ОБЗОР СОВРЕМЕННЫХ СИСТЕМ ШИФРОВАНИЯ

© Фёдоров М.Ю.[♣]
Филиал Московского государственного индустриального университета, г. Кинешма

В данной статье рассматривается современная проблематика применения систем шифрования. Производится сравнительный анализ основных криптографических методов защиты информации и предлагаются отдельные подходы к совершенствованию их использования.

Бурное развитие информационных технологий в XXI в. представляет обществу огромный спектр услуг и возможностей для коммуникации. Современный человек уже не может обойтись без персонального компьютера, в котором он хранит свои личные данные, формирует электронные отчеты, таблицы, базы данных, управляет финансовыми потоками своей фирмы и т.д. Существует следующая зависимость – чем секретнее информация, тем больше желающих ей обладать, поэтому каждый, будь то рядовой пользователь или крупная компания, стремятся защитить конфиденциальную информацию от несанкционированного доступа (НСД).

Современные информационные и коммуникационные технологии позволяют всем пользователям хранить и обмениваться огромными потоками информации, но при этом она становится более уязвимой по причине увеличения объема и расширения круга лиц, имеющих доступ к ней. Следовательно, все больше актуальной становится проблема защиты информации от НСД, над решением которой постоянно работают специалисты.

Криптографические методы защиты информации в основном классифицируют по количеству ключей в криптоалгоритмах [1]: бесключевые; алгоритмы с одним или с двумя ключами – открытым и секретным (рис. 1).

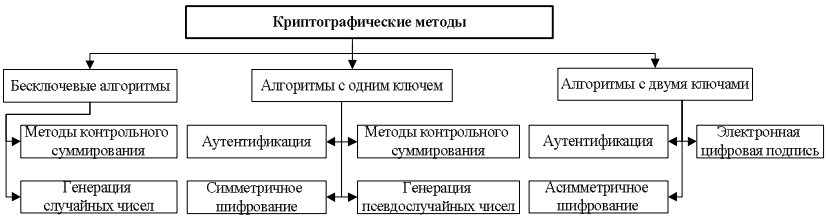

Рис. 1. Классификация криптографических методов

Рассмотрим некоторые криптографические методы (табл. 1) [2].

[♣] Старший лаборант, ассистент кафедры № 63 «Прикладная информатика в экономике», аспирант.

Таблица 1

Описание некоторых критпографических методов

Название метода	Описание метода
Аутентификация	Подтверждение подлинности. Позволяет проверить, является ли пользователь (или компьютер в сети) тем, за кого он себя выдает. Простейшей схемой аутентификации является текстовый ввод логина и пароля. Применение данной схемы является слабым методом защиты. Для повышения ее эффективности применяется специальные административно-технические меры, расширенной и многофакторной аутентификации, основанных на физических компонентах и биометрических данных.
Генераторы случайных (ГСЧ) и псевдослучайных чисел (ГПСЧ)	Алгоритм генерирующий последовательность случайных чисел, подчиняющихся определенному закону распределения. Довольно часто применяются в криптографии для генерации секретных ключей (которые должны быть совершенно случайными) к алгоритмам, в электронно-цифровой подписи, а также в большинстве схем аутентификации. Для получения абсолютно случайных чисел необходим качественный генератор, его можно реализовать на основе симметричного шифрования.
Электронная цифровая подпись (ЭЦП)	Реквизит электронного документа, позволяющий подтвердить целостность и авторство данных. Алгоритмы ЭЦП используют два вида ключей: секретный – для вычисления электронной подписи и открытый – для ее проверки. Российским стандартом ЭЦП является ГОСТ Р 34.10-2001 основанный на вычислениях точек эллиптической кривой. При использовании криптографически стойкого алгоритма ЭЦП, грамотном использовании и хранении секретного ключа, злоумышленник не в состоянии вычислить верную электронную подпись документа.
Методы криптографического контрольного суммирования	Используются в методах защиты, обработки и анализа информации, позволяют контролировать целостность и подлинность данных. К ним относятся хэширование (преобразование данных в последовательность бит фиксированной длины), вычисление имитовставок (применяется для защиты от фальсификации сообщения используя секретный ключ), коды аутентификации сообщений. Приведенные методы используются в ЭЦП для подписания не всех данных, а только их хеш; для подтверждения целостности данных в тех случаях, когда использование ЭЦП не приемлемо, а также в различных схемах аутентификации.

Большинство критпографических методов основано на различных видах шифрования информации.

Под шифрованием информации мы понимаем преобразование открытой информации в зашифрованную путем замены и перемещения бит данных (чаще всего такая информация называется шифртекстом). Для корректной расшифровки необходима функция расшифровывания, которую используют при шифровании, а также секретный ключ. Ключ мы рассматриваем как определенное секретное состояние показателей алгоритмов шифровки и расшифровки. Для затруднения криптоанализа перед шифрованием информацию необходимо подвергнуть статистическому кодированию (архивации

и сжатию). После выполнения процесса архивации, информация будет занимать меньший объем, уменьшится избыточность, а энтропия возрастет.

Алгоритмы шифрования делят на две категории (рис. 1):

1. алгоритмы симметричного шифрования (DES, ГОСТ 28147-89, IDEA, AES, Twofish, Blowfish, Lucifer, SEED, CAST, XTEA и др.);
2. алгоритмы асимметричного шифрования (RSA, ГОСТ Р 34.10-2001, Elgamal).

Алгоритмы симметричного шифрования основаны на том, что участники обмена сообщениями для шифрования и дешифрования используют один и тот же ключ, который должен храниться в секрете обеими сторонами и передаваться по защищенным каналам связи. Процесс обмена сообщениями между абонентами мы сформулируем следующим образом (рис. 2).

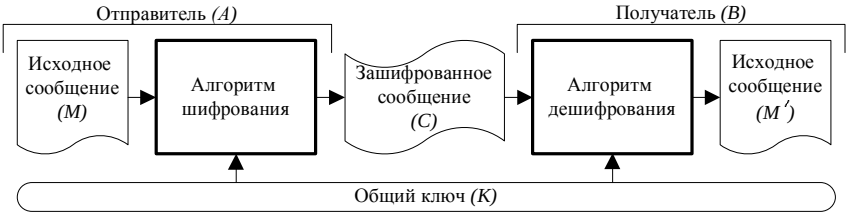

Рис. 2. Схема симметричного шифрования в общем виде

Перед началом обмена сообщениями участники должны позаботиться о наличии у них идентичного секретного ключа (K). Затем отправитель (A) зашифровывает сообщение (M) своим секретным ключом и отправляет сообщение (C) получателю (B). Адресат расшифровывает сообщение аналогичным ключом и получает исходное сообщение (M').

Для того чтобы в результате дешифрования было получено сообщение идентичное исходному ($M = M'$), необходимо использовать одну и ту же функцию (алгоритм) шифрования-дешифрования, а также общий ключ к алгоритмам. При отсутствии одинакового ключа невозможно дешифровать сообщение за достаточно короткий период времени даже при современных вычислительных мощностях.

Симметричное шифрование делят на два вида [1, 2]:

1. блочное шифрование – информация разбивается на блоки фиксированной длины и дальнейшем они шифруются методом перестановок (простая и двойная перестановки, одиночная по ключу и перестановка «магический квадрат»), и замен;
2. потоковое шифрование – информация шифруется посимвольно (побитно) с помощью гаммирования. Данный вид шифрования можно рассматривать как частный случай блочного шифрования, т.к. шифруются блоки единичной длины.

Проанализировав современные алгоритмы шифрования, мы видим, что они работают по весьма схожему принципу – сообщение преобразуется при помощи ключа шифрования в течение нескольких итераций (раундов). Расмотрим классификацию алгоритмов по их структуре (табл. 2) [3, 4].

Таблица 2

Классификация алгоритмов по структуре

Название алгоритма	Характеристика алгоритма
Алгоритмы симметричного шифрования на основе сети Фейстеля	Обрабатываемый блок данных разбивается на несколько субблоков (обычно на два), один из которых обрабатывается функцией и в дальнейшем накладывается на необработанный субблок. После чего субблоки меняются местами, при переходе от одного блока к другому меняется ключ, его выбор зависит от конкретного алгоритма шифрования. Операция выполняется до тех пор, пока не будут обработаны все данные. К достоинствам можно отнести простоту аппаратной реализации и хорошую изученность алгоритма, к недостаткам, то, что за один раунд шифруется только половина входного блока.
Алгоритмы симметричного шифрования на основе подстановочно-перестановочных сетей (SP-сеть)	Алгоритмы данной сети обрабатывают данные путем замен (строится таблица замен, на основе которой в дальнейшем обрабатываются данные) и перестановок зависящих от ключа шифрования. Основное отличие от сети Фейстеля, в том, что за один раунд обрабатывается шифруемый блок данных целиком. Сеть представляет собой «сэндвич» с последовательно чередующимися P и S блоками, в качестве которых выступают различные математические функции. Данный вид сетей используется реже, чем сети Фейстеля.
Алгоритмы симметричного шифрования со структурой «квадрат»	Шифруемый данные представляются как двумерный массив, и шифрование производится над отдельными битами, столбцами или строками.
Алгоритмы симметричного шифрования с нестандартной структурой	Уникальные алгоритмы, так как их невозможно причислить ни к одному из перечисленных выше типов, что дает дополнительные просторы для изобретательности.

Алгоритмы асимметричного шифрования (системы ЭЦП) основаны на том, что участники обмена сообщениями используют два ключа – открытый и секретный. Открытый ключ используется для шифрования сообщения (расшифровать сообщение открытым ключом не удастся), а закрытый только для дешифрования. Процесс обмена сообщениями между абонентами мы формулируем следующим образом (рис. 3).

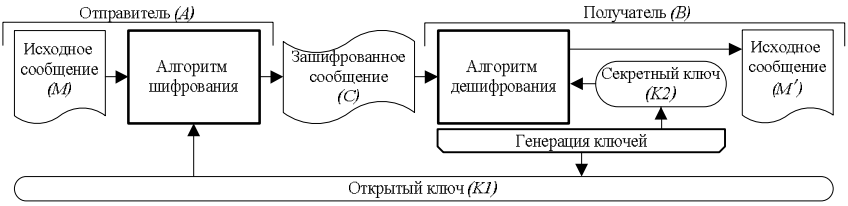

Рис. 3. Схема асимметричного шифрования в общем виде

Один из участников – получатель (*B*) генерирует оба ключа (*K*1 и *K*2), один из которых (*K*1) он свободно распространяет по каналам связи всем желающим участвовать в обмене информационными данными, а другой (*K*2) хранит в тайне. Отправитель (*A*), шифрует сообщение (*M*) открытым ключом (*K*1) и отправляет полученные данные (*C*) получателю, а он в свою очередь дешифрует полученное сообщение своим секретным ключом (*K*2) и получает исходное сообщение (*M'*).

Криптосистема с открытым ключом использует определенные необратимые математические функции. Сложность вычислений таких функций не линейна, она возрастает быстрее, чем длина ключа. Данный вид шифрования чаще всего используется для шифрования небольших блоков данных, а также в ЭЦП и при шифровании секретного ключа от симметричного алгоритма шифрования.

У современных систем шифрования есть свои достоинства и недостатки. Например, у симметричных алгоритмов скорость работы минимум в три раза выше (в зависимости от длины ключа), при одинаковых характеристиках криптостойкости, они хорошо изучены, сравнительно просты в реализации и не требовательны к вычислительным ресурсам, в сравнении с асимметричными алгоритмами. Однако в криптосистемах с открытым ключом не нужно беспокоиться о надежном секретном хранении ключа у собеседника, а также часто менять его, так как существует открытый ключ, которым может воспользоваться любой участник переписки.

В настоящее время мы видим, что информатизация и автоматизация всех сфер человеческой деятельности приводит к росту угроз несанкционированного доступа к информации, следовательно, существует необходимость постоянной поддержки, обновления и совершенствования методов ее защиты. Основная проблема для фирм и конечных пользователей заключается в выборе из значительного количества программно-аппаратных систем шифрования тех вариантов информационных продуктов, которые в большей степени отвечали бы специфике (алгоритмы, скорость работы, криптостойкость и т.п.) и поставленным задачам защиты данных. По оценкам криптоаналитиков надежность используемых алгоритмов и программных средств гарантирует защиту информации. Мы считаем, что современные системы шифрования должны применяться повсеместно и интегрироваться в работу пользователей, а не быть отдельным комплексом, запускаемым только по требованию.

Список литературы:

1. Ященко В.В. Введение в криптографию. – СПб.: Питер, 2001.

2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009.

3. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. – М.: Горячая линия – Телеком, 2002.

4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.

МЕТОДЫ СЖАТИЯ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ОРТОГОНАЛЬНЫХ ВЕЙВЛЕТ ПРЕОБРАЗОВАНИЙ

© Филиппов Т.К.
ОАО «Сургутнефтегаз», г. Сургут

С прогрессом средств вычислительной техники и широким распространением мультимедиа контента всё большая часть информации в вычислительных системах представляется в виде цифровых изображений. Поэтому проблема улучшения алгоритмов сжатия изображений достаточно актуальна. Сжатие изображений важно как для увеличения скорости передачи по сети, так и для эффективного хранения. С другой стороны, широкое использование цифровых изображений приводит к необходимости разработки средств их идентификации и защиты авторских прав. На сегодняшний день существует большое число методов цифрового маркирования изображений, решающих эту задачу. Однако, большинство методов не совместимы с методами сжатия изображений. Решение проблемы сжатия изображения использовало достижения и стимулировало развитие многих областей техники и науки.

Для уменьшения объема графических данных используют большое число алгоритмов сжатия, к которым предъявляется много жёстких требований, как по объёму сжатого файла, качеству восстановленного изображения, так и по ресурсоёмкости самого алгоритма сжатия. К тому же из-за широкого развития сетевых технологий важно, чтобы методы сжатия позволяли постепенно «прорисовывать» изображение в процессе закачки из сети.

Выявление структуры данных – ключевой аспект эффективного преобразования данных. Среди существующих алгоритмов сжатия можно выделить спектральные методы сжатия, фрактальные методы сжатия и методы сжатия на основе аппроксимаций.

Помимо JPEG, MPEG к спектральным методам сжатия относятся методы, основанные на вейвлет преобразовании. Данные вейвлет преобразования могут быть представлены в виде поддерева, которое может быть эффективно закодировано.

Возможен также смешанный фрактально-вейвлетовый метод кодирования изображения, в котором вейвлет сжатию подвергаются однородные объекты, выделяемые на исходном изображении.