УДК 004

РАЗРАБОТКА ВИРТУАЛЬНОЙ ЛАБОРАТОРИИ «АСИММЕТРИЧНЫЙ АЛГОРИТМ ШИФРОВАНИЯ RSA» ДЛЯ СИСТЕМЫ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

Кичаев Евгений Андреевич
магистрант
Сидоров Дмитрий Петрович
кандидат технических наук
Мордовский государственный университет им. Н.П. Огарёва, Саранск
author@apriori-journal.ru

Аннотация. В статье рассматривается создание виртуальной лаборатории по дисциплине «Защита информации» для системы дистанционного образования. Тематика представленной разработки посвящена асимметричному алгоритму шифрования RSA. Программа является Windows приложением, которое в удобной форме отображает всю последовательность вычислений, необходимых для шифрования по алгоритму RSA.

Ключевые слова: виртуальная лаборатория, дистанционное образование, алгоритм, RSA, шифрование, криптография.

THE DEVELOPMENT OF VIRTUAL LABORATORY «RSA ASYMMETRIC ENCRYPTION ALGORITHM» FOR DISTANCE EDUCATION

Kichaev Evgeny Andreyevich
undergraduate
Sidorov Dmitry Petrovich
candidate of technical sciences
Mordovian state university of N.P. Ogaryov, Saransk

Abstract. The article deals with the creation of a virtual laboratory on discipline «Information Security» for the distance education system. Topics presented devoted to the development of an asymmetric encryption algorithm RSA. The program is a windows application that is in a convenient form displays the entire sequence of computations necessary for encryption algorithm RSA.

Key words: virtual laboratory, distance education, algorithm, RSA, encryption, cryptography.

В XXI веке массовое распространение компьютеров и развитие сетевых технологий сделало возможным внедрение системы дистанционного образования. Интернет стал огромным прорывом, появилась возможность общаться и получать обратную связь от любого студента, где бы он ни находился. Распространение «быстрого интернета» дало возможность использовать онлайн семинары (вебинары) для обучения. Таким образом популярность дистанционного образования продолжает расти, активно развиваются новые направления и методики обучения. Все больше ВУЗов вводят в учебную программу поддержку системы дистанционного образования [7].

Для реализации возможности дистанционного обучения необходимо обеспечить студентов всем необходимым учебным материалом и реализовать возможность дистанционного выполнения лабораторных работ по предметам учебного плана. Для этого разрабатываются электронные приложения, максимально приближенные к реальным лабораторным работам и точно повторяющие все условия при их выполнении в интерактивном виде, а также наглядно показывающие и поясняющие все стороны и этапы этих лабораторных работ. Например, такой подход отражен в [3].

Именно с этой целью было разработано приложение «Виртуальная лаборатория: Асимметричный алгоритм шифрования RSA», реализующее функционал лабораторной работы по соответствующей теме дисциплины «Защита информации» [4; 5]. Программа представляет собой Windows приложение, основные функции которого, наглядно представлены в диаграмме прецедентов (рис. 1).

Здесь можно выделить несколько основных функций. Прежде всего, это сам лабораторный практикум, наглядно разъясняющий работу алгоритма на простых примерах. Изучение разбито на этапы, соответствующие этапам настоящего алгоритма шифрования. Каждый этап сопровождается развернутым пояснением его особенностей и советами по

выбору тестовых данных. На рис. 2 представлен вариант изучения одного из этапов алгоритма.

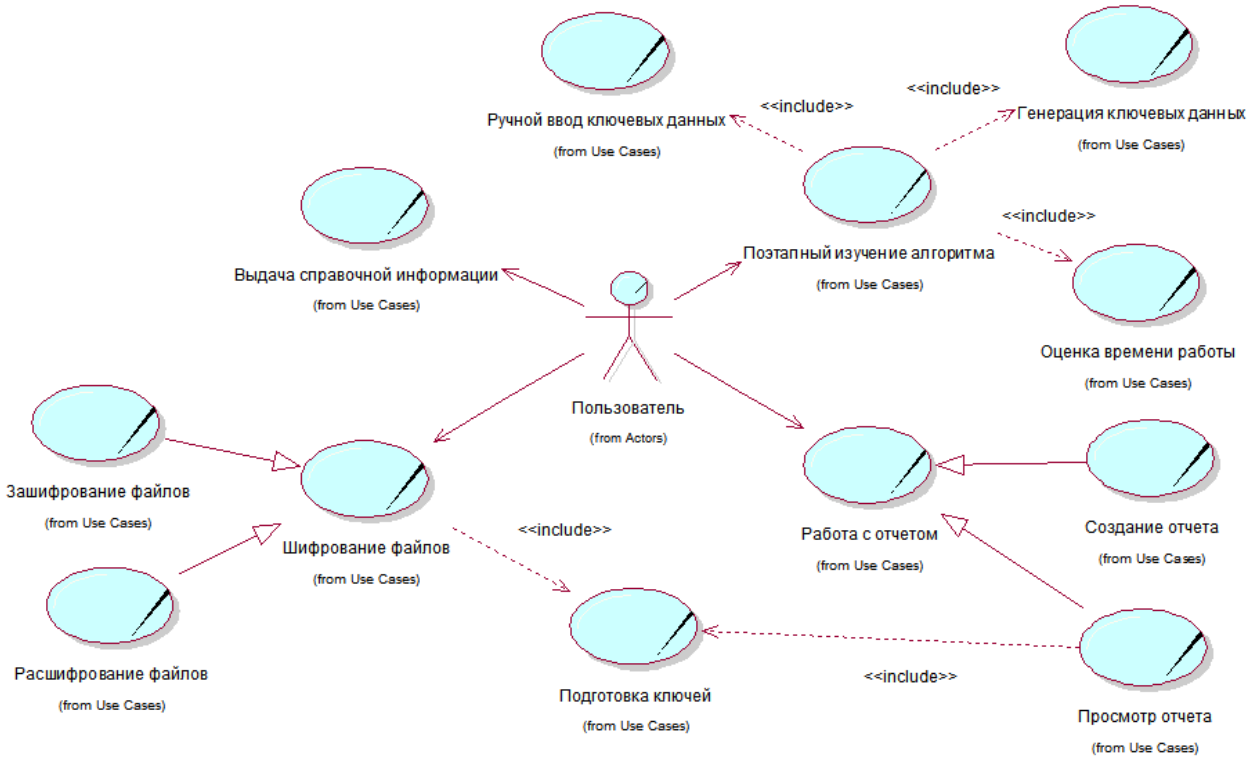

Рис. 1. Диаграмма прецедентов

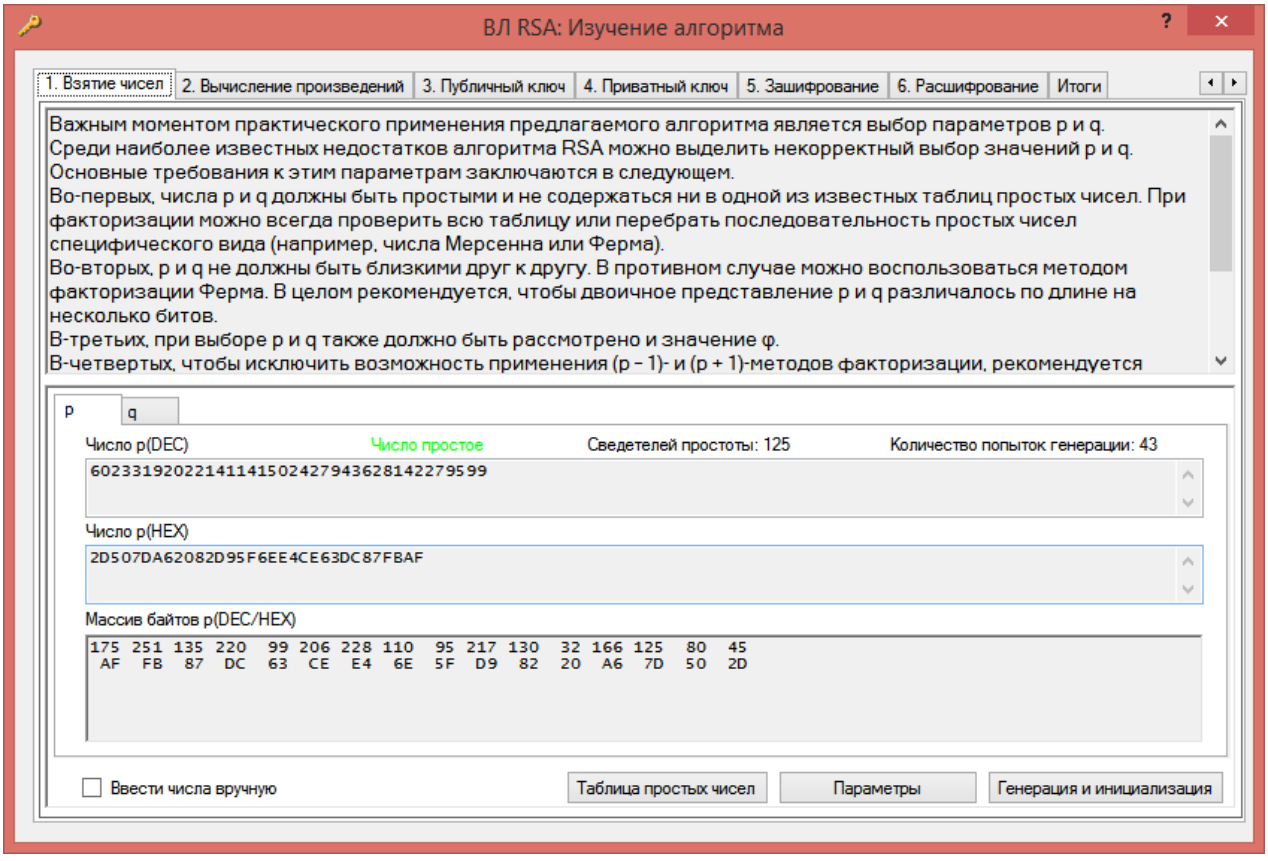

Рис. 2. Окно изучения алгоритма

Следующей функцией является работа с отчетами. По окончании изучения алгоритма пользователю предоставляется возможность сохранить файл отчета о проделанной работе для его дальнейшей передачи преподавателю. Он может быть открыт для просмотра средствами этого же приложения (рис. 3).

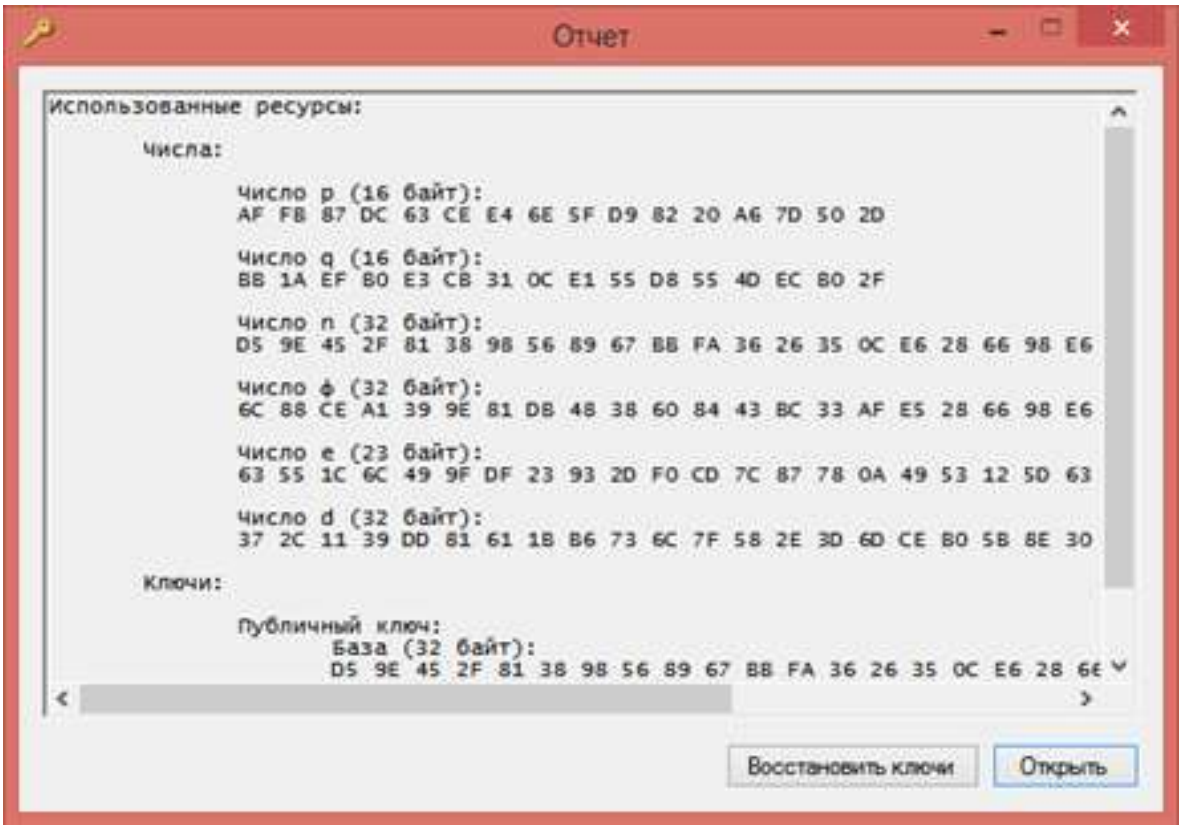

Рис. 3. Форма отчета

Так же одной из важнейших функций приложения является предоставления полного систематизированного теоретического материала по изучаемому предмету. Вся информация в удобной форме собрана в специальный справочник, реализованный по типу файлов справки. Данный подход хорош тем, что студенту не придется искать информацию по интересующему его вопросу в сторонних источниках. Он может получить ее сразу, не отвлекаясь от изучения предмета. Важной особенностью справочной системы является быстрый и удобный поиск как по наименованиям разделов и глав, так и по ключевым словам.

Поскольку в данном практикуме рассматривается алгоритм шифрования, в приложение была добавлена возможность зашифрования и расшифрования файлов, и соответственно, возможность генерации открытых (public) и закрытых (private) ключей. Этот функционал может оказаться полезным тем, кто не хочет тратить время на поиск программ для шифрования. Это так же дает возможность показать студентам практическое применение изучаемого алгоритма шифрования. На рис. 4 показан пример шифрования файла.

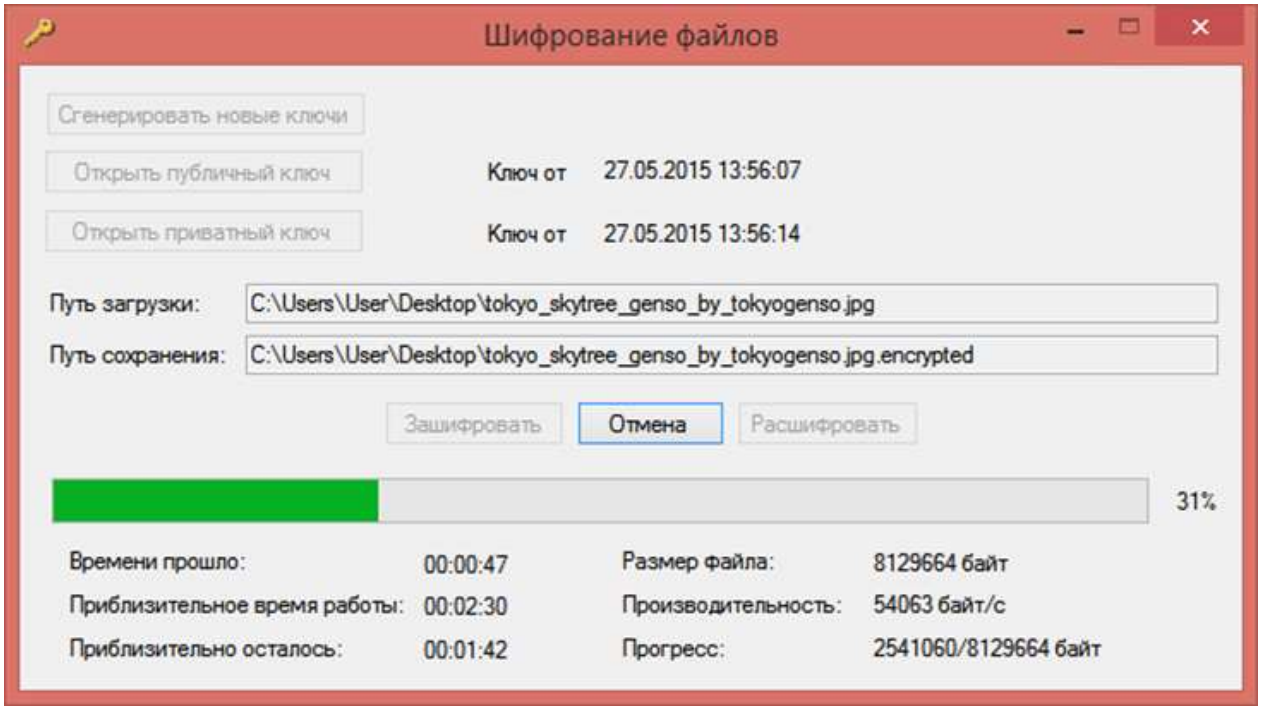

Рис. 4. Окно шифрования файлов

Стоит уделить некоторое внимание внутренней структуре приложения. Оно реализовано на программной платформе .NET Framework на объектно-ориентированном языке программирования C# [1; 2].

Особенностью реализации данного алгоритма является то, что хотя сам по себе он относительно простой, но требует для своей работы некоторые вспомогательные алгоритмы, такие как стандартный и расширенный алгоритмы Евклида, алгоритм теста Миллера-Рабина на простоту чисел, бинарный алгоритм возведения в степень чисел по модулю, а

также алгоритмы генерации больших простых чисел [6]. На рис. 5 представлена диаграмма классов разработанного приложения.

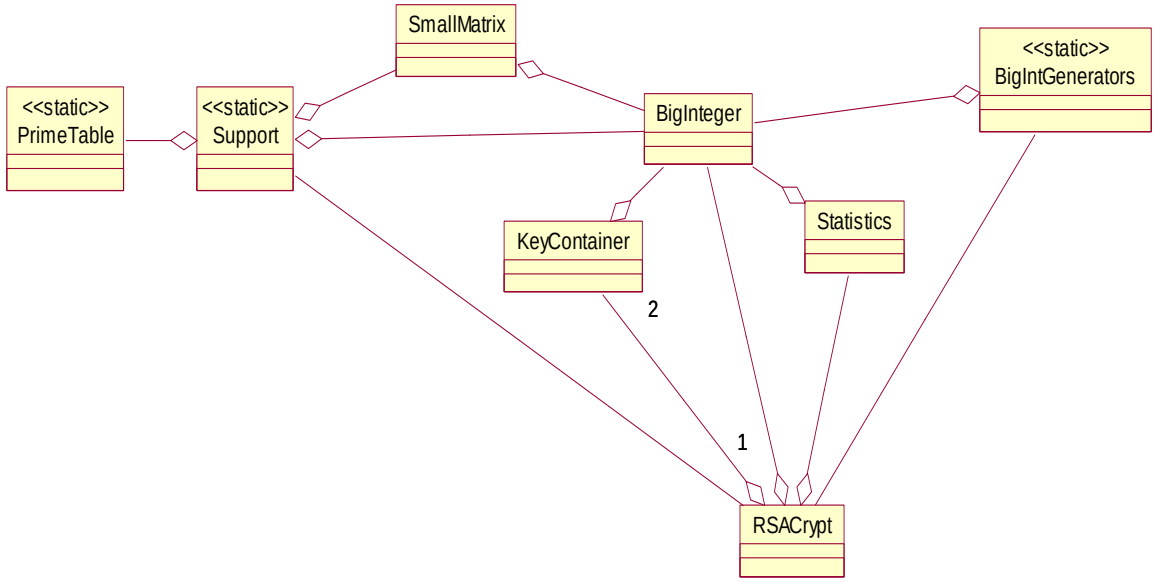

Рис. 5. Диаграмма классов приложения

Класс BigInteger лежит в основе алгоритма шифрования, поэтому он находится на самом нижнем уровне реализации, что отражено связями агрегации. Стоит отметить, что качественная реализация данного класса «с нуля» требует значительных временных затрат, в противном случае он не будет отличаться хорошим быстродействием по сравнению с готовым классом, взятым из библиотеки. По этим причинам реализация класса BigInteger была импортирована из существующей библиотеки.

Верхний уровень реализации представлен классом RSACrypt, что так же отражено связями агрегации.

Класс KeyContainer служит, как следует из названия, для хранения ключей и работы с ними. В алгоритме используются два ключа – публичный и приватный. Соответственно кратность связи этого класса с классом RSACrypt – два к одному.

Класс Support является вспомогательным статическим классом, содержащим параметры настроек приложения, а также вспомогательные

алгоритмы, необходимые для работы алгоритма шифрования RSA, о которых говорилось выше.

Класс SmallMatrix был реализован для расширенного алгоритма Евклида, использующего умножение матриц.

Класс PrimeTable содержит таблицу простых чисел в диапазоне от 1 до 10 000. Поскольку тест Миллера-Рабина является вероятностным, его работа с малыми числами может содержать серьезные погрешности. Дабы избежать подобной проблемы, был реализован данный класс.

Класс BigIntGenerators служит контейнером для методов генерации больших простых чисел.

Класс Statistics содержит в себе всю статистическую информацию, собираемую при изучении работы алгоритма и отражаемую в отчете.

Таким образом, студент помимо изучения алгоритма шифрования RSA захватывает достаточно большой пласт информации, занимаемый вспомогательными алгоритмами, знать устройство и работу которых необходимо для понимания основного алгоритма. Более того, подобные знания приветствуются в таких отраслях как программирование и оптимизация программного кода.

В заключение нужно отметить, что данное приложение и направление в целом имеет довольно большой потенциал. На данный момент на основе созданного приложения уже ведутся исследования и работы по дальнейшему его развитию: разработка полноценной программной платформы, поддерживающей модульность и расширяемость; реструктуризация отчетов для увеличения их информативности; организации клиент-серверной архитектуры приложения; разработки тестового комплекса для студентов.

Список использованных источников

1. Александров Э.Э. Введение в программирование на языке С: учеб. пособие / Э.Э. Александров, В.В. Афонин. Саранск: Изд-во Мордов. ун-та, 2009. 316 с.
2. Александров Э.Э., Афонин В.В., Программирование на языке С в Microsoft Visual Studio 2010. [Электронный ресурс]. Режим доступа: http://www.intuit.ru/department/pl/prcmsvs2010
3. Афонин В.В., Федосин С.А. О структурировании лабораторно-практических занятий при изучении дисциплин программирования // Образовательные технологии и общество. 2014. Т. 17. № 4. С. 497-506. [Электронный ресурс]. Режим доступа: http://ifets.ieee.org/russian/depository/v18_i2/pdf/5.pdf (дата обращения 20.10.2015).
4. Классические симметричные шифры: метод. указания к лаборатор. работам по курсу «Методы и средства защиты компьютерной иноформации» / сост.: Д.П. Сидоров, В.В. Афонин; под общ. ред. проф. С.А. Федосина. Саранск: Изд-во Мордов. ун-та, 2010. 56 с.
5. Современные симметричные криптосистемы и хэш-функции: метод. указания к лаборатор. работам по курсу «Методы и средства защиты компьютерной иноформации» / сост.: Д.П. Сидоров, В.В. Афонин; под общ. ред. проф. С.А. Федосина. Саранск: Изд-во Мордов. ун-та, 2011. 68 с.
6. Федосин С.А. Методы и средства защиты компьютерной информации: учеб. пособие / С.А. Федосин. Саранск: Изд-во Мордов. ун-та, 2005. 112 с.
7. Панфилов С.А., Аббакумов А.А. Информационная поддержка управления качеством образовательной деятельности // Образовательные технологии и общество. 2015. Т. 18. № 2. С. 472-477. [Электронный ресурс]. Режим доступа: URL:http://cyberleninka.ru/article/n/o-strukturirovanii-laboratorno-prakticheskih-zanyatiy-pri-izuchenii-distsiplin-programmirovaniya (дата обращения 20.10.2015).