Крахмаль Александр Викторович
Студент кафедры систем управления в проектировании ТУСУРа
Телефон: (3822) 73 83 37

S.K. Zeman, S.N. Vladimirov, E.V. Krokhmal, A.V. Krakhmal
Program complex for analysis of temperature fields induced with induction sources

Developed by authors program complex for analysis of temperature fields and deformation processes in composition solid-state objects heating with induction sources is discussed. Applied orientation of this complex concerned with computer simulation and optimization of the engineering development of the processes of assembling — dismantling of components and mechanisms conjugated with hot seating.

УДК 004.312.26

Е.В. Игоничкина

Учебный программный комплекс по изучению отечественных стандартов функции хэширования и цифровой подписи

В статье приведен обзор алгоритмов цифровой подписи. Дано описание разработанного автором учебного программного комплекса по изучению отечественных стандартов функции хэширования ГОСТ Р 34.11-94 и цифровой подписи ГОСТ Р 34.10-2001.

1. Введение

В последнее время все больше и больше внедряются в нашу повседневную жизнь информационные технологии, пытаясь захватить в ней все: от важнейших государственных проектов до решения обычных бытовых проблем. Вместе с огромной пользой и, казалось бы, неограниченными возможностями новые технологии приносят и новые проблемы. Одной из них является проблема защиты информации от несанкционированного посягательства тех, кто доступа к этой информации иметь не должен. В связи с этим почти одновременно с развитием информационных и компьютерных технологий начали развиваться и технологии защиты информации, развитие которых с некоторой точки зрения гораздо более критично, чем развитие непосредственно информационных технологий. Ведь с совершенствованием систем защиты совершенствуются и методы взлома, обхода этих защит, что требует постоянного пересмотра и увеличения надежности защиты информации.

Способов защиты информации существует очень много, но каждый из них всегда можно отнести к одному из двух видов: физическое сокрытие информации от противника и *шифрование* информации. Зашифрованную информацию можно свободно распространять по открытым каналам связи без боязни ее раскрытия и нелегального использования. Хотя, конечно же, такая защита не абсолютно надежна, и каждый из способов шифрования характеризуется своей *стойкостью*, т.е. способностью противостоять криптографическим атакам.

Данная статья посвящена одной из важнейших задач криптографии — *электронной цифровой подписи* (*digital signature*). Электронная цифровая подпись (ЭЦП) необходима для однозначного и никем неоспоримого установления автора какого-либо документа. Фактически, ЭЦП служит аналогом обычной подписи, которая устанавливает подлинность какого-либо документа или договора. Но поскольку в последнее время огромное количество договоров и документов заключается с использованием электронных и компьютерных средств, то поставить на них обычную подпись не представляется возможным. Именно в таких ситуациях и используется электронная цифровая подпись. Электронная цифровая подпись создана для того, чтобы избежать подделок, а также искажений передаваемых сообщений.

2. Обзор алгоритмов ЭЦП

Технология применения системы электронной цифровой подписи предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа. Иначе говоря, открытый ключ является необходимым инструментом, позволяющим проверить подлинность электронного документа и автора подписи. Открытый ключ не позволяет вычислить секретный ключ [1].

Для генерации пары ключей (секретного и открытого) в алгоритмах ЭЦП используются разные математические схемы, основанные на применении однонаправленных функций. Эти схемы разделяются на две группы. В основе такого разделения лежат известные сложные вычислительные задачи:

- задача факторизации (разложения на множители) больших целых чисел;
- задача дискретного логарифмирования.

Первой и наиболее известной во всем мире конкретной системой ЭЦП стала система **RSA**, математическая схема которой была разработана в 1977 г. в Массачусетсском технологическом институте США. Алгоритм получил свое название по первым буквам фамилий его авторов: Rivest, Shamir и Adleman. Надежность алгоритма основывается на трудности факторизации больших чисел.

Более надежный и удобный для реализации на персональных компьютерах алгоритм ЭЦП был разработан в 1984 г. американцем арабского происхождения Тахером Эль Гамалем и получил название **El Gamal Signature Algorithm (EGSA)**.

Идея EGSA основана на том, что для обоснования практической невозможности фальсификации ЭЦП может быть использована более сложная вычислительная задача, чем разложение на множители большого целого числа, — задача дискретного логарифмирования.

Алгоритм цифровой подписи **Digital Signature Algorithm (DSA)** предложен в 1991 г. в США для использования в стандарте цифровой подписи DSS (Digital Signature Standard). Алгоритм DSA является развитием алгоритма ЭЦП EGSA. По сравнению с алгоритмом ЭЦП EGSA алгоритм DSA имеет преимущества: сокращены объем памяти и время вычисления подписи. Недостатком же является необходимость выполнять при подписывании и проверке подписи сложные операции деления по модулю большого числа.

Отечественный алгоритм цифровой подписи, определяемый **ГОСТ Р 34.11-4**, концептуально близок к алгоритму DSA. Различие между ними заключается в использовании параметров ЭЦП разного порядка, что приводит к получению более безопасной подписи при использовании отечественного стандарта.

Алгоритмы цифровых подписей **Elliptic Curve Digital Signature Algorithm (ECDSA)** и **ГОСТ Р 34.10-2001** являются усовершенствованием цифровых подписей соответственно DSA и ГОСТ Р 34.10-94. Эти алгоритмы построены на базе математического аппарата эллиптических кривых над простым полем Галуа.

3. Учебный программный комплекс

Развитие вычислительной техники и рост компьютеризации учебных заведений открывают сегодня возможности широкомасштабного внедрения информационных технологий в учебный процесс. В данной работе создан учебный программный комплекс, позволяющий получить теоретическую информацию по хэш-функции и ЭЦП, а также навыки практической работы с отечественными стандартами хэш-функции ГОСТ Р 34.11-94 и ЭЦП ГОСТ Р 34.10-2001.

Процесс подписи некоторого сообщения состоит из нескольких этапов:

1) генерация секретного ключа;

2) генерация открытого ключа;

3) хэширование подписываемого сообщения;

4) формирование цифровой подписи.

Подписанное сообщение и открытый ключ передаются получателю, который проверяет цифровую подпись на подлинность.

Процесс проверки цифровой подписи также состоит из нескольких этапов:

1) формируется хэш-значение полученного сообщения;

2) осуществляется проверка цифровой подписи;

3) выносится решение о подлинности ЭЦП.

В соответствии с перечисленными этапами процессов формирования и проверки ЭЦП программа содержит следующие функциональные блоки:

1) блок хэширования;

2) блок генерации секретного ключа;

3) блок генерации открытого ключа;

4) блок формирования цифровой подписи;

5) блок проверки цифровой подписи.

Учитывая то, что данный программный комплекс предназначен для использования в учебных целях, был разработан блок справочной информации, который содержит краткую информацию по хэш-функции и цифровым подписям, а также задание для лабораторной работы.

Учебный программный комплекс разработан в среде программирования Borland C++ Builder 6.0 и рассчитан на использование операционных систем Windows 98/2000/XP.

Меню учебного программного комплекса состоит из трех пунктов: вычисления, справка и выход.

Пункт меню «Вычисления» содержит следующие опции.

• Вычисление хэш-функции. При выборе данной опции открывается окно «Вычисление хэш-функции» (рис. 1), которое позволяет определить хэш-значение произвольного файла при заданных пользователем начальном хэш-векторе и таблице замен. Полученный результат может быть сохранен в файл. Также пользователь получает информацию о времени хэширования сообщения.

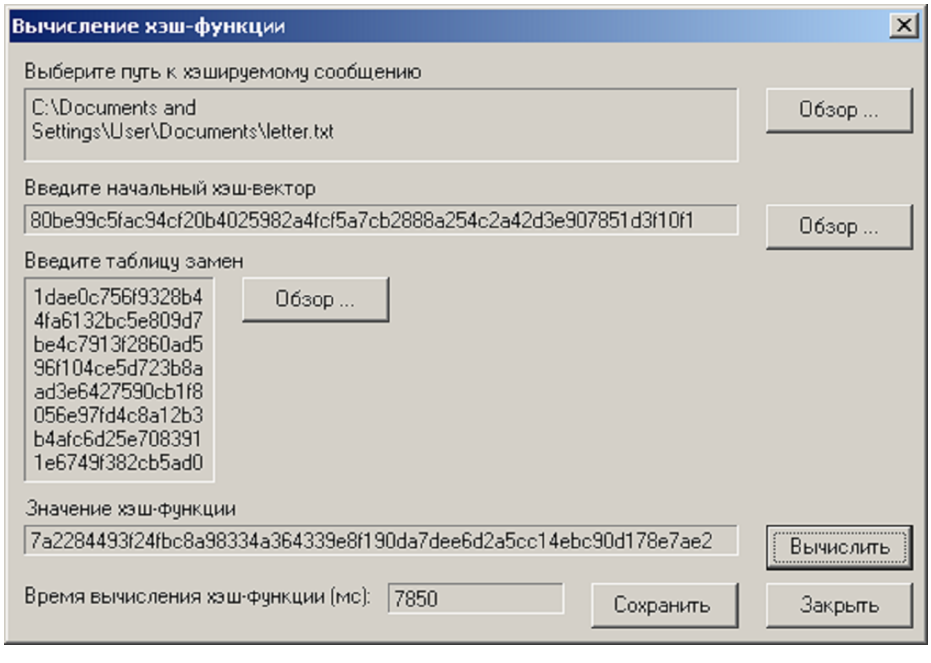

Рис. 1 — Окно «Вычисление хэш-функции»

• Генератор псевдослучайных чисел. При выборе данной опции открывается окно «Генератор псевдослучайных чисел» (рис. 2). Пользователь получает возможность ввести параметры своего генератора, произвести вычисления и сохранить полученный результат в файл.

В качестве генератора псевдослучайных чисел используется функция вида

$$X_{n+1} = (a\,X_n + c) \bmod m,\ n \geq 0, \qquad (1)$$

где X_0 — начальное значение, $X_0 \geq 0$; a — множитель, $a \geq 0$; c — приращение, $c \geq 0$; m — модуль, $m > X_0$, $m > a$, $m > c$; n — порядковый номер очередного целого числа, порождаемого функцией (1).

Эта функция называется линейной конгруэнтной (совпадающей) последовательностью.

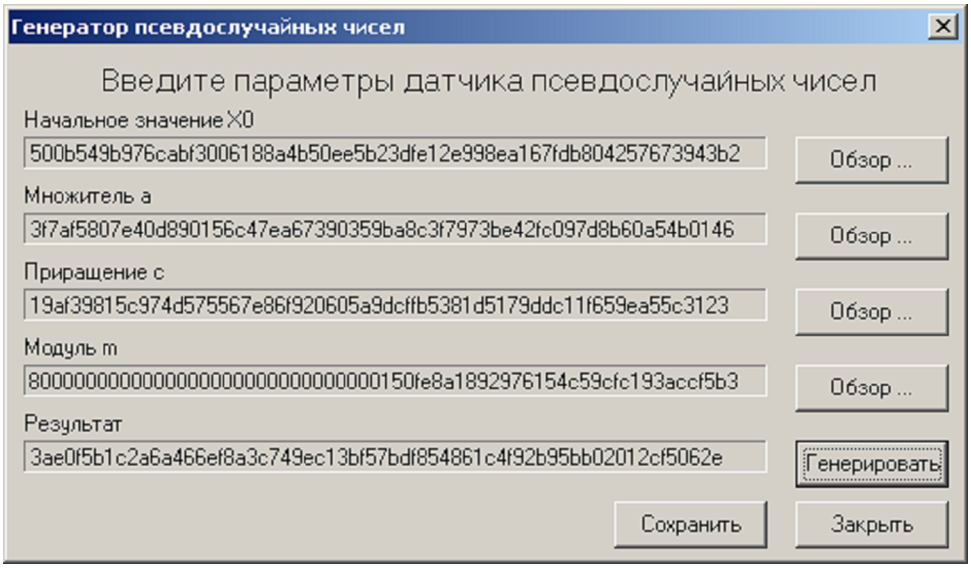

Рис. 2 — Окно «Генератор псевдослучайных чисел»

• Вычисление открытого ключа. При выборе данной опции открывается окно «Вычисление открытого ключа» (рис. 3). Пользователь получает возможность вычислить открытый ключ для имеющегося у него секретного ключа и параметров схемы ЭЦП.

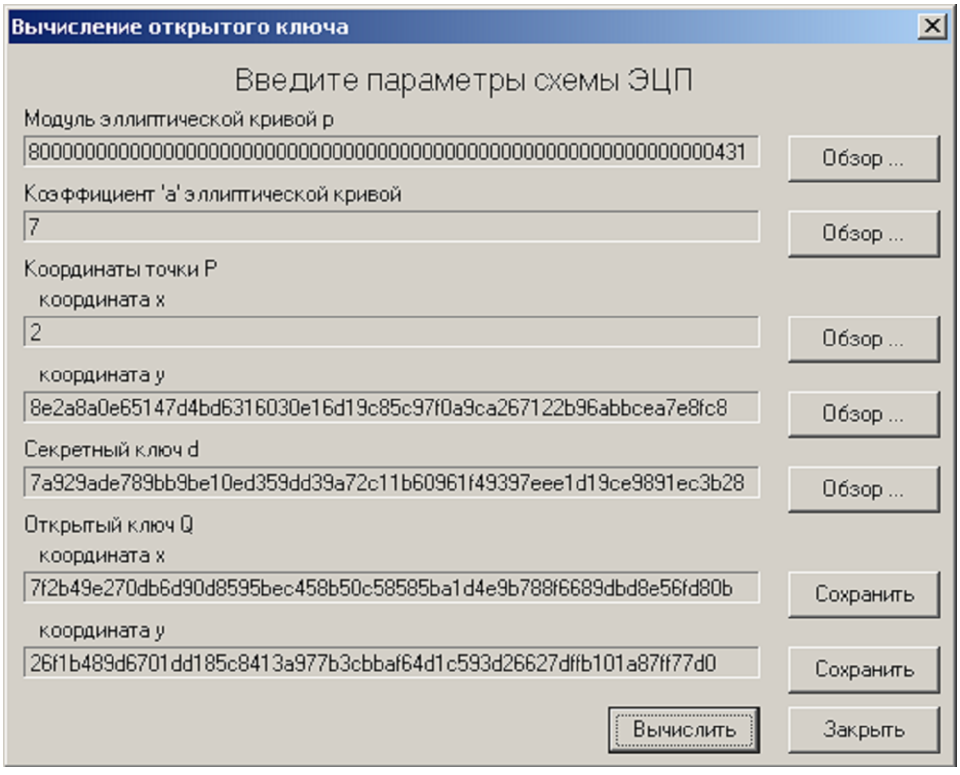

Рис. 3 — Окно «Вычисление открытого ключа»

• Формирование ЭЦП. При выборе данной опции открывается окно «Формирование ЭЦП» (рис. 4). Пользователь получает возможность после ввода всех необходимых для расчетов параметров вычислить цифровую подпись и сохранить полученный результат в файл.

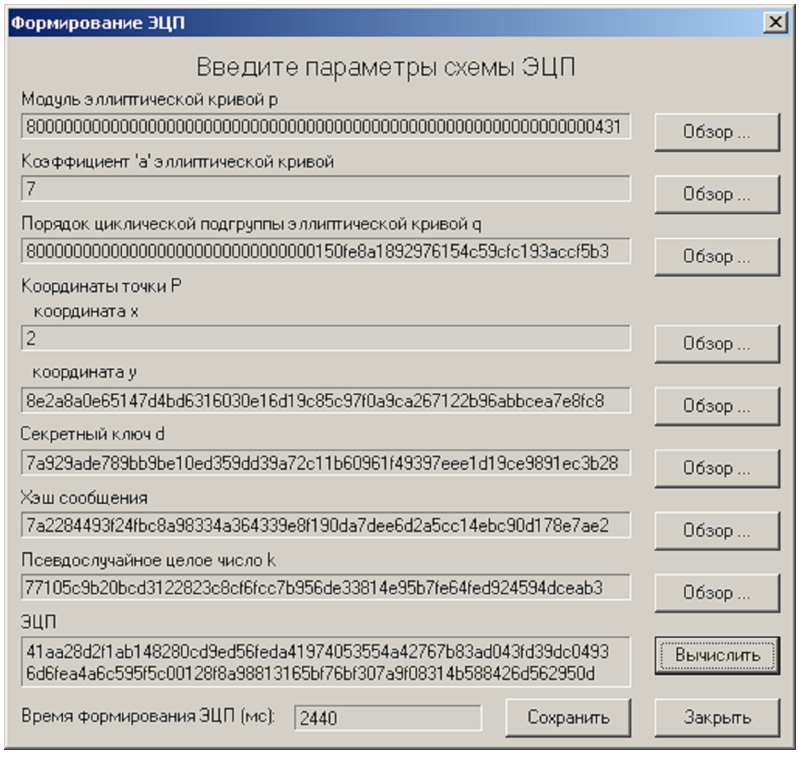

Рис. 4 — Окно «Формирование ЭЦП»

• Проверка ЭЦП. При выборе данной опции открывается окно «Проверка ЭЦП» (рис. 5). Пользователь получает возможность после ввода всех необходимых для расчетов параметров проверить подлинность цифровой подписи.

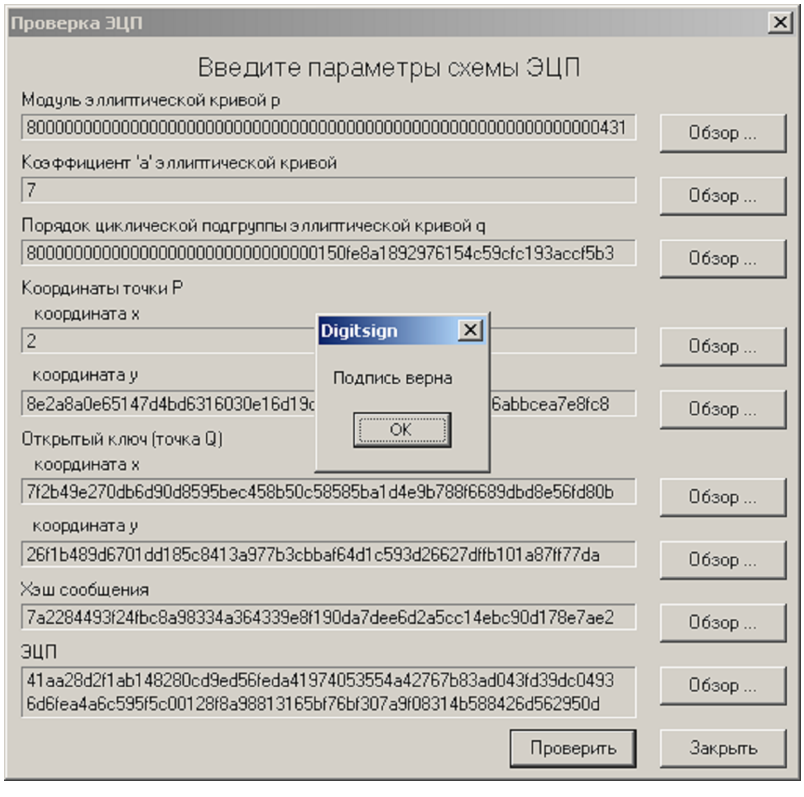

Рис. 5 — Окно «Проверка ЭЦП»

Пункт меню «Справка» содержит следующие опции.

- Задание на лабораторную работу.
- Справка.
- О программе.

Разработанный учебный программный комплекс может быть использован для проведения лабораторных работ для студентов специальности 075600 «Информационная безопасность телекоммуникационных систем» по дисциплинам «Программно-аппаратные средства обеспечения информационной безопасности» и «Криптографические методы защиты информации».

Литература

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.

Игоничкина Екатерина Викторовна
Ассистент кафедры радиотехнических систем ТУСУРа
Телефон: (3822) 41 35 59
E-mail: iev109@mail.ru

E.V. Igonichkina
Educational programm complex for learning of the domestic standards of function of hashing and digital signature

In the article the review of algorithms of a digital signature is adduced. The description of an educational program complex for learning domestic standards function of hashing GOST R 34.11-94 and the digital signature GOST R 34.10-2001 is resulted.

УДК 570.8

М.Ю. Катаев, А.В. Лончин, А.В. Мардяшов

Программная система моделирования и обработки данных сканирующего пассивного фурье-спектрометра

В статье приводится описание программы, предназначенной для расчета спектра излучения атмосферы на горизонтальных трассах с помощью сканирующего пассивного Фурье-спектрометра.

Введение

Как известно, в настоящее время экология атмосферы привлекает огромное внимание человечества ввиду интенсивного развития промышленности и увеличения количества транспорта. Для предотвращения экологических загрязнений необходимо знание различных атмосферных характеристик, получение которых, как правило, требует применения сложных промышленных технологий или дорогостоящих измерительных приборов.

Со времен Ньютона оптическая спектроскопия всегда была одним из самых информативных методов исследования вещества. За прошедшее время способы регистрации излучения посредством оптической спектроскопии существенно модернизированы. Однако принципы построения спектральных приборов до середины XX века практически не менялись. Большинство приборов традиционно строили по одной и той же схеме: излучение фокусируется на входную щель прибора, прошедшее излучение параллельным пучком направляется на диспергирующий элемент (долгое время это была призма, в XX веке она стала заменяться на дифракционную решетку) и после фокусировки на выходной щели излучение регистрируется каким-либо приемником излучения. На данный момент выделяются два основных метода анализа экологической ситуации городов (промышленных зон), основанных на применении лазерных систем, — активный и пассивный. В отличие от пассивных, активные