Н.В.ПАЦЕЙ, П.П.УРБАНОВИЧ
Белорусский государственный технологический университет
(г.Минск)

НЕКОТОРЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ ТИПОВЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

1. Для защиты информации от утечки по каналам передачи могут использоваться различные способы: подавление побочных электромагнитных излучений и наводок экранами, фильтрами, маскирующими шумами; шифрование сообщений; физическое ограничение доступа и другие средства. Наиболее радикальным способом представляется шифрование. На практике применяются два классических и наиболее распространенных типа криптосистем: симметричные (закрытые, с одним ключом) и асимметричные (открытые, с двумя ключами).

2. Практически все современные криптосистемы построены по принципу Кирхгоффа: секретность сообщения определяется секретностью ключа. Самым известным зарубежным аналогом схемы с симметричным ключом, построенным по этому принципу, может служить DES-алгоритм (Data Encryption Standard), способный функционировать в режимах электронной кодовой книги (ECB), обратной связи по шифротексту (CFB), сцепления блоков шифра (CBC) и обратной связи по выходу (OFB). Слабыми местами в нем являются выбранная длина блока в 64 бита и ключ в 54 бита, а также относительно простой алгоритм назначения ключей и сложность начальных перестановок [1]. Используя дифференциальный или линейный криптоанализ, можно вскрыть 16-кратный DES-алгоритм [2]. Число циклов шифрования управляет параметром диффузии, обусловленной операциями перестановок, поэтому желательно увеличить число циклов до 32 [2]. Кроме того, DES может быть раскрыт прямым перебором ключей в объеме 2^{56} с помощью нескольких тысяч микросхем, одна из которых способна проверить $5*10^7$ ключей (что возможно с учетом постоянного прогресса в микроэлектронике, но пока является дорогостоящим) за 7 часов [3]. Пространство ключей может быть сокращено в силу свойства дополнительности DES-алгоритма (т.е. инвариантности по отношению к результату операции дополнения исходного текста, ключа или шифрованного текста). Другой способ раскрытия алгоритма - представление его в виде просматриваемой таблицы. Получаемые из исходного все шифрованные тексты накапливаются (объём памяти равен $56*2^{56}=4*10^{18}$ бит) и сортируются, используя весь объём ключевого пространства [2]. В силу всего вышесказанного DES-алгоритм нецелесообразно применять при передаче конфиденциальной информации.

3. Свое дальнейшее развитие DES получил в государственном стандарте Союза ССР (ГОСТ 28147-89), в котором предусматривалось увеличение длины ключа до 256 бит (соответственно увеличился объём ключевого пространства) и были предложены реализации

произвольных перестановок в блоках [4]. Несмотря на ряд усовершенствований, государственный стандарт не лишен недостатков. Например, режим простой замены отличается низкой криптостойкостью: одинаковые блоки исходного текста дают одинаковые блоки шифротекста. Возникают вопросы при длине массива информации (в байтах) не кратной 8: чем дополнить блок до 8 байтов? И, кроме того, необходимо хранить количество информационных байтов последнего блока исходного текста [5,6].

4. Для шифрования массивов информации на основе криптографических систем асимметричного типа используют методы дискретного типизирования, вероятностного шифрования, выполнение математических операций над эллиптическими кривыми. До настоящего времени еще ни одна из систем с открытым ключом, кроме RSA (Rivest-Shamir-Adleman), не была столь устойчива к многочисленным попыткам нарушения защиты. Криптостойкость системы основана на допущении о вычислительной неосуществимости разложения сверхбольших чисел на сомножители. Работа в этом направлении ведется интенсивно. Уже достигнуты значительные результаты в совершенствовании методов и техники разложения больших чисел [7]. Это создает большую угрозу применению криптографической системы RSA.

5. В последнее время предлагается применять в алгоритме числа в 250 и даже в 300 десятичных разрядов, при этом число операций в наилучших из известных алгоритмов факторизации больших чисел становится $1{,}2*10^{23}...2{,}7*10^{34}$, что находится за пределами современных информационных технологий [2]. Наиболее быстродействующие реализации RSA имеют скорость работы несколько тысяч бит в секунду (приблизительно в сотни раз медленнее реализаций DES), поэтому они практически не применяется в каналах с высокой скоростью передачи и для шифрования больших объемов информации [7].

6. Все криптоалгориты используют блочный, сверточный или комбинацию этих методов шифрования. Основной недостаток этих методов - размножение ошибок. Ошибочный бит при передаче вызовет блок ошибок в расшифрованном тексте. Требование зависимости текста шифровки от предыдущего участка повышает криптографическую стойкость, но противоречит требованию целостности информации.

7. Размножение ошибок отсутствует в потоковом методе шифрования. Он отличается простотой реализации и высокой скорость шифрования. Основной его недостаток - необходимость передачи синхронизирующей информации перед сообщением и применение дополнительного, случайно выбираемого ключа, который используется для модификации основного ключа. Для потокового шифрования нет типовых алгоритмов. Так HS3447 Cipher 1, B-Crypt с алгоритмом B152, STEN, Mesa 432, Secure X.25 - системы с засекреченными, оригинальными потоковыми алгоритмами. При использовании смешанных систем потокового и блочного шифрования получается шифр, не размножающий ошибки и в то же время усложняющий возможность определения какому биту открытого текста соответствует бит текста шифровки. Все же сложность системы декодирования и увеличение объема шифрованного сообщения являются существенными недостатками такого рода шифров.

8. Высокие требования, предъявляемые к целостности информации, параметрам быстродействия и криптостойкости, ограничивают применение упомянутых выше методов

шифрования и криптографических алгоритмов. В дальнейшем, видимо, будут сделаны попытки усовершенствовать существующие, а также разработать новые алгоритмы, обеспечивающие высокий уровень целостности, доступности и секретности информации. Новые поколения криптографических методов защиты компьютерных линий связи, скорее всего, будут связаны с применением концепции взаимодополнения алгоритмов достоверности и защиты информации.

Литература:

1. Pierce C.C., Crypto-privacy,1988.
2. Sead Muftic, Security mechanisms for computer networks, 1993.
3. Sinkov, Abraham., Cryptanalysis: A Mathematical Approach,1980.
4. ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая".
5. Винокуров А., ГОСТ не прост, а ... очень прост. //Монитор ,1995, N 1.
6. Винокуров А., Еще раз про ГОСТ //Монитор, 1995, N 5.
7. Building in Big Brother. The Cryptographic Policy Debate., Spriger-Verlag,1995.

В.В.ЛЕПИН

Институт математики АН Беларуси

(г.Минск)

КРИПТОАНАЛИЗ СИСТЕМЫ RSA

Криптосистема RSA, названная (по первым буквам фамилий) в честь Р.Риверса, А.Шамира и Л.Адлемана, которые изобрели ее в 1977 г., обладает следующими преимуществами систем с односторонней функцией:

1) возможность обмена шифрованными сообщениями по открытым каналам связи и открытость ключей;

2) задача вскрытия шифра включает в себя трудоемкую задачу факторизации большого числа;

3) позволяет решать новые криптографические задачи, отличные от шифрования (цифровая подпись и др.).

Способность криптосистемы успешно противостоять атакам со стороны квалифицированных криптоаналитиков называется криптостойкостью. Достаточно ли криптостойка система, которая основывается на трудоемкости факторизации больших чисел (ключей), обеспечивающих ее секретность? Какой размер ключа достаточен для обеспечения требуемой секретности?

В 1976 известный специалист в комбинаторной теории чисел Р.Гью писал, что он сильно удивится, если кто либо сможет факторизовать любые 80-значные числа в настоящем веке. По оценке Р.Ривеста, сделанной им в 1977 г., 125-разрядный ключ, равный произведению двух простых чисел по 63 разряда каждое, можно было считать вполне надежным. Время,