Программы шифрования

Компьютерная тайнопись

Программы

Криптография (а по-русски — тайнопись, или «тайное письмо») стара как мир. Известно, что еще Цезарь в своей переписке использовал шифр, который сегодня называется его именем. Продолжая разговор, начатый в предыдущих номерах нашего журнала («Информация, шифры, компьютеры» №6 2001, «Криптографические стандарты третьего тысячелетия» №7 2001), хотелось бы перевести его в практическую плоскость и рассказать о программах, которыми могут воспользоваться все желающие, чтобы защитить свою, как принято сейчас выражаться, приватность.

Кстати, один из проводившихся в Германии опросов показал, что 71% пользователей не шифруют свою электронную почту, считая это чересчур утомительным занятием, 25% шифруют только самые секретные с их точки зрения послания и 4% не дают никакого шанса любителям почитать чужие письма, шифруя все и вся.

Все же я призываю не слишком обольщаться недоступностью и закрытостью того, что вы зашифруете при помощи описанных далее программ. Тем не менее определенные трудности считывания вашей информации для чересчур любопытных коллег, начальников и прочих персонажей вы создадите, если воспользуетесь даже самыми простыми методами. При помощи несложных программ можно получить достаточно защищенную, на мой взгляд, систему. Как говорится, твори, выдумывай, пробуй. Кстати, специалисты утверждают, что расшифровать предварительно зашифрованный файл в «домашних условиях» весьма затруднительно, даже если применялись сравнительно простые средства шифрования.

Не нужно забывать, однако, что все нами творимое должно быть в рамках закона. Посмотрим для начала, что говорит российское законодательство о вопросах разработки и использования средств криптографии. Существует Указ Президента РФ от 3 апреля 1995 г. №334, который называется «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации». Он направлен на исполнение положений Закона Российской Федерации «О федеральных органах правительственной связи и информации». В нем ведется речь о государственных учреждениях, в том числе о банках, поэтому для нас представляет интерес всего один пункт. В нем говорится о запрещении «...в интересах информационной безопасности Российской Федерации и усиления борьбы с организованной преступностью» юридическим и физическим лицам заниматься «разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации, без лицензий, выданных Федеральным агентством правительственной связи и информации при Президенте Российской Федерации».

Кроме того, не будучи специалистом, я не могу оценивать криптоустойчивость и прочие специфические параметры программ. Мои оценки касаются только удобства использования программы и ее стабильности.

Раздумывая над тем, что же выбрать для данного обзора, я решил не останавливаться на таком монстре, как всем известная PGP. О ней написаны целые книги, которые все желающие могут изучить. Скажу только, что в настоящее время созданы русификаторы для некоторых версий этой программы (http://www.softlist.ru/cgi-bin/program.cgi?id=2450 — для 6.5.5i 1 и http://www.softlist.ru/cgi-bin/program.cgi?id=2390 — для 6.0.2i 1), которые могут облегчить жизнь пользователям, слабо владеющим английским языком.

Мы же рассмотрим более простые и менее известные широкому кругу пользователей программы, разработанные российскими и немецкими специалистами.

Программы эти создавались как небольшими фирмами, так и программистами-энтузиастами, поэтому их возможности находятся примерно на одном уровне. Также, на мой взгляд, достаточно интересно посмотреть что предлагают для защиты информации обычного пользователя немецкие коллеги, продукты которых не слишком известны в России. Между тем эти программы предлагают достаточно интересные и необычные решения, используя которые вы сможете снизить степень риска распространения вашей личной информации, например метод стеганографии, при котором информация маскируется в графическом файле.

Также я хочу обратить внимание читателей еще на один момент. Если вы решите воспользоваться какой-либо из этих программ, то помните, что у ваших адресатов должна быть установлена такая же или равноценная по возможностям программа, с помощью которой они смогут расшифровать полученное сообщение.

■ ■ ■ Игорь Строгов

TSCRYPT

Будьте осторожнее

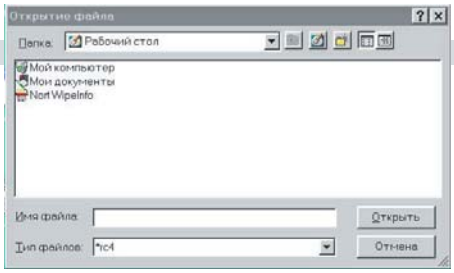
Хочу предупредить, что после скачивания из Интернета любую программу необходимо обязательно проверять антивирусом. Файл скачанной мною немецкой программы под названием TSCRYPT — tscpt32f.exe — оказался, согласно диагнозу Dr.Web, неизлечимым вирусом по имени BackDoor.Noknok.801. Ее создатель — некто Thomas Schoessow (http://www.tschoessow.de).

Определения

Криптография и криптоанализ

Для начала дадим некоторые определения, чтобы неискушенному читателю стало понятно, о чем пойдет речь. Итак, проблемами защиты информации путем ее преобразования занимается криптология (kryptos — тайный, logos — наука). Криптология имеет два направления — криптография и криптоанализ. Цели этих направлений прямо противоположны и напоминают об извечном соревновании снаряда и брони. Криптография занимается поиском и исследованием математических методов преобразования информации. Сфера интересов криптоанализа — исследование возможностей дешифрования информации без знания ключа. Ключ (далее в некоторых случаях он называется паролем) — это определенная информация (хранимая в строжайшем секрете), необходимая для беспрепятственного дешифрования текстов. Под шифрованием мы будем понимать преобразование исходного текста, который носит также название открытого текста, в шифрованный (или закрытый) текст. Соответственно, дешифрование — процесс, обратный шифрованию. На основе ключа шифрованный текст определенным образом преобразуется в исходный. Чтобы узнать, как это происходит, отсылаю читателей к вышеназванным статьям, а также к многочисленной специальной литературе, в изобилии имеющейся в книжных магазинах.

CryptoCommander 1.0



ПЛЮСЫ/МИНУСЫ

+ простота использования
+ малый размер
– программа не требует подтверждения пароля
– не реализована обработка нескольких файлов одновременно

Начать хотелось бы с бесплатной, очень простой программки, созданной Артемом Власевским, — CryptoCommander v. 1.0, которая предназначена для кодирования и декодирования файлов по алгоритму RC4.

После запуска программы появляется маленькое окошко. Далее порядок работы таков.

- Ввести код предстоящей операции, которую вы хотите осуществить: 0 — шифрование, 1 — дешифрование. (Если будет введено другое значение, то чуть позже программа выдаст сообщение об ошибке и закончит работу.)
- Далее следует выбрать один файл для обработки (обработка нескольких файлов пока не реализована). Если выбрано шифрование, файл может быть любым. Если дешифрование — выбирается файл с расширением RC4. Попытки обработать данной программой другие типы файлов могут привести к порче и потере информации.

После того как вы выбрали необходимую операцию, нужно ввести пароль для ее выполнения. Пароль не должен быть пустым. Будьте внимательны: программа не требует подтверждения пароля, что, на мой взгляд, относится к ее недостаткам.

Если все прошло успешно, то далее (в зависимости от произведенной операции):

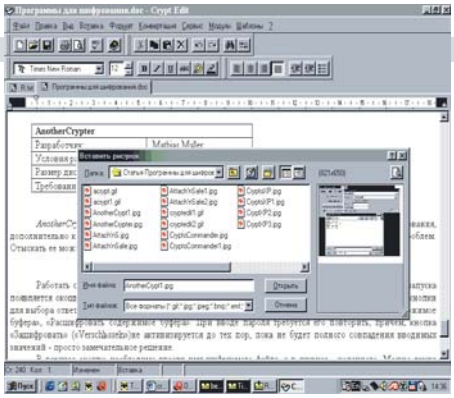
- в том же каталоге (где находится оригинал) создается файл имя_оригинала.rc4, причем имя оригинала берется вместе с расширением;
- в том же каталоге (где находится шифрованная копия) воссоздается оригинальный файл с именем <имя_шифрованной_копии>, но уже без расширения RC4.

Учтите, даже если веденный пароль неверен, процедура дешифрации состоится, только вместо читаемого документа вы получите абракадабру. Поэтому необходимо быть предельно внимательным и предварительно создавать резервную копию обрабатываемого файла, но сохранять ее в другой папке. Одноименные файлы заменяются программой без предупреждения.

CryptoCommander v. 1.0.

Разработчик ▸ Артем Власевский
Сайт разработчика ▸ http://www.megalink.ru/~devart/
Размер дистрибутива ▸ 674 Кбайт
Требования к системе ▸ Windows 95/98/NT
Условия распространения ▸ freeware

CryptEdit



ПЛЮСЫ/МИНУСЫ

+ стабильность работы и многофункциональность
+ установка уровня криптоустойчивости
+ собственный защищенный формат сохранения файлов
– справка по программе только на английском языке

Еще один российский продукт — текстовый редактор CryptEdit, о котором было уже упомянуто в июньском номере нашего журнала. Сама по себе эта программа просто великолепна и идеально подходит для повседневного использования. А встроенный модуль шифрования позволяет надежно скрывать любой документ от посторонних глаз. Можно создавать шаблоны документов, в том числе и зашифрованных. Также есть поиск и замена текста, просмотр буфера обмена, предварительный просмотр и другие интересные функции.

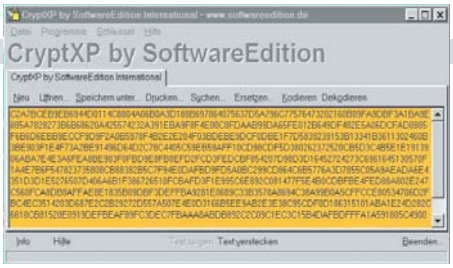
На уникальной для текстовых редакторов функции шифрования (в том числе и двоичных файлов) хотелось бы остановиться подробнее. Во-первых, созданный в CryptEdit документ может быть сохранен в особом формате — PTF (Protected Text Format). Защищенный паролем зашифрованный текст (используемые алгоритмы — RC4, MD5) прочесть невозможно. Единственный способ его посмотреть — открыть в CryptEdit, введя соответствующий пароль.

Во-вторых, имеющийся модуль позволяет шифровать любые другие файлы. Для удобства в установках параметров (меню «Правка -> Параметры») можно задать пароль по умолчанию, который будет применяться ко всем шифруемым текстам. Здесь же можно установить и уровень криптостойкости PTF-файлов — от высокого до низкого. Сам по себе текстовый редактор очень удобен (по своим возможностям скорее даже процессор), его можно смело рекомендовать всем (и не только шпионам), кому претит использование пиратских копий того же Microsoft Word. Единственное «но» — справка представлена только на английском языке.

CryptEdit

Разработчик ▸ Илья Ульянов, PolySoft
Сайт разработчика ▸ http://ps.yaroslavl.ru
Размер дистрибутива ▸ 1,1 Мбайт
Требования к системе ▸ Windows 95/98/NT
Условия распространения ▸ freeware

CryptXP



ПЛЮСЫ/МИНУСЫ

+ возможность неоднократного шифрования одного документа
+ шифрование документа из буфера обмена
+ возможность печатать в режиме «скрытый текст»
– малая величина обрабатываемых файлов
– немецкоязычный интерфейс

Не менее интересным представляется продукт германских программистов CryptXP, единственный недостаток которого в немецкоязычном интерфейсе. Тем не менее методом научного тыка освоить ее совсем нетрудно.

CryptXP — это текстовый редактор, имеющий целый ряд дополнительных (кроме шифрования) функций. К сожалению, он способен загружать и шифровать лишь небольшие по объему тексты — около 30 Кбайт.

Открыв окно программы с несколько непривычным желтым фоном, можно:

- начать вводить текст с помощью клавиатуры;
- скопировать его из буфера другой программы (например, Word);
- открыть нужный файл (только в текстовом формате) с помощью кнопки Offnen — «Открыть», которая из-за проблем со шрифтами может иметь вид «Цffnen».

При этом активизируются кнопки меню на нижней панели: Neu — «Создать документ», Speichern unter… — «Сохранить как…», Drucken — «Печать», Suchen — «Поиск», Ersetzen — «Заменить», Kodieren — «Зашифровать», Dekodieren — «Расшифровать». На верхней панели нас интересует только одна кнопка: Schlussel — «Ключ», которая (опять-таки из-за шрифтов) может выглядеть как «Schlьssel».

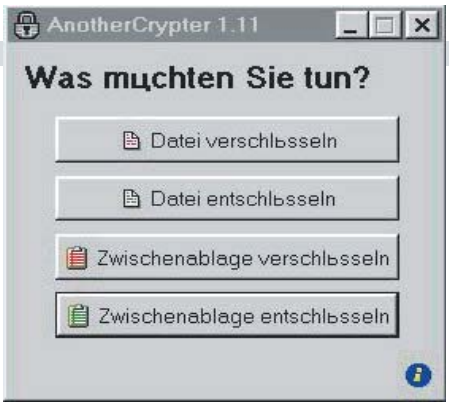
Перед тем как зашифровать текст, необходимо установить ключ кнопкой Schlussel (по умолчанию там установлено слово CryptXP). Ключ может представлять собой комбинацию знаков любой длины (в окно установки ключа я загрузил текст размером 33 Кбайт, и программа сработала). Для повышения стойкости закодированного текста его можно зашифровать повторно, нажав еще несколько раз кнопку Kodieren. Естественно, что и при раскодировании нужно будет нажать на кнопку «Декодировать» столько же раз.

Еще одна интересная функция CryptXP — возможность печатать в режиме скрытого текста. При этом можно спокойно печатать дальше. Вернуть текст на экран можно кнопкой Text zeigen.

CryptXP

Разработчик ▸ Software Edition International
Сайт разработчика ▸ www.softwareedition.de
Размер дистрибутива ▸ 720 Кбайт
Требования к системе ▸ Windows 95/98/NT
Условия распространения ▸ freeware

Another Crypter



ПЛЮСЫ/МИНУСЫ

+ возможность шифрования содержимого буфера обмена
+ достаточно большой объем шифруемого текста
+ простота работы
– интерфейс на немецком языке

AnotherCrypter использует метод блочного шифрования, дополнительно сжимая файл. Она очень проста и работает без каких-либо проблем. Работать с этой программой одно удовольствие, несмотря на импортный интерфейс.

После запуска появляется окошко, на котором написано: Was mochten Sie tun? — «Чего изволите?». Ниже располагаются кнопки для выбора ответа, то есть режима работы: «Зашифровать файл», «Расшифровать файл», «Зашифровать содержимое буфера», «Расшифровать содержимое буфера». При вводе пароля требуется его повторить, причем кнопка «Зашифровать» (Verschlusseln) не активизируется до тех пор, пока не будет полного совпадения вводимых значений.

В верхнее окошко необходимо ввести имя шифруемого файла, а в нижнее — конечного. Можно также нажать кнопку Quelldatai uberschreiben («Переписать исходный файл»), и тогда он будет заменен зашифрованным.

Очень интересная функция программы — шифрование содержимого буфера обмена. Зашифрованный текст можно сохранить в текстовом формате, и он будет представлять собой буквенно-цифровую комбинацию, не имеющую для постороннего взгляда никакого смысла. Размер помещаемого в буфер текста может быть достаточно большим, а расшифровать его можно, опять-таки, только используя буфер.

Рекомендовать эту программу специалистам, обеспокоенным сохранностью своей информаци, я бы не стал, однако для шифрования небольших служебных документов она вполне подходит.

AnotherCrypter

Разработчик ▸ Матиас Мюллер
Сайт разработчика ▸ http://www.sharefree2000.de/Utilities/Sicherheit/another_crypter.htm
Размер дистрибутива ▸ 385 Кбайт
Требования к системе ▸ Windows 95/98
Условия распространения ▸ freeware

Attach'n Safe

ПЛЮСЫ/МИНУСЫ

+ возможность скрывать информацию в других файлах
+ шифрование по алгоритму Blowfish
– малая величина обрабатываемых файлов
– неудобный порядок работы

Еще одна программа германского производства, но уже не бесплатная. Работает без оплаты в течение 30 дней, при этом никаких функциональных ограничений, характерных для демоверсий, не наблюдается.

Attach'n Safe позволяет не только шифровать файлы по алгоритму Blowfish (440-битный ключ), но и прятать их в безобидные картинки форматов JPG или BMP, которые внешне никак от этого не меняются. Например, текст данной статьи я спрятал в скриншоте программы.

Есть у программы и недостатки. Они, правда, обусловлены небольшим размером, занимаемым ею на диске. Во-первых, от вас потребуется знание немецкого языка (хотя бы со словарем). Во-вторых, невозможно развернуть довольно-таки пестрое окно в полноэкранный режим.

Обработка текста с помощью этой программы может показаться поначалу несколько замысловатой. Тем не менее, освоившись, можно работать легко и просто. Нужно только помнить, что ряд кнопок в нижней части окна служит для шифрования, а в правом нижнем углу — для дешифрования.

Итак, вначале необходимо напечатать в окне текст (или скопировать его из буфера). После этого кнопкой Keywahl («Выбор ключа») выбрать файл с ключом. Имя файла, в котором записан ключ, появляется над окном с текстом. В случае если ключ еще не задан, его следует создать. Для этого в окошке под кнопкой Key speichern unter... («Сохранить ключ как...») введите набор символов (не более 55) и сохраните файл, который получит расширение ANK.

Затем с помощью кнопки Objektwahl («Выбор объекта») выберите графический файл (автор рекомендует небольшой JPG- или BMP-рисунок), в котором мы и спрячем послание. Имя выбранного файла также отобразится в верхнем окне над текстом. Теперь все готово к тому, чтобы зашифровать и спрятать текст.

Для запуска процесса кодирования необходимо нажать кнопку Generieren («Запуск»). После завершения процесса программа сообщит об этом. Рисунок с вложением можно смело пересылать по электронной почте в виде прикрепленного файла. Кстати, регистрация программы предусматривает выдачу двух лицензий, что очень даже логично.

Для извлечения текста из картинки необходимо:

- выбрать кнопкой Lese-Key («Ключ для расшифровки») файл с ключом, совпадающим с тем, что применялся для зашифровки текста. Если файл еще не создан, то это можно сделать способом, аналогичным вышеописанному, с помощью кнопки Key speichern unter... («Сохранить ключ как...»);
- выбрать кнопкой Lese-Objekt («Считываемый объект») файл с вложением;
- нажать кнопку Objekt auslese («Считать объект»).

После этого в окне появится расшифрованный текст сообщения.

И еще: кнопка Einstellungen («Установки») позволяет задать путь к папкам, в которых размещены шифруемые файлы, файлы с ключами для зашифровки, файлы с рисунками, файлы с ключами для расшифровки, рисунки с запрятанными в них текстами.

Заметим, что с расшифровкой длинных текстов программа не справляется. Впрочем, это не умаляет заслуг автора, создавшего такой интересный и оригинальный продукт.

Attach'n Safe

Разработчик ▸ Инго Смекель
Сайт разработчика ▸ http://www.is-soft.de
Размер дистрибутива ▸ 473 Кбайт
Требования к системе ▸ Windows 95/98/2000/NT 4.0
Условия распространения ▸ shareware

Arcrypt 4.0

Чувство патриотизма требует рассказать еще о чем-нибудь родном, отечественном. Очень хорошо, на мой взгляд, задумана программа Arcrypt 4.0 — Advanced Russian Crypt (как говорится, аналогов за рубежом не имеет). По словам создателя, Arcrypt — это симметричная криптосистема, использующая алгоритм RCR2, который принадлежит к классу блочных шифров. В силу их очень высокой криптостойкости российский и американский стандарты шифрования основаны именно на этом классе шифров.

А дальше «бочка дегтя»: на сегодняшний день это очень сырая программа, которая никак не хотела запускаться в нормальном режиме, постоянно сворачиваясь в иконку в трее, и достать ее оттуда не было никакой возможности. Так что и оценить ее толком мне не удалось.

Тем не менее при соответствующей доработке, которой и занимается ее автор, у этой программы, на мой взгляд, есть все шансы завоевать большое количество поклонников.

Arcrypt 4.0

Разработчик ▸ С. М. Нечипоренко
Сайт разработчика ▸ http://arcrypt.narod.ru
Размер дистрибутива ▸ 695 Кбайт
Требования к системе ▸ Windows 95/98
Условия распространения ▸ freeware