4. Smith P. and Lennon M. LUC: A new public key system // Proceedings of the IFIP TC11 Ninth International Conference on Information Security. North-Holland. □ 1993. □ P.103–117.

5. Smith P. and Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms // In Advances in Cryptology Asiacrypt '94, Springer-Verlag. □ 1995. □ P. 357□364.

6. Bleichenbacher D., Bosma W., and Lenstra A. Some remarks on Lucas-based cryptosystems // In Advances in Cryptology Crypto'95, Springer-Verlag. □ 1995. □ P.386 □□396.

7. Laih C.-S., Tu F.-K., and Tai W.-C. On the security of the Lucas function // Information Processing Letters. □ 1995. □ №53. P. 243–247.

8. Маркушевич А.И. Возвратные последовательности. □ М.: Наука, 1975. □ 48с.

9. Воробьев Н.Н. Числа Фибоначчи. □ М.: Наука, 1992. □ 192 с.

10. Horadam A.F. A generalized Fibonacci Sequence // Amer. Math. Monthly. □ 1961. □ Vol.68. □ P. 455 □□459.

11. Лужецький В.А., Яремчук Ю.Є. Рекурентні V_k -послідовності // Вісник ВПІ. - 1999. - №6. - С. 53 - 59.

12. Лужецький В.А., Яремчук Ю.Є. Про один клас рекурентних послідовностей // Наукові праці Донецького державного технічного університету. Серія "Проблеми моделювання та автоматизації проектування динамічних систем". - 1999. - № 10. - С. 62 - 70.

Надійшла 31.01.2002

УДК 681.322

Гроздов Г.Г.

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ КРИПТОАЛГОРИТМОВ В ПРОГРАММНЫХ СРЕСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрены возможности наиболее популярных современных программных средств защиты информации по использованию криптоалгоритмов. Приведены причины ненадежности этих средств, даны рекомендации для оптимального использования их возможностей.

Основным показателем, характеризующим развитие современных информационных технологий, является ежегодный рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь.

Данная работа посвящена рассмотрению вопросов, связанных с методами криптографической защиты информации. Криптографические методы защиты информации являются неотъемлемой частью теории защиты информации. В современных вычислительных системах методы криптографии могут применяться для защиты информации, передаваемой по каналам связи, для аутентификации передаваемой информации или права на доступ к данным, для хранения данных на носителях в шифрованном виде и в других целях.

Выделим этапы развития криптографических методов защиты информации. Весь период с древних времен до 1949 года можно представить как период донаучной криптологии. Достижения этого периода были построены скорее на интуиции и вере, чем на научных доказательствах. Ситуация кардинально изменилась с выходом в 1949

году работы [1]. В этой работе были сформулированы такие понятия, как теоретическая и практическая стойкость криптосистем, совершенная секретность, были сформулированы требования к ключам в совершенно секретной системе. По причинам, описанным в предлагаемых материалах, публикация Шеннона не привела к бурному росту числа публикаций по этой проблематике. С публикацией в 1976 году работы [2] произошел настоящий прорыв в области криптографической защиты информации. В этой работе впервые было показано, что секретная связь возможна без передачи ключа между отправителем и получателем. Поэтому период с 1949 по 1976 год можно назвать периодом научной криптологии с секретными ключами, а третий период начался в 1976 году и продолжается по сей день. Это - период криптографии с открытыми ключами (об этапах развития криптографии с открытыми ключами подробно изложено в [3]).

Все существующие на сегодня методы криптографической защиты информации можно разделить на следующие группы методов: хеширования, кодирования, шифрования и комбинированные методы.

Перечислим основные требования к методам криптографической защиты информации:

- зашифрованный текст должен поддаваться чтению только при наличии ключа (информации, необходимой для беспрепятственного криптографического преобразования текстов);
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- не должно быть простых зависимостей между ключами, используемыми в методах;
- знание взломщиком алгоритма преобразования не должно повлиять на надежность защиты информации этим методом;
- незначительное изменение ключа преобразования или входных данных должно приводить к существенному изменению выходных данных;
- алгоритм должен по возможности допускать как аппаратную, так и программную реализацию;
- число операций, необходимых для получения входной информации методом полного перебора должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных вычислительных средств.

В отдельных случаях к алгоритмам криптографической защиты информации могут быть предъявлены дополнительные требования.

Автором работы проведен сравнительный анализ наиболее распространенных алгоритмов хеширования. Рассматривались такие алгоритмы, как MD2, MD4, MD5, SHA, ГОСТ Р34.11-94. В качестве критериев оценки алгоритмов хеширования использовались время вычисления хеш-функции и стойкость к криптоатакам. По мнению автора, наилучшим алгоритмом хеширования является ГОСТ Р34.11-94.

Все существующие алгоритмы шифрования могут быть классифицированы. В качестве параметров классификации алгоритмов выберем их следующие характеристики: размер обрабатываемых данных, способ работы с ключами. По размерам обрабатываемых данных существующие алгоритмы классифицированы как блочные и поточные; по способу работы с ключами преобразования - как симметричные и асимметричные.

Автором рассмотрены возможности наиболее популярных в настоящее время алгоритмов симметричного шифрования таких, как BLOWFISH, DES, FEAL, IDEA, RC2, RC5,Triple DES, ГОСТ 28147-89.

Сделан обзор математических алгоритмов, на которых построено большинство современных асимметричных криптосистем. Рассмотрены следующие алгоритмы: RSA, Месси-Омуры, Эль-Гамаля, Диффи-Хелмана, на основе задачи укладки ранца. Практически все рассмотренные асимметричные алгоритмы обладают большой

вычислительной сложностью, поэтому целесообразно использовать их для ключевого обмена. Шифрование передаваемой информации при этом лучше осуществлять с помощью симметричных методов.

В настоящее время алгоритмы криптографической защиты информации реализованы во многих программных средствах защиты информации. Автором работы были исследованы возможности наиболее популярных из свободно распространяемых программных средств криптографической защиты данных: PGP, BestCrypt и Cremlin.

Вкратце рассмотрим возможности и характерные особенности использования этих продуктов.

В настоящее время в глобальной сети Internet фактическим стандартом шифрования является программа PGP (Pretty Good Privacy), первая версия которой была разработана в 1991 году. Эта программа является сильным средством криптографической защиты. Сила PGP не в том, что никто не знает, как ее взломать, иначе как используя "лобовую атаку", а в превосходно продуманном и чрезвычайно мощном механизме обработки ключей, быстроте работы, удобстве для пользователей. Именно эти факторы (и бесплатное распространение) сделали PGP фактическим стандартом электронной переписки во всем мире.

PGP предоставляет пользователям широкие возможности использования методов криптографии с открытым ключом. В программе реализован механизм генерации пар ключей (особенности криптографических алгоритмов рассмотрены в [1,2,3]). В PGP могут быть использованы следующие методы шифрования: RSA и DSA (асимметричные алгоритмы), тройного преобразования DES, IDEA, CAST (симметричные алгоритмы). Реализованы следующие алгоритмы хеширования: MD5, RIPEMD-160, SHA-1.

На сегодняшний день существуют версии программы PGP, реализованные под такие операционные системы, как UNIX, Macintoch, VAX, Windows.

В настоящее время актуальна проблема защиты информации на жестких дисках персональных компьютеров.

Из свободно распространяемых программ в сети Интернет, программа BestCrypt является наилучшим средством для создания шифрованных логических дисков. Программа предлагает на выбор пользователя следующие алгоритмы шифрования: BlowFish, DES и

ГОСТ 28147-89. Для достижения максимального результата необходимо выбирать алгоритм ГОСТ 28147-89.

Существуют версии этой программы для следующих операционных систем: Dos, Windows 95/98, Windows NT. На шифрованных логических дисках целесообразно хранить не только всю секретную информацию, но и другие программы шифрования (например, PGP со всеми секретными ключами).

Кроме создания шифрованных дисков BestCrypt позволяет полностью на физическом уровне производить шифрование дискет, что очень удобно для передачи секретной информации.

Программа Kremlin является как бы логическим дополнением программы BestCrypt. Она позволяет шифровать файлы и электронную почту по многим алгоритмам, по выбору пользователя (IDEA, тройного преобразования DES, CAST и другим). Однако главным ее достоинством является возможность необратимого удаления всех временных файлов Интернет, логических журналов, а также всех файлов, которые укажет пользователь. Кроме того, программа способна осуществить невосстановимое обнуление информации на свободном месте жесткого диска и в файле виртуальной памяти Windows.

На сегодняшний день существуют апробированные и хорошо зарекомендовавшие себя методы криптографической защиты данных. Их стойкость к разного рода атакам доказана математически либо сводится к решению сложной математической задачи.

Казалось бы, применение подобных методов в информационных системах должно обеспечить конфиденциальность защищаемой информации.

Тем не менее, в средствах массовой информации периодически появляются сообщения о найденных "дырах" в системах защиты информации или о фактах "взлома" подобных систем.

Попытаемся объяснить данное противоречие.

Методы криптографической защиты являются лишь *малой частью* систем защиты информации. Использование в таких системах криптографически стойких методов вовсе не гарантирует того, что подобная система не может быть взломана нарушителем.

Для того, чтобы построить защищенную информационную систему разработчику необходимо быть подготовленным не хуже потенциального нарушителя. Разработчик должен знать об уязвимых местах информационных систем и причинах их возникновения. Другими словами, зная способы преодоления систем защиты информации, легче противодействовать подобным попыткам. Поэтому в настоящее время особую важность приобретает анализ проводимых атак на защищенные системы с целью определения причин их ненадежности.

Перечислим причины, в силу действия которых вычислительные системы, использующие методы криптографической защиты информации могут быть "взломаны":

- экспортные ограничения криптоалгоритмов;
- ошибки, заложенные при проектировании и реализации систем защиты информации;
- скомпрометированные пароль и закрытый ключ;
- не до конца удаленные файлы;
- вирусы и программы-закладки;
- файлы подкачки (виртуальная память);
- утечка данных в многопользовательских системах, нарушение режима физической безопасности;
- криптоанализ.

Самая простая атака может быть осуществлена в том случае, если пользователь оставит где-нибудь записанный пароль или ключ шифрования. Если злоумышленник получит их, а затем и файл с шифрованным сообщением, он сможет его прочесть. Поэтому особое внимание следует уделять защите паролей и ключей шифрования [6, 7, 8,9].

В современных операционных системах (Windows или MacOS) используется технология под названием "виртуальная память". Это удобно, поскольку с тех пор, как графический интерфейс стал нормой, программы занимают все больше и больше места, а пользователи предпочитают запускать 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 ключи, пароли, расшифрованные сообщения, из оперативной памяти, на жесткий диск.

К файлу подкачки может получить доступ каждый, кому физически доступен компьютер. Эту проблему можно решить, установив специально программное обеспечение, стирающее данные в файле подкачки (например, Kremlin 2.21).

Другим возможным средством является отключение механизма виртуальной памяти в

операционной системе. Это позволяет сделать и MS Windows, и MacOS. Отключение виртуальной памяти означает, что потребуется больше физически установленных микросхем оперативной памяти, для того чтобы в нее вошло все.

Современные программы криптографической защиты информации (BestCrypt, Cremlin, PGP) были созданы для использования на персональном компьютере, находящимся под физическим контролем лишь одного пользователя.

Эти программы не предназначены для защиты исходных открытых данных в многопользовательской системе. Они также не может предотвратить использования злоумышленниками различных способов доступа к закрытому ключу во время его использования. Нарушение режима физического доступа может позволить злоумышленнику захватить файлы с исходным текстом или отпечатанные сообщения. Серьезно настроенный противник может выполнить это различными способами.

Из изложенного выше можно сделать следующие выводы:

1. При планировании мероприятий по защите информации целесообразно применять комплексный подход:

– всю важную информацию (в том числе и программы для шифровки электронной почты типа PGP) храните на зашифрованном диске (разделе жесткого диска) созданного, например, с помощью программы BestCrypt;

– установите программу Kremlin 2.21 и настройте ее таким образом, чтобы при каждом выходе из Windows она обнуляла: свободное место на всех дисках, содержимое виртуальной памяти (файл подкачки), все файлы истории, лог файлы и т.д.;

– с помощью программы PGP шифруйте всю электронную корреспонденцию (рекомендуемые версии 2.6.3ia - для DOS и 6.0i для Windows);

– периодически производите полную замену всех паролей;

– для надежного шифрования файлов, находящихся на жестком диске используйте программы Kremlin и PGP.

2. При выборе пароля руководствуйтесь следующими рекомендациями:

– и используйте очевидные фразы, которые легко угадать, например, имена своих детей или супруги;

– используйте в пароле пробелы и комбинации цифр, символов 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 перебрать словарь известных цитат;

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

– используйте максимально длинные пароли - чем длиннее пароль, тем труднее его угадать.

3. Никогда не защищайте секретную информацию с помощью архиваторов и защиты предлагаемой MS Office.

4. Для большей надежности иногда имеет смысл использовать не одну, а несколько систем шифрования (например, шифровать E-Mail сначала с помощью NDEC, а затем с помощью PGP).

5. Всегда осуществляйте физический контроль за носителями информации.

Перейдем к рассмотрению проблем использования алгоритмов криптографической защиты информации. Наиболее важные из них перечислены ниже:

- применение методов сжатия и кодирования данных;
- преобразование сообщений большого объема;
- распределение сеансовых ключей;
- нахождение способов решения существующих NP-полных задач.

По мнению автора, при разработке новых криптосистем первоочередной задачей будет выбор NP-полной задачи.

Список литературы:

1. *К.Шеннон* "Теория связи в секретных системах". Москва: Иностранная Литература ,1963, с. 332 - 402.
2. *W. Diffie, M.E. Hellman* "New directions in cryptography". IEEE Trans.Informat.Theory, Vol. IT-22, pp, 644-654, Nov. 1976
3. *У.Диффи* "Первые десять лет криптографии с открытым ключом " В кн.: Тематический выпуск " Защита информации ". ТИИЭР , 1988 , № 5,с. 54-73.
4. *К.Ю. Гундарь., А.Ю. Гундарь, Д.А. Янишевский* "Защита информации в компьютерных системах". Киев: Корнейчук. 2000

5.Use of a taxonomy of security faults. COAST Laboratory, Purdue University, Technical report TR-96-051.

6.Abbott R.,Chin J. Security analysis and enhancements of computer operating system. NBSIR 76-1041, National Bureau of Standarts, ICST, April 1976.

7.Landwehr C, Bull A.,McDermott J A taxonometry of computer security flaws, with examples.Information Technology Division, code 5542, Naval research laboratory, Washington D.C., 20375-5337.

8.Leveson N., Turner C.S. An investigation of the Therac-25 accidents. UCI TR92-108, Inf. And Comp. Sci. Dept.,of Cal-Irvine, Irvine, CA.

Поступила 15.12.2001
После доработки 18.01.2002

УДК 621.391

Гороховский А.И.

ОБ ОДНОМ ПОДХОДЕ К КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Термин "компьютерная преступность" впервые появился в американских, а потом и в других зарубежных изданиях в начале 60-х годов. По мнению криминологов, ЭВМ в наше время многообещающее оружие проведения корыстных преступлений. Кроме преимуществ современных информационных технологий, компьютеризация несет в себе ряд отрицательных последствий, которые сегодня, к сожалению, практически остаются вне законодательного и правового поля Украины.

Перечень компьютерных преступлений в настоящее время стал значительно шире. Среди наиболее распространенных - воровство денег, материальных ценностей, машинной информации, машинного времени, несанкционированное использование системы, саботаж и вандализм. Воровство денег в электронных банковских системах взаиморасчетов составляет 45% всех преступлений, связанных с использованием ЭВМ. И только 10-15% компьютерных преступников становятся известными. Одной из причин этого становится то, что многие пострадавшие организации не сообщают о них из-за боязни потерять свою репутацию или совершения повторных преступлений.

Естественно, возникает потребность защитить информацию от несанкционированного доступа, кражи, уничтожения и других преступных действий. Отдельно встает вопрос о защите авторских прав на информационные продукты: программы, алгоритмы, данные, результаты.

Частные фирмы и государственные учреждения вынуждены приобретать все более совершенные и, следовательно, более дорогие аппаратные и программные средства защиты информации, затраты на эти цели за последних годы возросли на 66%, а доходы от их продажи в начале 90-х годов составили порядка 1 млрд. долларов [1].

Несмотря на столь бурное развитие методов защиты конфиденциальной информации в этом направлении научных исследований и практических разработок есть множество не решенных проблем.