**BC/NW 2015 № 2 (27):13.5**

**СОВРЕМЕННЫЕ КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

Мизинов С.В., Русинов С.Г., Добряков П.С., Нефедов Е.Ю.

С развитием общества и появлением письменности все оживленнее велась переписка, и все больше возникала необходимость в средствах ее засекречивания. Соответственно, возникали все более совершенные и хитроумные шифры. Сначала при заинтересованных лицах появились шифровальщики, потом группы из нескольких шифровальщиков, а затем и целые шифровальные отделы. Когда объемы подлежащей засекречиванию информации стали критическими, в помощь людям были созданы механические устройства для шифрования. Надо сказать, что основными потребителями криптографических услуг были дипломатические и шпионские миссии, тайные канцелярии правителей и штабы войсковых соединений. Для начального этапа развития криптографии характерно следующее:

- защите подвергались исключительно текстовые сообщения, написанные на естественных языках, так как других типов дискретно представленных данных просто не существовало;

- шифрование сначала осуществлялось вручную, позднее были изобретены сравнительно несложные механические приспособления, поэтому использовавшиеся тогда шифры были достаточно простыми и несложными;

- криптография и криптоанализ были скорее искусством, чем наукой, научный подход к построению шифров и их раскрытию отсутствовал;

- криптография использовалась в очень узких сферах: для обслуживания высших правящих слоев и военной верхушки государств;

- основной задачей криптографии была защита передаваемых сообщений от несанкционированного доступа к ним, поскольку шифровались исключительно текстовые сообщения, никаких дополнительных методов защиты от навязывания ложных данных не применялось – вероятность получить нечто осмысленное после дешифрования искаженного зашифрованного текста была ничтожно мала в силу огромной избыточности, характерной для естественных языков.

Появление в середине прошлого столетия первых электронно-вычислительных машин кардинально изменило ситуацию. С проникновением компьютеров в различные сферы жизни возникла принципиально новая отрасль хозяйства – информационная индустрия. Объем циркулирующей в обществе информации с тех пор стабильно возрастает по экспоненциальному закону. Фактически, на пороге нового тысячелетия человечество создало информационную цивилизацию, в которой от успешной работы средств обработки информации зависит само благополучие и даже выживание человечества в его нынешнем качестве. Произошедшие за этот период изменения можно охарактеризовать следующим образом:

- объемы обрабатываемой информации возросли за полвека на несколько порядков;

- сложилось такое положение вещей, что доступ к определенным данным позволяет контролировать значительные материальные и финансовые ценности, информация приобрела стоимость, которую во многих случаях даже можно подсчитать;

- характер обрабатываемых данных стал чрезвычайно многообразным и более не сводится к исключительно текстовым данным;

- информация полностью «обезличилась», то есть особенности ее материального представления потеряли свое значение (достаточно сравнить письмо прошлого века и современное послание по электронной почте);

- характер информационных взаимодействий чрезвычайно усложнился, и наряду с классической задачей защиты передаваемых текстовых сообщений от несанкционированного доступа, возникли новые задачи сферы защиты информации, ранее стоявшие и решавшиеся в рамках используемых «бумажных» технологий, например подпись под электронным документом и вручение электронного документа «под расписку»;

- субъектами информационных процессов теперь являются не только люди, но и созданные ими автоматические системы, действующие по заложенной в них программе;

- вычислительные мощности современных компьютеров подняли на совершенно новый уровень как возможности по реализации шифров, ранее немыслимых из-за своей высокой сложности, так и возможности аналитиков по их взлому.

Перечисленные выше изменения привели к тому, что в результате широкого распространения компьютеров в деловой сфере практическая криптография сделала в своем развитии огромный скачок, причем сразу по нескольким направлениям:

- во-первых, были разработаны стойкие блочные шифры с секретным ключом, предназначенные для решения классической задачи – обеспечения секретности и целостности передаваемых или хранимых данных. Они до сих пор остаются основой криптографии, наиболее часто используемыми средствами криптографической защиты;

- во-вторых, были созданы методы решения новых, нетрадиционных задач сферы защиты информации, наиболее известными из которых являются задача подписи цифрового документа и открытого распределения ключей.

Таким образом, термин «криптография» далеко ушел от своего первоначального значения – «тайнопись», «тайное письмо». Сегодня эта дисциплина объединяет методы защиты информационных взаимодействий различного характера, опирающиеся на преобразование данных по секретным алгоритмам, включая алгоритмы, использующие секретные параметры. Далее будет приведена классификация наиболее известных и широко используемых сегодня криптосистем и криптографических методов. Но сначала приведем основные понятия и определения криптографии:

Алфавит - конечное множество используемых для кодирования информации знаков. Примерами алфавитов, использующихся в современных информационных системах могут служить: Z2 (бинарный алфавит) = {0,1}, Z8 (восьмеричный алфавит) = {0,1,2,…,7}, Z16 (шестнадцатеричный алфавит) = {0,1,2,…,E,F}, Z256 - все символы стандартного кода ASCII.

Текст - упорядоченный набор из элементов алфавита.

Шифрование - преобразовательный процесс, при котором исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Все криптографические методы можно разделить по пяти основным параметрам:

1. Симметричные и асимметричные. Симметричными называются криптосистемы, которые используют один и тот же ключ как для шифрования информации, так и для ее дешифрования. Асимметричными называются криптосистемы, которые используют для шифрования и дешифрования разные ключи - открытый и закрытый, первый для шифрования, второй - соответственно для дешифрования.

2. Потоковые и блочные. Потоковыми называются криптосистемы, которые обрабатывают информацию по одному биту, каждый бит отдельно от других. Блочными называются криптосистемы, которые перед обработкой информации разбивают ее на блоки определенной длины и только потом производят какие-либо операции уже над блоками.

3. С бесконечным ключом, с конечным ключом, с ключом, полученным с помощью генератора псевдослучайных чисел (независимо от его конечности/бесконечности). Криптосистемами с бесконечным ключом называются те, которые используют для шифрования ключ бесконечной длины – например числа Пи, е или другие периодические и непериодические дроби. Криптосистемами с конечным ключом называются те, которые используют для шифрования ключ определенной длины. Криптосистемами с ключом, полученным с помощью генератора псевдослучайных чисел, называются те, что используют для шифрования ключ, который получен путем последовательной записи чисел, выданных генератором псевдослучайных чисел.

4. Моноалфавитные и многоалфавитные. Моноалфавитными называются криптосистемы, в которых в соответствие с методом шифрования исходный текст заменяется на другой текст, но все символы текста, как до шифрования, так и после, являются символами одного алфавита. Многоалфавитными называются криптосистемы, в которых каждый символ шифруемого текста (все они являются символами одного алфавита) заменяется в соответствие с методом шифрования на некоторый символ из совершенно другого алфавита.

5. С шифрованием перестановкой и с шифрованием заменой. Криптосистемами с шифрованием перестановкой называются те, в которых шифрование текста происходит путем перестановки каким-либо образом символов исходного текста (число символов и сами символы остаются теми же, изменяются лишь их позиции в тексте). Криптосистемами с шифрованием заменой называются те, в которых шифрование происходит путем замены символов исходного текста на другие символы в соответствие с методом шифрования.

Следует заметить, что большинство современных криптосистем являются составными, то есть сочетают в себе различные способы шифрования - и замену, и перестановку, применяя для этого различные комбинации различных математических (и не только) функций.

Вполне очевидно, что с момента появления криптографических методов и их внедрения на практике, появилась необходимость оценивать эффективность их работы. На настоящий день к современным криптосистемам предъявляются следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться дешифрованию только при наличии ключа;

- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

- знание алгоритма шифрования не должно влиять на надежность защиты;

- даже незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения;

- структурные элементы алгоритма шифрования должны быть неизменными;

- дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

- длина шифрованного текста должна быть равной длине исходного текста;

- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

- любой ключ из множества возможных должен обеспечивать надежную защиту информации;

- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом незначительное изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

В настоящее время оценка уже используемых криптографических методов стала особенно актуальной. Задача определения эффективности средств защиты зачастую более трудоемкая, чем их разработка, требует наличия специальных знаний и, как правило, более высокой квалификации, чем задача разработки. Эти обстоятельства приводят к тому, что на рынке появляется множество средств криптографической защиты информации, про которые никто не может сказать ничего определенного. При этом разработчики держат криптографический метод (как показывает практика, часто нестойкий) в секрете. Однако задача точного определения данного криптографического метода не может быть гарантированно однозначной хотя бы потому, что он известен только разработчикам. Кроме того, если нарушитель нашел способ преодоления защиты, то не в его интересах об этом заявлять. Поэтому обществу должно быть выгодно открытое обсуждение систем защиты информации массового применения, а сокрытие разработчиками криптографического метода должно быть недопустимым.

**Литература**

1. Сюэдзя Лай и Джеймс Месси. Марковские шифры и дифференциальный криптоанализ , EuroCrypt 1991. - 42 с

2. Менезес А., Ванстон С. Практическое применение дискретной математики в криптографии, EuroCrypt 1990. - 287 с

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты, М. Триумф 2002. - 816 с.