PGP. Принцип функционирования. Свойства ключа.

Установка и применение программы PGP

Куделя А.Г.

PGP – это криптографическая (шифровальная) программа с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности.

- Главное преимущество этой программы состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи т.к. эта программа построена на новом принципе работы – публичной криптографии или обмене открытыми (публичными) ключами, где пользователи могут открыто посылать друг другу свои публичные ключи с помощью сети «Интернет» и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц к их конфиденциальным сообщениям.
- В PGP применяется принцип использования двух взаимосвязанных ключей: открытого и закрытого. К закрытому ключу имеете доступ только вы, а свой открытый ключ вы распространяете среди своих корреспондентов.
- Великолепное преимущество этой программы состоит также в том, что она бесплатная и любой пользователь, имеющий доступ к Интернету, может ее «скачать» на свой компьютер в течение получаса. PGP шифрует сообщение таким образом, что никто кроме получателя сообщения, не может ее расшифровать. Создатель PGP Филипп Циммерман открыто опубликовал код программы, который неоднократно был исследован специалистами крипто-аналитиками высочайшего класса и ни один из них не нашел в программе каких-либо слабых мест.

КАК PGP РАБОТАЕТ

- Когда пользователь шифрует сообщение с помощью PGP, то программа сначала сжимает текст, что сокращает время на отправку сообщения через модем и увеличивает надежность шифрования. Большинство приемов криптоанализа (взлома зашифрованных сообщений) основаны на исследовании «рисунков», присущих текстовым файлам, что помогает взломать ключ. Сжатие ликвидирует эти «рисунки» и таким образом повышает надежность зашифрованного сообщения. Затем PGP генерирует сессионный ключ, который представляет собой случайное число, созданное за счет движений вашей мышки и нажатий на клавиши клавиатуры.
- Как только данные будут зашифрованы, сессионный ключ зашифровывается с помощью публичного ключа получателя сообщения, который отправляется к получателю вместе с зашифрованным текстом.
- Расшифровка происходит в обратной последовательности. Программа PGP получателя сообщения использует закрытый ключ получателя для извлечения временного сессионного ключа, с помощью которого программа затем дешифрует зашифрованный текст.

КЛЮЧИ

- Ключ – это число, которое используется криптографическим алгоритмом для шифрования текста. Как правило, ключи - это очень большие числа. Размер ключа измеряется в битах. Число, представленное 1024 битами – очень большое. В публичной криптографии, чем больше ключ, тем его сложнее взломать.
- В то время как открытый и закрытый ключи взаимосвязаны, чрезвычайно сложно получить закрытый ключ исходя из наличия только открытого ключа, однако это возможно при наличии большой компьютерной мощности. Поэтому крайне важно выбирать ключи подходящего размера: достаточно большого для обеспечения безопасности и достаточно малого для обеспечения быстрого режима работы. Кроме этого, необходимо учитывать личность того, кто намеревается прочитать ваши зашифрованные сообщения, насколько он заинтересован в их расшифровке, каким временем он обладает, и какие у него имеются ресурсы.
- Более большие ключи будут более надежными в течение более длительного срока времени. Поэтому если вам необходимо зашифровать информацию с тем, чтобы она хранилась в течение нескольких лет, то необходимо использовать более крупный ключ.
- Ключи хранятся на жестком диске вашего компьютера в зашифрованном состоянии в виде двух файлов: одного для открытых ключей, а другого - для закрытых. Эти файлы называются «кольцами» (keyrings). В течение работы с программой PGP вы, как правило, будете вносить открытые ключи ваших корреспондентов в открытые «кольца». Ваши закрытые ключи хранятся в вашем закрытом «кольце». При потере вашего закрытого «кольца» вы не сможете расшифровать любую информацию, зашифрованную с помощью ключей, находящихся в этом «кольце».

ЦИФРОВАЯ ПОДПИСЬ и ХЭШ-ФУНКЦИЯ

- Огромным преимуществом публичной криптографии также является возможность использования цифровой подписи, которая позволяют получателю сообщения удостовериться в личности отправителя сообщения, а также в целостности (верности) полученного сообщения. Цифровая подпись исполняет ту же самую функцию, что и ручная подпись. Однако ручную подпись легко подделать. Цифровую же подпись почти невозможно подделать.
- Еще одно важное преимущество использования PGP состоит в том, что PGP применяет так называемую «хэш-функцию», которая действует таким образом, что в том случае какого-либо изменения информации, пусть даже на один бит, результат «хэш-функции» будет совершенно иным. С помощью «хэш-функции» и закрытого ключа создается «подпись», передаваемая программой вместе с текстом. При получении сообщения получатель использует PGP для восстановления исходных данных и проверки подписи.
- При условии использования надежной формулы «хэш-функции» невозможно вытащить подпись из одного документа и вложить в другой, либо каким-то образом изменить содержание сообщения. Любое изменение подписанного документа сразу же будет обнаружено при проверке подлинности подписи.

ПАРОЛЬНАЯ ФРАЗА

- Большинство людей, как правило, знакомы с парольной системой защиты компьютерных систем от третьих лиц.
- Парольная фраза – это сочетание нескольких слов, которое теоретически более надежно, чем парольное слово. В виду того, что парольная фраза состоит из нескольких слов, она практически неуязвима против так называемых «словарных атак», где атакующий пытается разгадать ваш пароль с помощью компьютерной программы, подключенной к словарю. Самые надежные парольные фразы должны быть достаточно длинными и сложными и должны содержать комбинацию букв из верхних и нижних регистров, цифровые обозначения и знаки пунктуации.
- Парольная фраза должна быть такой, чтобы ее потом не забыть и чтобы третьи лица не могли ее разгадать. Если вы забудете свою парольную фразу, то уже никогда не сможете восстановить свою зашифрованную информацию. Ваш закрытый ключ абсолютно бесполезен без знания парольной фразы и с этим ничего не поделаешь.

ОСНОВНЫЕ ШАГИ В ИСПОЛЬЗОВАНИИ ПРОГРАММЫ PGP

- 1. Установите программу на свой компьютер. Руководствуйтесь краткой инструкцией по инсталляции программы, приведенной ниже.
- 2. Создайте закрытый и открытый ключ. Перед тем, как вы начнете использовать программу PGP, вам необходимо генерировать пару ключей, которая состоит из закрытого ключа, к которому имеете доступ только вы, и открытый ключ, который вы копируете и свободно передаете другим людям (вашим корреспондентам).
- 3. Распространите свой открытый ключ среди своих корреспондентов в обмен на их ключи. Ваш открытый ключ, это всего лишь маленький файл, поэтому его можно либо воткнуть в сообщение, копировать в файл, прикрепить к почтовому сообщению или разместить на сервере.
- 4. Удостовериться в верности открытого ключа. Как только вы получите открытые ключи своих корреспондентов, то их можно внести в «кольцо» открытых ключей. После этого вам необходимо убедиться в том, что у вас действительно открытый ключ вашего корреспондента. Вы можете это сделать, связавшись с этим корреспондентом и, попросив его зачитать вам по телефону «отпечатки пальцев» (уникальный идентификационный номер) его открытого ключа, а также сообщив ему номер вашего ключа. Как только вы убедитесь в том, что ключ действительно принадлежит ему, вы можете его подписать и таким образом подтвердить ваше доверие к этому ключу.
- 5. Шифрование и удостоверение корреспонденции вашей цифровой подписью. После генерации пары ключей и обмена открытыми ключами вы можете начать шифрование и удостоверение ваших сообщений и файлов своей цифровой подписью. Если вы используете почтовую программу, которая поддерживается программой PGP, то вы можете шифровать и дешифровать всю вашу корреспонденцию, находясь прямо в этой программе. Если же ваша почтовая программа не поддерживается программой PGP, то вы можете шифровать вашу корреспонденцию другими способами (через буфер обмена или шифрованием файлов целиком).
- 6. Дешифровка поступающих к вам сообщений и проверка подлинности отправителя. Когда кто-либо высылает вам зашифрованное сообщение, вы можете дешифровать его и проверить подлинность отправителя этого сообщения и целостность самого сообщения. Если ваша почтовая программа не поддерживается PGP, то вы можете сделать это через буфер обмена.
- 7. Уничтожение файлов. Когда вам необходимо полностью удалить какой-либо файл, вы можете исполнить команду wipe (стереть). Таким образом, удаленный файл уже невозможно будет восстановить.

PGP диск

- PGP диск – это удобное приложение, которое позволяет вам отвести некоторую часть вашего жесткого диска для хранения конфиденциальной информации. Это зарезервированное место используется для создания файла под именем <PGP disk>.
- Хотя это всего лишь один файл, он действует подобно вашему жесткому диску в том отношении, что он выполняет функцию хранения ваших файлов и исполняемых программ. Вы можете его себе представить в виде флоппи дискеты или внешнего жесткого диска. Для того, чтобы использовать программы и файлы, находящиеся на нем, вы его устанавливаете <mount>, после чего его можно использовать также, как любой другой диск. Вы можете установить программы внутри этого диска либо копировать на него файлы. После того, как вы отключите <unmount> этот диск, он станет недоступным для третьих лиц и для того, чтобы открыть его, необходимо ввести парольную фразу, которая известна только вам. Но даже разблокированный диск защищен от несанкционированного доступа. Если ваш компьютер зависнет во время использования диска, то его содержание будет зашифровано.
- Одним из наиболее важных преимуществ и удобств использования программы PGPdisk является тот факт, что теперь нет необходимости шифровать большое количество файлов, в которых находится конфиденциальная информация. Теперь можно переместить все конфиденциальные файлы и даже программы на такой диск и таким образом избежать необходимости каждый раз расшифровывать какой-либо файл при его открытии.

Как создать новый PGP диск

1. Запустите программу PGPdisk
2. Исполните команду New, после чего на экране появится мастер создания PGP диска.
3. Нажмите на next
4. Появится окошко создания PGP диска, в котором необходимо указать путь, где новый диск под названием <New PGPdisk1> надо сохранить.
5. Нажмите на кнопку Save и файл под этим названием сохранится на диске, выбранном вами (по умолчанию на диске C).
6. Под надписью <PGPdisk Size field> введите цифру, обозначающую размер PGP диска и не забудьте выбрать килобайты или мегабайты там же.
7. Под надписью <PGPdisk Drive Letter Field> подтвердите букву, которую вы присвоите новому диску.
8. Нажмите на next
9. Введите парольную фразу, которую в дальнейшем необходимо будет вводить для установки нового диска. Введите парольную фразу два раза.
10. Нажмите на next
11. При необходимости подвигайте мышку или нажимайте на кнопки на клавиатуре для того, чтобы программа сгенерировала новый ключ
12. Нажмите на next. Столбик покажет вам инициализацию создания нового диска.
13. Еще раз нажмите на next, с тем, чтобы окончательно установить новый PGP диск.
14. Нажмите на Finish.
15. Введите название нового диска.
16. Нажмите на Start
17. Нажмите на OK (на диске еще нет данных). Компьютер скажет вам, когда закончится форматирование диска.
18. Нажмите на кнопку Close на окне форматирования. Теперь ваш новый диск появится на том диске, который вы ранее указали (по умолчанию диск C). Для того, чтобы открыть диск, надо дважды нажать на него мышкой.

Установка и Закрытие PGP диска

- Как только новый диск будет создан, программа PGP автоматически его установит с тем, чтобы вы могли начать его использовать. После того, как вы закончили работу с конфиденциальной информацией, необходимо отключить диск. После отключения диск его содержимое будет зашифровано в виде зашифрованного файла.
- Для открытия PGP диска надо дважды щелкнуть по нему мышкой и дважды ввести парольную фразу в появившееся окно программы. Вы сможете убедиться в том, что PGP диск открылся, зайдя в мой компьютер и увидев, что рядом с диском C появился диск D. В том случае, если у вас уже есть диск D, то новый диск получит следующую букву E и т.д. Зайти на новый диск можно через мой компьютер или другую оболочку просмотра файлов.
- Использование установленного PGP диска
- На диске PGP можно создавать файлы, каталоги, перемещать файлы или каталоги, либо стирать, т.е. можно делать те же самые операции, что и на обычном диске.
- Закройте все программы и файлы, имеющиеся на диске PGP, т.к. невозможно закрыть диск, если файлы на этом диске до сих пор еще открыты. Теперь зайдите в мой компьютер выделите мышкой диск PGP, нажмите на правую кнопку мышки и выберите команду <unmount> в появившемся меню <PGP disk>.
- Как только диск будет закрыт, то он исчезнет из моего компьютера и превратится в зашифрованный файл на диске C.
- Еще один важный момент, на который необходимо обратить внимание, это настройки программы, которые позволяют автоматически закрыть диск в случае не обращения к диску в течение какого-либо периода времени. Для этого надо исполнить команду <prefs> в программе PGPdisk и в появившемся меню под названием <auto unmount> (автоматическое закрытие) выделить флажками все три команды:
- · auto unmount after __ minutes of inactivity (автоматически закрыть после __ минут бездействия). Здесь также необходимо указать количество минут.
- · auto unmount on computer sleep (автоматически закрыть при переходе компьютера в спящее состояние)
- · prevent sleep if any PGPdisks could not be unmounted (не позволить компьютеру перейти в состояние спячки, если PGP диск не был закрыт)

Смена и удаление парольной фразы

- Смена
- 1. Убедитесь в том, что PGP диск не установлен. Невозможно сменить парольную фразу в том случае, если диск установлен.
- 2. Выберите команду <Change Passphrase> из меню <File>
- 3. Выберите тот диск, парольную фразу для которго вы хотите изменить.
- 4. Введите старую парольную фразу. Нажмите на ОК. Появится окошко для ввода новой парольной фразы.
- 5. Введите новую парольную фразу. Минимальная длина парольной фразы: 8 знаков
- 6. Нажмите на ОК. Окошко новой парольной фразы <New passphrase> закроется.
- Удаление
- 1. Убедитесь в том, что PGP диск не установлен.
- 2. Выберите команду <Remove passphrase> из меню <File>. Появится окошко, которое попросит вас ввести парольную фразу, которую необходимо отменить.
- 3. Введите пароль и нажмите на ОК.
- Примечание: программу PGP можно бесплатно скачать в Интернете по следующему адресу: http://www.pgpi.com