Министерство образования Республики Беларусь
Учреждение образования «Барановичский государственный университет»
Студенческое научное общество БарГУ

СОДРУЖЕСТВО НАУК. БАРАНОВИЧИ-2016

Материалы XII Международной
научно-практической конференции
молодых исследователей

(Барановичи, 19—20 мая 2016 года)

В трёх частях

Часть 2

Барановичи
БарГУ
2016

УДК 001(082)

В части 2 сборника материалов XII Международной научно-практической конференции молодых исследователей «Содружество наук. Барановичи-2016» представлены результаты исследований в области физики и математики, а также рассмотрены актуальные проблемы в области информационных систем и технологий в образовании, науке и технике. Особое внимание уделено современным тенденциям в технологиях и материалах машиностроительного и сельскохозяйственного производств, а также экономическим аспектам развития предприятия, региона.

Сборник адресован научным работникам, аспирантам, магистрантам и студентам инженерных и экономических специальностей учреждений высшего образования.

Научное издание

СОДРУЖЕСТВО НАУК.
БАРАНОВИЧИ-2016

Материалы XII Международной
научно-практической конференции
молодых исследователей

(Барановичи, 19—20 мая 2016 года)

На русском, белорусском, английском языках

В трёх частях
Часть 2

Ответственный за выпуск Е. Г. Хохол
Технический редактор А. Ю. Сидоренко
Компьютерная вёрстка С. М. Глушак
Корректор Н. Н. Колодко

Подписано в печать 04.10.2016. Формат 60 × 84 $^{1}/_{8}$. Бумага ксероксная.
Отпечатано на копировально-множительной технике. Усл. печ. л. 28,00. Уч.-изд. л. 25,10. Тираж 9 экз. Заказ 681.

Учреждение образования «Барановичский государственный университет».
Свидетельство о государственной регистрации издателя № 1/424 от 09.09.2016.
Ул. Войкова, 21, 225404 г. Барановичи. Тел. 8 (0163) 45 46 28, e-mail: rio@barsu.by .

ISBN 978-985-498-736-1 (ч. 2)
ISBN 978-985-498-734-7

УДК 519.72

Е. В. Цебрук
Учреждение образования «Барановичский государственный университет», Барановичи

РАЗРАБОТКА КОМПЬЮТЕРНОЙ ВЕРСИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ АЛГОРИТМА RSA ДЛЯ ПРИМЕНЕНИЯ В ЛОКАЛЬНОЙ СЕТИ

Введение. Проблема защиты информации в компьютерных системах, предназначенных для обработки данных, постоянно находится в центре внимания не только специалистов по разработке этих систем, но и широкого круга пользователей. Широкое распространение и применение вычислительной техники очень резко повысили уязвимость накапливаемой, хранимой и обрабатываемой информации в компьютерных системах обработки данных.

В функционирующих локальных сетях как никогда актуальна проблема защиты информации от несанкционированного использования или искажения. Прямое применение криптографических систем защиты информации резко замедляет её передвижение. Практическим средством устранения этой проблемы является применение цифровой подписи.

Целью работы является изучение аспекта формирования цифровой подписи, методики определения авторства и целостности передаваемой информации. Объект исследования — информация, передаваемая по локальной сети. Предмет исследования — цифровая подпись блоков передаваемой информации.

Передача информации по сети значительно увеличивает скорость обмена данными, возникает проблема установления подлинности автора и отсутствия изменений в полученном документе. Поэтому задачей работы является разработка системы, предоставляющей защиту передаваемых сообщений от возможных видов злоумышленных действий.

Основная часть. Общепризнанные приёмы установления подлинности физической подписи под документом абсолютно не пригодны при обработке документов в электронной форме. Решением данного вопроса является алгоритм системы электронного подписания документов. При использовании цифровой подписи информация не шифруется и остаётся доступной любому пользователю, имеющему к ней доступ.

Электронная цифровая подпись представляет собой уникальное число, зависящее от подписываемого документа и секретного ключа абонента. В качестве подписываемого документа может быть использован любой файл. Подписанный файл создаётся из неподписанного путём добавления в него одной или более электронных подписей.

Система электронной цифровой подписи включает две основные процедуры: формирование цифровой подписи, проверку цифровой подписи [1, с. 254].

Проверить сформированную подпись может любое лицо, так как ключ проверки подписи является открытым. При положительном результате проверки подписи делается заключение о подлинности и целостности полученного сообщения, т. е. о том, что это сообщение действительно отправлено тем или иным отправителем и не было модифицировано при передаче по сети [2, с. 113].

Для создания приложения была использована интегрированная среда разработки программного обеспечения MS Visual Studio 2012, т. е. один из её компонентов — Visual C#.

Приложение имеет клиент-серверную архитектуру. Клиент и сервер могут находиться как в рамках одной вычислительной системы, так и на различных компьютерах, связанных сетью. Приложение позволяет производить отправку как текстовых сообщений, так и различных видов файлов по сети. Для установления подлинности автора и отсутствия изменений в полученном документе приложение позволяет сформировать электронную цифровую подпись на базе алгоритма RSA. В качестве подписываемого документа может быть использован любой файл. После получения цифровой подписи файлы (документ, файл открытого ключа с расширением .key и файл цифровой подписи с расширением .eds) могут быть отправлены получателю. В свою очередь получатель имеет возможность проверки подлинности полученного файла.

При обмене сетевыми сообщениями используется принцип работы протокола TCP (протокол управления передачей), разработанный для надёжной доставки сетевой информации, позволяющий успешно обмениваться файлами и текстовыми сообщениями. Протокол TCP для своей функциональности требует наличие постоянного соединения между сетевыми процессами. Разбивая отсылаемое сообщение на части, называемые пакетами, протокол TCP помечает их таким образом, что независимо от очереди доставки этих пакетов сообщение будет собрано точно, так как оно и было изначально, причём при потере части данных механизм протокола управления передачей запросит потерянные пакеты повторно. При этом он ещё и проверяет целостность каждого пакета.

Исходный код клиентского и серверного приложения, демонстрирующего сетевую работу по протоколу TCP, построен на высокоуровневых классах TcpListener и TcpClient. Данные классы инкапсулируют в себе более низкоуровневый класс Socket, предоставляя готовые настройки для прослушивающего сокета — класс TcpListener, и сокета, создающего клиентское подключение, — класс TcpClient.

Приложение имеет три вкладки, реализованные с помощью компонента TabControl. Вкладка «Обмен файлами и сообщениями» позволяет произвести запуск сервера, а также отслеживает подключение клиентов. На данной вкладке пользователи имеют возможность обмениваться необходимыми сообщения либо файлами (рисунок 1).

Вкладка «Генерация ключа» позволяет получить электронную цифровую подпись для выбранного пользователем файла (рисунок 2).

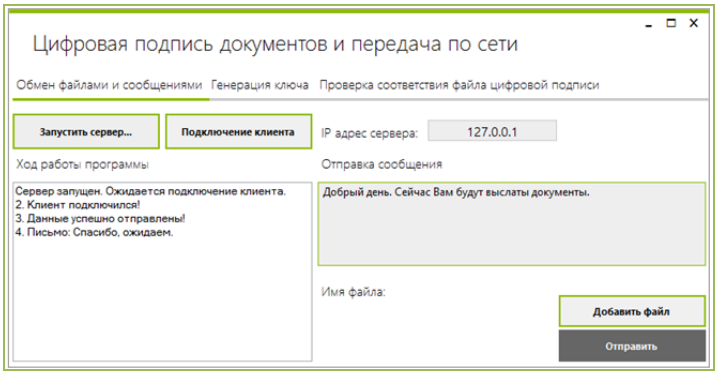

Рисунок 1 — Вкладка «Обмен файлами и сообщениями»

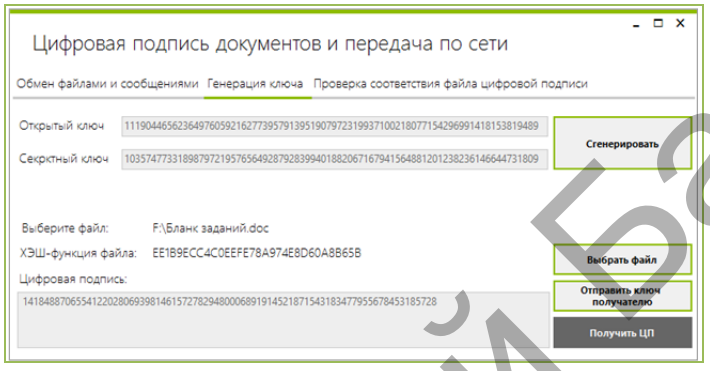

Рисунок 2 — Вкладка «Генерация ключа»

Заключение. В среде MS Visual Studio 2012 на языке C# разработан клиент-серверный программный продукт, позволяющий передавать данные по локальной сети, также учитывающий нюансы работы с криптографической системой RSA и электронной цифровой подписью на её основе. Разработанная версия электронной цифровой подписи пригодна для реализации в локальной сети.

Метод формирования и проверки цифровой подписи RSA даёт возможность обработки и подписания документа одновременно несколькими пользователями. При этом размер подписи не увеличивается.

Список цитируемых источников

1. Конопелько В. К., Липницкий В. А. Теория прикладного кодирования : учеб. пособие. Минск : БГУИР, 2004. 285 с.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие. М. : ФОРУМ, 2008. 416 с.

УДК 624.072.2

А. В. Шах, Я. К. Левшунов
Учреждение образования «Барановичский государственный университет», Барановичи

РАЗРАБОТКА ПРОГРАММНОГО ПРИЛОЖЕНИЯ ДЛЯ РАСЧЁТА ФЕРМОВЫХ БАЛОЧНЫХ КОНСТРУКЦИЙ МЕТОДОМ КОНЕЧНЫХ ЭЛЕМЕНТОВ

Введение. Ферма — это стержневая система, стержни которой между собой соединены с помощью шарниров. Фермы широко используются в современном строительстве, в основном для перекрытия больших пролётов в целях уменьшения расхода применяемых материалов и облегчения конструкций, например, в строительных большепролётных конструкциях типа мостов, стропильных систем промышленных зданий, спортивных сооружений, а также при возведении небольших лёгких строительных и декоративных конструкций — павильонов, сценических конструкций, тентов и подиумов.

Фюзеляж самолёта, корпус корабля, несущий кузов автомобиля (кроме открытых кузовов, работающих как простая балка), автобуса или тепловоза, вагонная рама со шпренгелем, с точки зрения сопромата, являются фер-