение по защите электронной почты);
- http://ergeal.ru/txt/archive/cs/Smell/new1999/Email.htm (Архивы Замка Дракона / Лекции ВМиК / Сети / Электронная почта).