РАЗРАБОТКА ЛАБОРАТОРНОЙ РАБОТЫ НА ТЕМУ «ДОКАЗАТЕЛЬСТВО С НУЛЕВЫМ ЗНАНИЕМ»

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

Н. В. Пенкрат, П. А. Мазалев

Е. В. Николаенко – ст. преподаватель

Разработана лабораторная работа на тему «Доказательство с нулевым знанием», включающая соответствующее программное обеспечение и методические указания

Выполнение обучающимися и студентами лабораторных и практических работ формирует учебно-аналитические умения, способствует обобщению и систематизации теоретических знаний. Ведущей дидактической целью лабораторных работ является экспериментальное подтверждение и проверка существенных теоретических положений учебной дисциплины. При изучении криптографических алгоритмов, использующих для доказательства подлинности участников процедуру доказательства с нулевым знанием, целесообразно проведение лабораторной работы. Следовательно, необходимо интуитивно понятное программное обеспечение, позволяющее экспериментально проверить методику расчета, проводимого в рамках процедуры доказательства с нулевым знанием.

Программа для исследования работы алгоритмов доказательства подлинности с нулевым знанием написана на языке C++ (рисунок 1). Объем загрузочного модуля программы – 500 кБ. Программа работает с операционной системой Windows XP и выше. Архитектура процессора − x86. Объем оперативной памяти – 2МБ. Программа позволяет вести журнал расчетов результатов выполнения лабораторной работы для каждого студента (рисунок 2).

В рамках лабораторной работы предлагается рассмотреть три алгоритма доказательства с нулевым знанием − алгоритм Фиата-Шамира, Гиллу-Кискатра и Шнорра (рисунок 3).

В поля, доступные для редактирования, необходимо ввести значения, согласно допустимым диапазонам (указаны в соответствующем разделе справки, которая вызывается по нажатию кнопки «Помощь») − рисунок 4.

Тогда в полях, недоступных для редактирования, после нажатия кнопки «Рассчитать» отобразятся результаты работы алгоритма. В противном случае отобразится сообщение о соответствующей ошибке (рисунок 5).

Рис. 1 – Окно загрузки программы

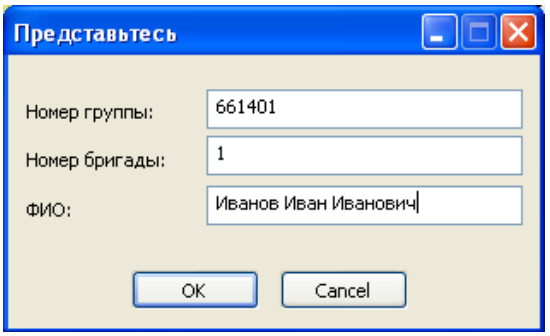

Рис. 2 – Окно идентификации студента

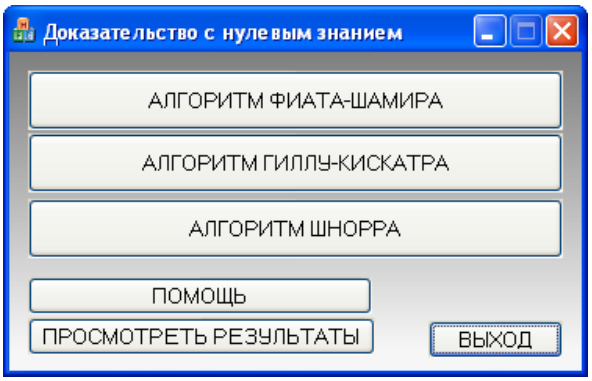

Рис. 3 – Окно выбора алгоритма

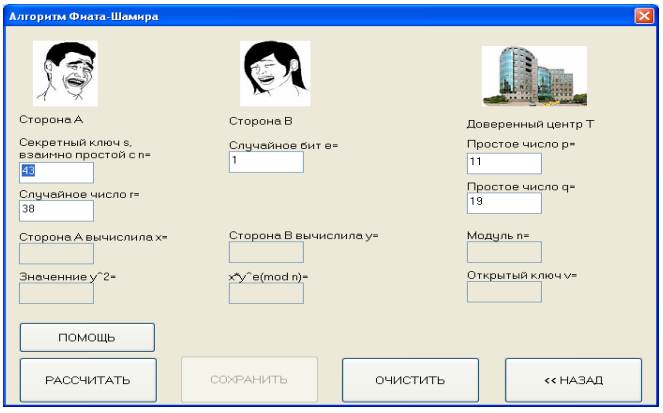

Рис. 4 − Окно ввода значений

Для занесения результатов выполнения алгоритма в отчет необходимо нажать кнопку «Сохранить» и в отобразившемся диалоговом окне задать имя файла, в котором будет сохранен отчет. При работе с программой существует возможность «дописывания» файла отчета. Просмотреть отчет можно, нажав кнопку «Просмотреть результаты» (рисунок 6).

Методические указания к выполнению лабораторной работы включают теоретические сведения, инструкции по работе с программой, рекомендации по оформлению отчета, контрольные вопросы. Контрольные вопросы составлены по принципу «от простого к сложному». Так, например, одним из вопросов первого уровня является вопрос: «Дайте определение понятия -идентификация‖». В качестве примера более сложных вопросов: «Докажите, что алгоритм Фиата-Шамира обладает всеми тремя свойствами доказательства с нулевым знанием» либо «Составьте блок схему алгоритма Шнорра».

В результате разработки лабораторной работы создан комплекс, включающий методические указания и программное обеспечение, необходимый для качественного усвоения студентами темы «Доказательство с нулевым знанием».

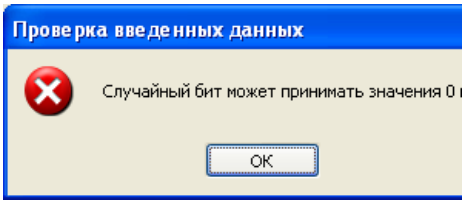

Рис. 5 − Сообщение об ошибке

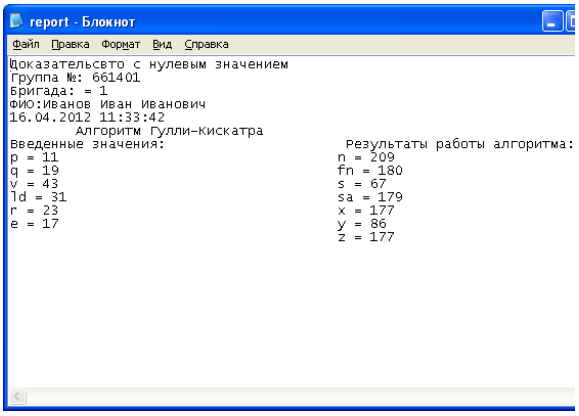

Рис. 6 – Отчет о выполнении лабораторной работы

Список литературы

1. Голиков, В. Ф. Криптографическая защита информации в телекоммуникационных системах / В. Ф. Голиков, А. В. Курилович. – Мн. : БГУИР, 2006. – Ч. 1. – с. 55. – Ч. 2. – с. 55.

2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. − 816 с.