электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 10, октябрь 2015

УДК 004.056.55

Применимость алгоритмов симметричного шифрования в информационных системах

***Дмитроца С.М.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Компьютерные системы и сети»

Научный руководитель: Гуренко В.В., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Компьютерные системы и сети»
wgurenko@bmstu.ru

Введение

В современных информационных системах особое внимание уделяется конфиденциальности данных, т.е. противостоянию несанкционированному доступу, искажению или разрушению конфиденциальной информации. С этой целью широко применяются криптографические методы защиты данных.

Шифрование предусматривает обратимое преобразование незащищенной (открытой) информации в зашифрованную (закрытую) форму – шифротекст [1], в которой она не представлена полностью доступной для неавторизованного пользователя. При шифровании используются ключи, наличие которых означает возможность зашифрования и/или расшифрования данных.

В данной работе рассмотрены виды современных криптосистем. Путём сравнительного анализа выявлены их преимущества и недостатки по выбранным критериям, сделаны выводы относительно их применимости в современных информационных системах.

1. Типы криптосистем

Современные криптосистемы можно однозначно разделить по способу использования ключей на криптосистемы с секретным ключом (симметричные) и с открытым ключом (асимметричные). Симметричной является система, в которой для зашифрования и расшифрования используется один и тот же ключ. Схема передачи сообщения с применением алгоритма симметричного шифрования представлена на рис. 1. К симметричным криптосистемам относятся DES [2], AES [3], ГОСТ 28147-89 [4] и т.д. Относительно но-

вым направлением в криптографии стало изобретение асимметричных криптосистем с открытым ключом, таких как RSA, DSA или Эль-Гамаль [5, 6].

В асимметричных криптосистемах для зашифрования и расшифрования применяют различные, практически не выводимые друг из друга ключи, один из которых (ключ расшифрования) делается секретным, а другой (ключ зашифрования) – открытым. Этим достигается возможность передавать секретные сообщения по незащищенному каналу без предварительной передачи секретного ключа (рис. 2).

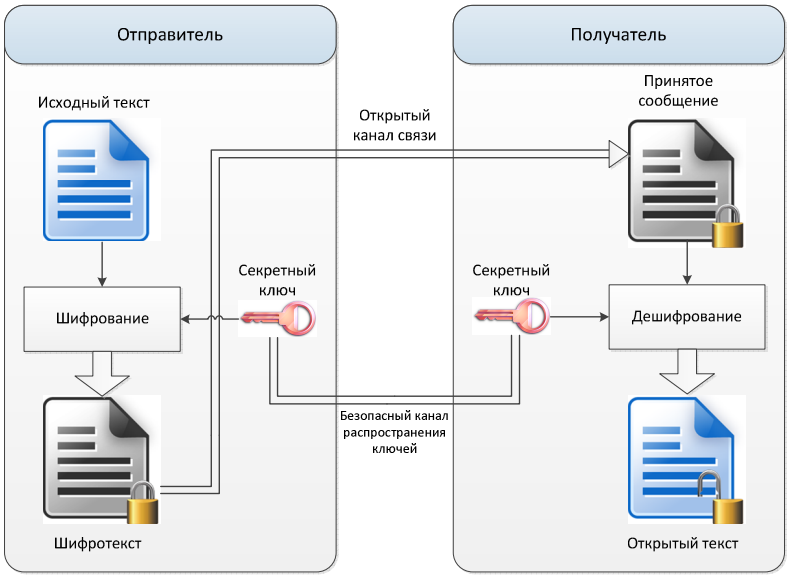

Рис. 1. Схема симметричного шифрования

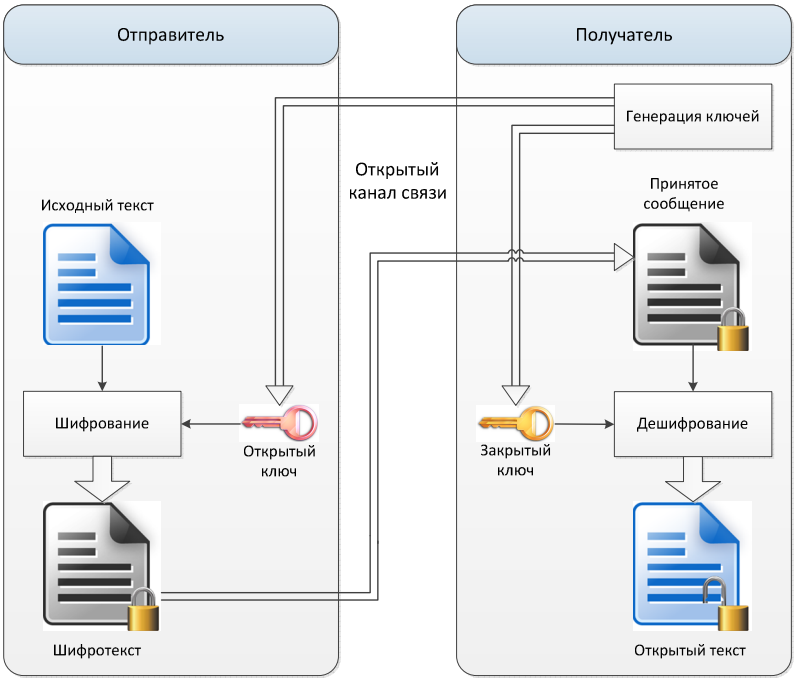

Рис. 2. Схема асимметричного шифрования

2. Симметричное шифрование

В настоящее время симметричные шифры — это:

- блочные шифры, которые обрабатывают информацию блоками определенной длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановок, называемыми раундами. Результатом повторения раундов является лавинный эффект — нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных, когда незначительное расхождение последовательностей бит на входе приводит к их большому различию на выходе раундовой функции;
- поточные шифры, в которых шифрование проводится над каждым битом либо байтом открытого текста с использованием гаммирования [7]. Поточный шифр может быть легко создан на основе блочного, запущенного в специальном режиме (например, ГОСТ 28147-89 в режиме гаммирования).

Большинство симметричных шифров используют сложную комбинацию большого количества подстановок и перестановок. Многие такие шифры используют несколько (иногда до 80) раундов, причем на каждом раунде применяется свой подключ, получаемый разворачиванием исходного секретного ключа. Множество неких подключей для всех раундов образует так называемое «расписание ключей» (key schedule).

Логично предположить, что одна и та же пара открытый текст/ключ будет преобразована в одинаковый шифротекст (рис. 3). Этого можно избежать с помощью инициализирующего вектора – блока случайных данных, накладываемого на текст на некотором этапе шифрования. На рис. 4 представлен один из методов его использования.

Рис. 3. Простейшее блочное преобразование по типу ECB

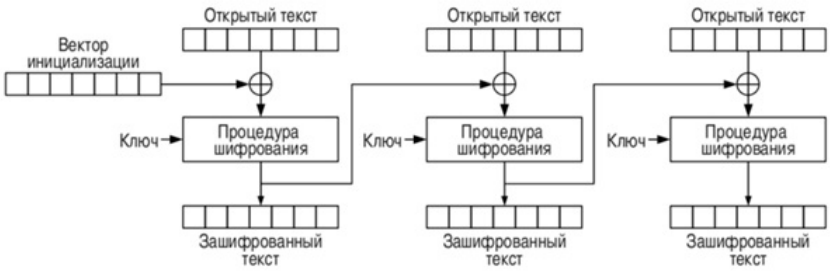

Рис. 4. Использование инициализирующего вектора в методе CBC

В табл. 1 приведены некоторые параметры выбранных для сравнения алгоритмов симметричного шифрования.

Таблица 1

Сравнительные данные некоторых симметричных криптосистем

Система шифрования	Длина ключа, бит	Размер блока, бит	Число раундов	Алгоритмическая основа	Перебор, MIPS x лет
DES	56 + 8 проверочных	64	16	сеть Фейстеля [8]	$5*10^2$
Triple DES	112 (2TDES) 168 (3TDES)	64	48 DES-эквивалентных	сеть Фейстеля	10^{18}
IDEA	128	64	8.5	модификация сети Фейстеля	10^{21}
ГОСТ 28147-89	256	64	32, 16	сеть Фейстеля	нет данных
RC5	0-2040 (128 по умолчанию)	32, 64, 128	1-255 (12 по умолчанию)	сеть Фейстеля	10^3 и выше
Blowfish	32 - 448	64	16	сеть Фейстеля	нет данных
AES [9] (Rijndael)	длина ключа и длина блока могут быть 128, 192 или 256 бит, независимо друг от друга		10, 12, 14	SP-сеть [10]	нет данных

Первым из выбранных для сравнения критериев является криптостойкость алгоритма, то есть его устойчивость к взлому. Взлом алгоритмов ГОСТ, AES и Blowfish атакой грубой силой (полным перебором) за разумное время на момент написания статьи невозможен. На алгоритм AES было проведено множество криптоатак: XSL-атака, атаки на основе связанных ключей, атака по сторонним каналам. Ни одна из проведенных атак не позволяет осуществить взлом алгоритма за разумное число операций. Эффективных атак на алгоритм Blowfish также не было выявлено. В 2011 году Николя Куртуа заявил [11],

что ему удалось взломать ГОСТ с помощью алгебраической атаки, однако на практике уязвимость данного алгоритма не была подтверждена.

Столь же важным в современных информационных системах параметром является скорость шифрования – второй критерий для сравнения. По данным сравнительного анализа, проведенного в университете Вашингтона в Сент-Луисе [12], самым быстрым алгоритмом на данный момент является Blowfish и его производные. На рис. 5 приведена сравнительная диаграмма времени выполнения некоторых алгоритмов симметричного шифрования. За эталонные 100% взят результат самого быстрого алгоритма.

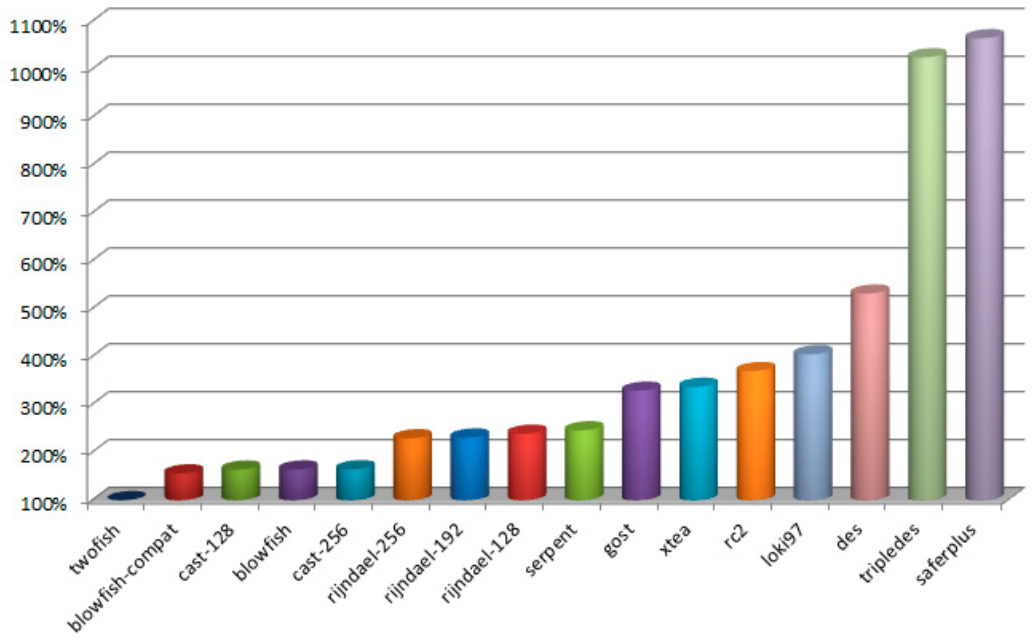

Рис. 5. Время выполнения алгоритмов

Из результатов сравнения следует, что среди современных симметричных криптосистем лучшими по выбранным критериям можно считать Blowfish и AES(Rijndael). При максимальной в классе скорости шифрования данные алгоритмы обеспечивают надежную защиту данных, так как при корректном применении указанных криптосистем ни на одну из них не представляется возможным провести успешную криптоатаку за разумное количество операций.

3. Сравнение с системами с открытым ключом

К достоинствам симметричных алгоритмов можно отнести:

- скорость процесса шифрования-расшифрования на 2-3 порядка выше, так как используется единственный ключ [5];

- простота реализации и модификации за счет более простых операций, меньшие требования к вычислительным ресурсам;
- меньшая требуемая длина ключа для сопоставимой криптостойкости алгоритма, что показано в табл. 2 [5];
- хорошая изученность за счет длительного периода применения технологии.

Таблица 2

Сравнение длин ключей при сопоставимой криптостойкости

Длина секретного ключа (симметричный алгоритм), бит	Длина открытого ключа (алгоритм с открытым ключом), бит
56	384
64	512
80	768
112	1792
128	2304

Недостатки, свойственные симметричным алгоритмам:

- проблема распределения ключей, то есть сложность управления ключами в большой сети. Означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети. Для сети в 10 абонентов требуется 45 ключей, для 100 уже 4950, для 1000 – 499500 и т. д. (по одному ключу на каждую пару);
- проблема алгоритма обмена ключами. Для его применения необходимо обеспечить надежную передачу ключей каждому абоненту, так как нужен защищенный канал для передачи каждого ключа обеим сторонам;
- необходимость обновления ключа после каждой сессии обмена данными.

Заключение

В современной криптологии криптостойкость алгоритмов шифрования определяется следующими параметрами.

1. Длина ключа. Бороться с методом полного перебора позволяет увеличение длины используемого ключа шифрования. Очевидно, увеличение его длины всего на 8 бит увеличивает число вариантов перебора в 2^8 раз, соответственно на 64 бита – в 2^{64} раз. Согласно закону Мура, вычислительная производительность микропроцессоров увеличивается в 100 раз каждые 10 лет. Следовательно, для сохранения криптостойкости тенденция

роста длины ключей для всех алгоритмов будет сохраняться. В этом вопросе значительно выигрывают алгоритмы симметричного шифрования, так как для обеспечения одинакового уровня защищенности требуются ключи меньшей длины, чем в асимметричных криптосистемах.

2. Нелинейность алгоритма преобразования. Современные криптосистемы неразумно пытаться взломать методом прямого перебора: в общем случае стоимость ресурсов, потраченных на проведение атаки «грубой силы», превышает ценность получаемой информации. С целью преодоления криптостойкости алгоритмов предпринимаются попытки отыскать уязвимости в самих алгоритмах шифрования, позволяющие раскрыть используемый ключ или часть открытого текста за приемлемое время, то есть за значительно меньшее число операций. Поэтому задача совершенствования и более глубокой проработки алгоритмов шифрования остается актуальной.

Учитывая указанные выше преимущества и недостатки современных алгоритмов симметричных и асимметричных криптосистем, имеет смысл разделить области их применения в различных информационных системах. Так, алгоритмы симметричного шифрования наиболее целесообразно применять для:

1) защиты локально хранящейся информации, в том числе на веб-страницах, так как скорость их работы значительно выше, чем алгоритмов с открытым ключом;

2) обмена информацией по открытому каналу связи между пользователями без аутентификации (так называемые «доверительные отношения»), поскольку для достижения сопоставимого уровня защищенности требуется использование ключей меньшей длины.

В то же время алгоритмы асимметричного шифрования логично использовать для:

1) организации защищенной сети обмена информацией для множества пользователей с применением методов аутентификации, так как управлять распределением ключей намного проще, чем планировать многопользовательский обмен по закрытому ключу;

2) создания электронной цифровой подписи электронных документов, исключающей возможность их незаметной модификации с момента создания и однозначно определяющей их принадлежность владельцу, так как логика реализации этой функции требует использования именно асимметричных систем.

В перспективе имеет смысл рассмотреть реализации алгоритмов симметричного шифрования, например, в веб-браузерах. В этом случае представляет интерес измерение скорости загрузки и обработки данных браузером и скорости их шифрования соответствующим алгоритмом при обеспечении определённого уровня защищенности данных,

зависящего от криптостойкости алгоритма. Имея в виду сохранение актуальности использования симметричных криптосистем, можно оценить соответствие реализованных алгоритмов шифрования заявленным характеристикам веб-браузеров.

Список литературы

1. Shannon C.E. Communication Theory of Secrecy Systems // Bell Systems Technical Journal. 1949. №28. P. 656–715. Available at: http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf, accessed 20.03.2015.
2. Federal Information Processing Standards Publication 46-3. Data Encryption Standard (DES). NIST, US Department of Commerce, Washington D.C, 1999. Available at: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, accessed 12.01.2015.
3. Federal Information Processing Standards Publication 197. Advanced Encryption Standard (AES). NIST, US Department of Commerce, Washington D.C, 2001. Available at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, accessed 12.01.2015.
4. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введ. 1990-01-07. М.: Изд-во стандартов, 1996. 28 с.
5. Брюс Шнайер. Прикладная криптография, 2-е изд. М.: Триумф, 2002. 816 с.
6. Nechvatal James. Public-Key Cryptography. NIST, Gaithersburg. 1990. 162 p. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.6603&rep=rep1&type=pdf, accessed 20.01.2015.
7. Гончаров Н.О. Симметричное шифрование (гаммирование) // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2011. № 3. Режим доступа: http://technomag.bmstu.ru/doc/187185.html (дата обращения 18.02.2015).
8. Сеть Фейстеля. Википедия – свободная энциклопедия. Режим доступа: https://ru.wikipedia.org/wiki/Сеть_Фейстеля (дата обращения 20.03.2015).
9. Ричард Смит. Разгадка тайны AES // Журнал сетевых решений/LAN. Электрон. журн. 2001. №5. Режим доступа: http://www.osp.ru/lan/2001/05/135172/ (дата обращения 21.12.2014).
10. SP-Сеть. Википедия – свободная энциклопедия. Режим доступа: https://ru.wikipedia.org/wiki/SP-сеть (дата обращения 20.03.2015).
11. Courtois N.T. Security Evaluation of GOST 28147-89 In View Of International Standardisation. Available at: http://eprint.iacr.org/2011/211.pdf, accessed 27.02.2015.
12. Abdel-Karim Al Tamimi. Performance Analysis of Data Encryption Algorithms. Available at: http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/, accessed 19.03.2015.