Амиров Азамат Жанбулатович,
доктор PhD, каф. ИТБ, КарГТУ,
г. Караганда, Республика Казахстан,
Дукенбаева Сандугаш Амангельдиновна,
магистрант, КарГТУ,
г. Караганда, Республика Казахстан

ИССЛЕДОВАНИЕ И АНАЛИЗ МЕТОДОВ И АЛГОРИТМОВ ШИФРОВАНИЯ ИНФОРМАЦИИ В АСИММЕТРИЧНОЙ КРИПТОСИСТЕМЕ

Аннотация. В проводимом исследовании по изучению и анализу современных методов и алгоритмов шифрования информации в асимметричных системах ставятся задачи оценить надежности существующих алгоритмов в асимметричных системах, проанализировать слабые места и требования к технике, как для шифрования, так и для взлома данного алгоритма, проанализировать быстродействие систем шифрования. В работе были использованы методы статистической обработки данных. Основные методы исследований: научный поиск, анализ и обобщение информационных материалов и результатов имитационных экспериментов.

Ключевые слова: RSA, шифрование, криптология, алгоритм, асимметричная криптосистема

В современном мире развитых технологий огромные потоки информации проходят через глобальную сеть Интернет. Часть из них носят конфиденциальный характер и требуют защиты от злоумышленников, пытающихся ее перехвата. В связи с этим очень важной задачей является ее защита.

Основным путем решения данной проблемы является создание защищенных каналов связи и шифрование информации. Наука, занимающаяся методами шифрования и дешифрования, называется криптологией. Существует множество различных методов шифрования информации в криптосистемах. Однако с каждым годом требования к ним растут, т.к. прогресс не стоит на месте. Техника постоянно усовершенствуется, а вместе с ней увеличивается возможности взлома алгоритма и прочтения зашифрованного текста.

На сегодняшний день криптология развивается в трех направлениях:

– привычные и хорошо известные алгоритмы RSA, Эль-Гамаля и др.;

– алгоритмы на основе эллиптических кривых и их разновидностей;

– алгоритмы, основанные на принципах квантовой механики.

В настоящее время в условиях быстрого развития информационных технологий помимо изобретения новых алгоритмов и методов шифрования, большое внимание уделяется их производительности при сохранении криптостойкости.

Актуальность исследования в изучении криптостойкости алгоритмов и методов шифрования и их быстродействие:

– во-первых, возросшее влиянием информации на многие стороны общественной жизни (социальной, экономической, политической);

– во-вторых, в связи с повсеместной и массовой компьютеризацией информационных процессов, широким внедрением и интеграцией информационно-вычислительных сетей во всемирную сеть с доступом к их ресурсам широких масс пользователей.

Практическая ценность данной работы заключается в том, что она предоставляет возможность для рядового пользователя выбрать наиболее надежный и быстродействующий алгоритм шифрования, что на сегодняшний имеет большое практическое значение.

При написании алгоритмов шифрования использовалась программа SharpDevelop версии 4.4. SharpDevelop – свободная среда разработки для C#, Visual Basic .NET, Boo, IronPython, IronRuby, F#, C++. Предоставляет интегрированный отладчик, который использует собственные библиотеки и взаимодействует с исполняющей средой .NET через COM Interop.

Анализ быстродействия алгоритма шифрования RSA

На сегодняшний день для обеспечения необходимого уровня безопасности алгоритмов, реализованных на основе RSA, Эль-Гамаля или p-метода Полланда необходим ключ не менее 1024 бит, т.е. число величиной 2^{1024}. Однако обычный ПК не обладает достаточной мощностью для подобных вычислений, поэтому для вычисления будут использовать значения в разы меньше.

Характеристики рабочей станции:

Процессор: Intel(R) Core(TM) i3 – 3337U CPU 1.80GHz, 1801 Mhz;

ОП: 4 Гб;

ОС: Windows 7 64-bit.

RSA

Исходные данные:

– текст в 690 символов (первая глава рассказа «The Chronicles of Narnia 1 – The Magician's Nephew»)

– параметры открытого ключа: N = 76053403, e = 32621371

Рисунок 1 – Временная таблица работы функций шифрования алгоритма RSA – Encode и InitKeyData

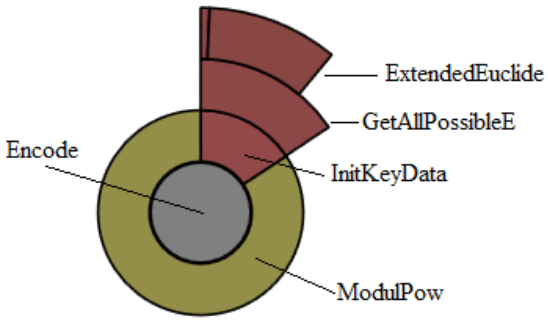

Рисунок 3 – Временная диаграмма работы функций шифрования алгоритма RSA – Encode и InitKeyData

15,72% времени, которое уходит на генерацию ключа, выполняются следующие функции:

InitKeyData – сама функция генерации ключа, в которую входит функция поиска простых чисел (GetNotDivideable);

GetAllPossibleE – функция, которая находит все возможные значения одного из параметров открытой пары, удовлетворяющие условию $ed \equiv 1 (\mathrm{mod}\ \phi(N))$.

ExtendedEuclide – функция, основанная на теории Евклида, которая вызывается при выполнении предыдущей функции.

Процесс расшифровки занимает немного меньше времени по сравнению с шифрованием сообщения, т.к. нет необходимости генерировать ключ, поскольку он уже сформирован – 4 минут 38 секунд (278308,648084 ms).

Name	Time spent	Time spent (self)	Time spent/call	Time spent (self)/ca	% of parent
⊞ RSA.decode	278308.648084ms	2.148625ms	278308.648084ms	2.148625ms	100.00%
RSA.ModuloPow	278286.363477ms	278286.363477ms	403.898931ms	403.898931ms	100.00%

Рисунок 1 – Временная таблица работы функции дешифрования алгоритма RSA – decode

В результате изучены принципы работы алгоритмов и методов шифрования в асимметричной криптосистеме (RSA, Эль-Гамаля, криптосистема Рабина, метод p-Полланда, алгоритмы на основе эллиптических кривых и принцип работы алгоритмов в квантовой криптографии); проанализированы «слабые» места алгоритмов; изучены существующие методы атак на алгоритмы; выполнена программная реализация алгоритмов шифрования RSA; проанализировано быстродействие реализованных алгоритмов.

СПИСОК ЛИТЕРАТУРЫ

1. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin "Experimental Quantum Cryptography" Journal of Cryptology vol.5, no.1, 1992, pp. 3-28

2. C. Chevalley, Introduction of the theory of algebraic functions of one variable – NY: American mathematical society, 1951

3. W.Diffie and Hellman. Multiuser cryptographic technique. In Proceedings of AFIPS 1976 NCC, pages 109-112. AFIPS Press, Montvale, N.J., 1976