УДК 004.056.55

ГИБРИДНЫЙ АЛГОРИТМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМЦИИ

Сывокобыльская Е.В., Удовика П.А., Зеленева И.Я., Иванов А.Ю.
Донецкий национальный технический университет, г.Донецк
Кафедра компьютерной инженерии
E-mail: kukareka@gmail.com, paul_u@mail.ru

Аннотация.
Сывокобыльская Е.В., Удовика П.А. Гибридный алгоритм криптографической защиты информации. *В статье рассматриваются проблемы блочного шифрования с использованием алгоритмов двух различных классов кодирования – симметричного и асимметричного, их совместное взаимодействие, проводится анализ системы криптографической защиты с поддержкой цифровой подписи.*

Введение.

Задача защиты информации в компьютерных системах превращается сегодня в одну из наиболее актуальных вследствие широкой распространенности таких систем, а также расширения локальных и глобальных компьютерных систем. В компьютерных сетях передаются огромные объемы информации государственного, военного, приватного характера, обладатели которой часто были бы категорически против ознакомления с этой информацией посторонних лиц.

Не менее важным заданием является широкое внедрение в разные сферы деятельности человека электронного документооборота, который должен быть обеспечен юридической силой подписанных электронных документов. Все эти и множество других задач защиты информации призвана решать криптография [1].

Постановка задач исследования.

Криптография с закрытым ключом подразумевает под собой шифрование информации на ключе, известном только получателю и отправителю, при чем кодирование и дешифровка выполняются с помощью одного и того же ключа [2]. Криптография с открытым ключом позволяет отправителю использовать публичный ключ для шифрования сообщения. Публичным ключом может воспользоваться любой желающий отправить письмо, однако расшифровать информацию с помощью своего приватного ключа может только получатель. Эти ключи так математически связаны между собой, что при изменении одного из них, информация будет искажена [3]. Основной недостаток асимметричной криптографии состоит в низкой скорости из-за сложных вычислений, требуемых ее алгоритмами, в то время как симметричная криптография традиционно показывает блестящую скорость работы. Однако симметричные криптосистемы имеет один существенный недостаток — её использование предполагает наличие защищенного канала для передачи ключей. Для того чтобы избежать низкой скорости алгоритмов асимметричного шифрования, генерируется временный симметричный ключ для каждого сообщения и только он шифруется асимметричными алгоритмами [4].

В данной работе выполнен анализ системы блочного шифрования, которая объединяет в себе принципы работы двух основных классов современных криптосистем, благодаря чему повышается криптостойкость полученного шифра. Совместное использование двух различных принципов шифрования позволяет компенсировать недостатки одной системы достоинствами другой. Предлагается алгоритм разработки системы блочного шифрования, которая использует для кодирования симметричный и асимметричный алгоритмы

вместе. В процессе ее работы генерируется пакет шифрованной информации, в который входят закодированные сеансовые ключи, подписанный хеш-образ и непосредственно сама информация.

В качестве использованных алгоритмов выступают:

- симметричный алгоритм DESX;
- асимметричный алгоритм RSA;
- алгоритм генерирования хеш-функции SHA.

Решение задачи и результаты исследований.

Гибридизация процесса заключается в следующем:

1) Часть исходного сообщения шифруется на сеансовом закрытом ключе.

2) Закрытый ключ шифруется на открытом ключе и добавляется шифрованный пакет информации.

3) Сеансовый закрытый ключ меняется, и пункты 1 и 2 повторяются до полной зашифровки сообщения.

Предлагаемая система будет функционировать по следующему принципу:

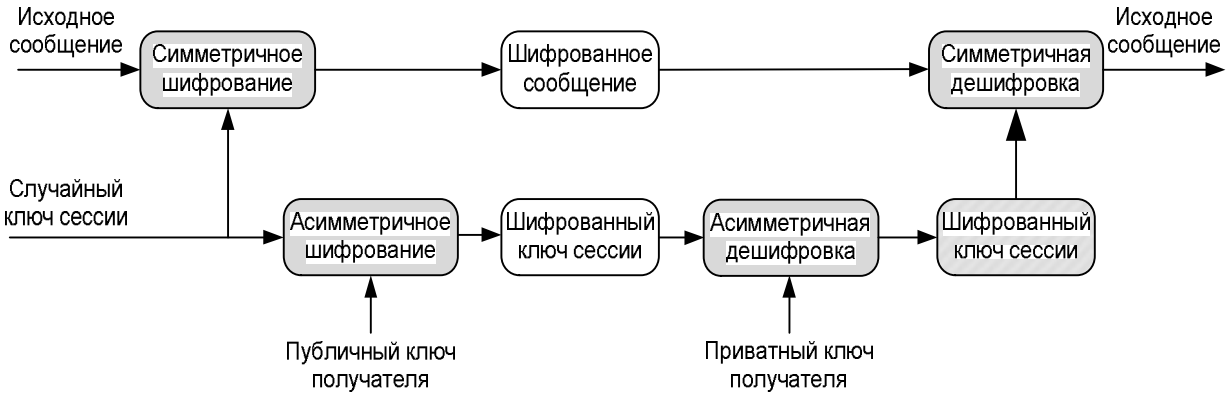

Рисунок 1 – Принцип функционирования разработанной системы шифрования.

На начальном этапе участники информационного обмена, используя протокол выработки общего секретного ключа, формируют общую секретную информацию (секретный ключ). На следующем этапе обмена используется криптосистема с секретным ключом с алгоритмом шифрования DESX. Алгоритм можно обозначить следующим образом:

$$C = DESX_{K1K2K3} = K3 \oplus DES_{K1}(K2 \oplus M), \qquad (1)$$

где С – шифрограмма, К1, К2 и К3 – сеансовые ключи, М – открытый текст.

Алгоритм DES работает с 64-битными входными блоками, поэтому использование одного симметричного ключа может быть чревато успешным осуществлением атак. Эта опасность существует из-за того, что размер информации в исходном файле значительно превышает размер кодированного блока, а ключ будет повторяться. Поэтому целесообразно периодически менять симметричные «зашумляющие» ключи К2 и К3, например через каждые 16 зашифрованных блоков. Т.е. на одних и тех же ключах будет зашифровано только (64/8)*16=128 байт исходной информации. Один такой период будем называть сессией.

DESX имеет всего на две операции XOR больше, чем оригинальный алгоритм DES, что не требует значительных затрат времени.

Одновременно наличие этих операций значительно улучшает стойкость шифрограммы к полному перебору ключей (полная длина составляет К1+К2+К3=64+64+64=192 бита), а также делает ее устойчивее к дифференциальному и линейному криптоанализу [5].

Сеансовый ключ используется для шифровки сообщения при помощи симметричного алгоритма. Он зашифровывается на открытом ключе (алгоритм RSA) получателя и присоединяется к ранее зашифрованному документу. Шифруемые данные необходимо разбить на блоки - числа от 0 до n - 1. Числа e и d являются ключами [4]. Шифрование и дешифровка данных производятся следующим образом:

- шифрование: $b = a^e \pmod n$; *(2)*
- дешифровка: $a = b^d \pmod n$. *(3)*

Сформированное таким образом сообщение отсылается получателю. Последний, получив сообщение, повторяет те же процедуры, но в обратном порядке – с помощью своего секретного ключа он восстанавливает сеансовый ключ и расшифровывает сообщение. Формат сообщения должен иметь следующий вид:

1 сессия кодированного текста	3 закодированных сессийных ключа	2 сессия кодированного текста	3 закодированных сессийных ключа	...	n сессия кодированного текста	3 закодированных сессийных ключа	цифровая подпись
128 байт	192 бита	128 байт	192 бита		128 байт	192 бита	160 бит

Рисунок 2 – Формат шифрованного сообщения

Для избежания атаки типа «посредник» (подмена публичного ключа) целесообразно использовать электронную цифровую подпись. Электронная цифровая подпись была изобретена после открытия асимметричной криптографии [6]. В разработанной системе она используется с алгоритмом RSA и функцией хеширования SHA. К сообщению M применим превращение с помощью приватного ключа d и назовем его цифровой подписью, то есть

$$S=M^d \bmod n. \qquad (4)$$

Сообщение M и его цифровая подпись S отправляются по назначению. Получатель, имея M, S и открытый ключ отправителя e может проверить соотношение

$$S^e \bmod n = M. \qquad (5)$$

Если вычисленное M совпадает с полученным, то подпись настоящая.

Т.к в данном случае подпись имеет ту же длину, что и сообщение, применяют *хеширование.* Хеш-функция выполняет одностороннее превращение двоичной последовательности произвольной длины в двоичную последовательность фиксированной длины. В случае использования хеш-функции алгоритм формирования цифровой подписи такой:

1) сообщение хешируется, т.е. вычисляется h(M);
2) к полученному h применяется асимметричное криптографическое преобразование с помощью приватного ключа. Для RSA — это

$$S=[h(M)]^d \bmod n. \qquad (6)$$

3) на принимающей стороне, после получения M и S, проверяется подписанное сообщение

$$S^e \bmod n = h(M) \qquad (7)$$

4) и одновременно вычисляется хеш-образ полученного сообщения h'(M), и если

$$h(M)=h'(M), \qquad (8)$$

то получатель уверен, что:

- сообщение M не было повреждено во время передачи по каналам связи;
- хеш-образ h(M) соответствует сообщению M и также не изменялся при передаче;
- сообщение написано владельцем приватного ключа d, и он согласен с его содержимым;
- отправитель не может отказаться от факта сообщения [6].

Выводы.

Принцип работы предложенной гибридной системы является по сути компромиссом между симметричной и асимметричной криптографией. Открытое шифрование устраняет опасность передавания ключей по открытым каналам, при чем его невысокая скорость обработки информации практически не повлияет на быстродействие системы, т.к. ключи занимают намного меньше места, чем само сообщение

В результате работы продукта, будет получен пакет информации, который только получатель сможет верно интерпретировать и расшифровать без помех. В данной системе в первую очередь будут заинтересованы небольшие предприятия, не нуждающиеся в громоздких и дорогостоящих средствах защиты информации, но желающие защитить свои важные документы от злоумышленников.

Список литературы

1. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996.
2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. — М.: Горячая линия — Телеком, 2002. — 175 с.
3. Столлинс Криптография и защита сетей. – М.: Вильямс, 2004. – 848 с.
4. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография - СПб: Изд."Лань", 2001
5. Масленников М.Е. Практическая криптография. – СПб.: БХВ-Петерб., 2003 – 464 с.
6. Остапов С.Е., Валь Л.О. Основи криптографії. – Чернівці: Книги – XXI, 2008. – 188 с