УДК 681.3.7

С.Н. ФИСУН, А.И. КОПЫЛОВ

Севастопольский национальный технический университет, Украина

МЕТОДИКА ШИФРОВАНИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНО-МЕТОДИЧЕСКОГО КОМПЛЕКСА VisualAES

Рассматривается программно-обучающая система шифрования данных симметричным алгоритмом AES, которая позволит пользователю оценить свои знания в области симметричных шифров, визуализировать раундовые преобразования алгоритма, а также закрепить знания, путём изучения теоретического модуля программы. Кроме того, в работе был проведён сравнительный анализ симметричных блочных алгоритмов шифрования на примере алгоритмов DES, 3DES и AES. В качестве основных критериев оценки выступали два параметра: скорость шифрования информации и криптостойкость используемого шифра.

Ключевые слова: *защита информации, алгоритмы шифрования, программно-обучающая система.*

Введение

Разработка программных комплексов, предназначенных для защиты информации от несанкционированного доступа в компьютерных системах (КС) требует реализации определенного числа криптографических алгоритмов, которые бы отвечали требованиям, предъявляемым к данной системе. Существуют два основных типа алгоритмов шифрования: симметричный и асимметричный. При использовании симметричных алгоритмов шифрования для шифрования и расшифровки сообщений используется один и тот же ключ. Основное преимущество симметричного шифрования заключается в быстроте шифрования и расшифровки сообщений. Однако у него есть один серьёзный недостаток: необходимость передачи ключа от одной стороны другой. Если при передаче ключ будет захвачен злоумышленниками, то шифрование потеряет всякий смысл [2]. Асимметричное шифрование избавлено от этого недостатка. При асимметричном шифровании используется пара ключей. Сообщение шифруется публичным ключом, который может быть известен каждому. Но расшифровано оно может быть только личным ключом, который хранится в секрете. Ключи связаны математически так, что, зная публичный ключ, нельзя вычислить личный. Это очень удобно, но за безопасность приходится платить низкой скоростью работы асимметричного шифра.

В работе рассматриваются сравнительный анализ, выделены основные особенности симметричного алгоритма шифрования AES по отношению к конкурентам. Во второй части работы рассматривается разработанная авторами программно-обучающая система шифрования данных.

1. Сравнительный анализ симметричных алгоритмов шифрования

Выполним сравнительный анализ трех наиболее популярных на сегодняшний день симметричных алгоритмов шифрования информации – DES (Data Encryption Standard), 3DES и AES (Advanced Encryption Standard). На эффективность функционирования систем шифрования влияют два основных параметра: скорость шифрования информации и криптостойкость используемого шифра.

Для оценки производительности рассматриваемых алгоритмов было разработано соответствующее программное обеспечение (ПО) на языках программирования Java и C#.

Алгоритмы были реализованы с использованием 2-х подходов:

1. Разработка программной системы шифрования данных по опубликованным криптографическим алгоритмам;

2. Разработка ПО с использованием криптографических сервисов, предоставляемых платформами .NET и Java.

Второй подход обладает не оспоримым преимуществом, т.к. позволяет значительно сократить время разработки программы.

Тестирование производительности выполнялась на компьютере с процессором Intel Pentium Dual Core E2180, с объемом оперативной памяти 3 Гб. В качестве ОС для тестирования были выбраны операционные системы корпорации Microsoft – Windows XP Professional (с Service Pack 3) и Windows Seven Ultimate Edition (с Service Pack 1).

Результаты тестирования сведены в табл. 1. Скорости алгоритмов сгруппированы следующим

образом. Первая группа ($I \in (0мс;100мс)$) обладает самой высокой скоростью выполнения, далее следуют вторая ($II \in (100мс;200мс)$) и третья ($III \in (200мс;\infty)$) группы.

Таблица 1

Выполнение шифрования и дешифрования на различных платформах.

Платформа / Алгоритмы	Windows 7				Windows XP			
	C#	J#	C# API	J# API	C#	J#	C# API	J# API
AES128	II	II	I	II	I	II	I	I
AES192	II	III	II	II	II	II	I	II
AES256	III	III	II	III	III	III	II	II
DES	II	II	II	II	II	II	II	II
3DES	III	III	III	III	III	III	II	III

Алгоритм AES обеспечивает последовательно высокое выполнение для шифрования, дешифрования, хотя выполнение и понижается для 192- и 256-битных ключей.

Также данный алгоритм является наиболее предпочтительным с точки зрения защиты шифруемой информации, поскольку на сегодняшний день в алгоритме не обнаружено существенных уязвимостей, позволяющих значительно понизить криптостойкость шифра [1].

Алгоритм DES также обеспечивает достаточно высокую скорость шифрования, дешифрования за счет простой структуры алгоритма и малой длинны ключа. Однако небольшой размер ключа одновременно является и недостатком данного алгоритма, поскольку он позволяет взломать алгоритм даже путем полного перебора.

Что касается алгоритма Triple DES, то по скорости шифрования / дешифрования он является аутсайдером, но при этом данный алгоритм обладает 168-битным ключом и как следствие высокой криптостойкостью.

По результатам тестирования производительности видно, что оптимальной программной платформой для разработки криптографического ПО является платформа .NET и язык программирования C#. Уровень производительности языка Java уступает платформе .NET, однако его можно рассматривать как инструмент для кроссплатформенной разработки.

Кроме того можно заметить, что подход с использованием криптографических сервисов, предоставляемых платформами .NET и Java является более производительным.

Также данный подход позволяет значительно сократить время разработки ПО.

2. Основные особенности алгоритма

Стандарт шифрования AES, специфицирующий алгоритм Rijndael [1], представляет собой симметричный блочный шифр, который работает с блоками данных длиной 128 бит и использует ключи 128, 192 и 256 бит (версии AES-128, AES-192, AES-256). Сам алгоритм может работать и с другими длинами блоков данных и ключей, но эта возможность в стандарт не вошла.

Как и алгоритм DES (а также большинство современных симметричных блочных шифров), алгоритм Rijndael (AES) состоит из большого количества повторяющихся преобразований — раундов. В минимальном варианте, когда размеры блока и ключа равны 128 бит, количество раундов равно 10. Для более крупных сообщений и ключей количество раундов может возрастать [2].

Перечислим основные особенности алгоритма:

1. Новая архитектура, получившая название «Квадрат». Она обеспечивает быстрое рассеивание и перемешивание информации, при этом за один раунд преобразованию подвергается весь входной блок.

2. В алгоритме применяется байт-ориентированная структура, удобная для реализации на 8-разрядных микроконтроллерах.

3. Эффективная аппаратная и программная реализация на различных платформах.

3. Описание программной системы

Рассмотрим разработанную авторами программно-обучающую систему шифрования данных с использованием алгоритма AES. Программа написана на языке программирования C#. Финальная отладка и тестирование программы велось в среде разработки Visual Studio 2010. Для запуска и управления работой программы «VisualAES» используется окно (рис. 1).

Рис. 1. Главное окно программы.

Программа включает в себя следующие компоненты:

– средства полноценной реализации алгоритмов: шифрования / дешифрования с использованием основных блочных режимов – ECB, CBC, CFB, OFB, CTR;

– средства визуализации раундовых преобразований шифра;

– справочные средства, позволяющие пользователю ознакомиться с теоретическими основами алгоритма AES;

– средства проверки знаний пользователя.

Основные области применения разработанной программной системы:

– практическое решение задач шифрования данных по стандарту AES;

– использование её в качестве дидактического материала в дисциплинах по защите информации.

Актуальность данной разработки обуславливается следующими фактами:

– во-первых, постоянно повышающимся интересом мирового сообщества к проблемам защиты информации – её конфиденциальности и аутентичности и, что ещё важнее, к вопросам надёжности принятого стандарта AES;

– во-вторых, отсутствием, по мнению авторов, удобного инструментария для визуализации решения поставленных задач.

Литература

1. Панасенко, С.П. Алгоритмы шифрования. Спец. справочник [Текст] / С.П. Панасенко. – СПб.: БХП Петербург, 2009. – 576 с.

2. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Текст] / А.А. Петров. – М.: ДМК, 2000. – 448 с.

Поступила в редакцию 25.03.2012

Рецензент: д-р техн. наук, проф., заведующий кафедры компьютерной инженерии В.А. Краснобаев, Полтавский национальный технический университет им. Юрия Кондратюка, Полтава, Украина.

МЕТОДИКА ШИФРУВАННЯ ДАНИХ З ВИКОРИСТАННЯМ ПРОГРАМНО-МЕТОДИЧНОГО КОМПЛЕКСА VisualAES

С.М. Фісун, А.І. Копилов

Розглядається програмно-навчальна система шифрування даних симетричним алгоритмом AES, яка дозволить користувачеві оцінити свої знання в області симетричних шифрів, візуалізувати раундові перетворення алгоритму, а також закріпити знання, шляхом вивчення теоретичного модуля програми. Крім того, в роботі було проведено порівняльний аналіз симетричних блокових алгоритмів шифрування на прикладі алгоритмів DES, 3DES і AES. В якості основних критеріїв оцінки виступали два параметри: швидкість шифрування інформації та криптостійкість використовуваного шифру.

Ключові слова: захист інформації, алгоритми шифрування, програмно-навчальна система.

METHODOLOGY OF ENCRYPTION DATA USING SOFTWARE COMPLEX VisualAES

S.N. Fisun, A.I. Kopylov

We consider the software-training system for encryption symmetric algorithm AES, which allows the user to evaluate their knowledge of symmetric ciphers, to visualize the round transformation algorithm, and also to consolidate the knowledge through the study of theoretical modules of the program. In addition, in a comparative analysis of symmetric block cipher algorithms, the example of DES, 3DES and AES. The main evaluation criteria were the two parameters: the speed of encryption and crypto-strength encryption is used.

Key words: data security, encryption, software and training system.

Фисун Сергей Николаевич – канд. техн. наук, доцент, доцент кафедры кибернетики и вычислительной техники Севастопольского национального технического университета, Севастополь, Украина.

Копылов Александр Игоревич – магистрант кафедры кибернетики и вычислительной техники Севастопольского национального технического университета, Севастополь, Украина.