ПРИМЕНЕНИЕ ПРИКЛАДНЫХ ПРОГРАММ УЧЕБНОГО НАЗНАЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ БУДУЩЕГО БАКАЛАВРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рычкова А.А., Гайфулина Д.А., Хакимова Э.Р.
ФГБОУ ВО «Оренбургский государственный университет», г. Оренбург

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность для формирования профессиональных компетенций (ПК-1, ПК-2) необходимо расширение учебно-методического и материально-технического обеспечений учебного процесса [1].

В процессе изучения дисциплины базового цикла «Криптографические методы защиты информации» на практических и лабораторных занятиях кроме изучения готовых криптографических программных средств будущие бакалавры выполняют исследование и разработку собственных программ.

В статье рассматривается опыт разработки и использования прикладной программы учебного назначения в ходе организации лабораторных работ по разделу «Криптографические протоколы».

Прикладная программа «Исследование криптографических методов формирования электронной подписи» предназначена для проверки подлинности отправляемых сообщений пользователями на основе электронной подписи [2]. Основными направлениями работы являются нахождение хеш-функции от отправляемого сообщения, вычисление электронной цифровой подписи отправителя и получателя на основе различных алгоритмах шифрования, а так же подтверждение или отклонение подлинности сообщения. В основе программы лежат алгоритмы формирования электронной подписи на основе таких алгоритмов шифрования как RSA, El Gamal, алгоритмы Диффи-Хеллмана и Фиата-Шамира, а та же алгоритмы вычисления хеш-функций и основы работы в среде «клиент-сервер». В программе предусмотрено наличие:

– теоретического материала по используемым алгоритмам формирования электронной подписи;

– графического представления происходящего процесса передачи сообщения и всех математических преобразований, происходящих в ходе формирования и передачи электронной подписи, а так же ее проверки;

– последовательность этапов формирования электронной подписи.

Список представленных алгоритмов формирования электронной подписи можно увидеть на левой панели программы или во всплывающем меню перейдя по вкладке «Режимы работы». В данном всплывающем меню имеются теоритические сведения об алгоритмах, а так же можно перейти к реализации, выбрав соответствующий тип алгоритма формирования электронной подписи. Главное окно программы показано на рисунке 1.

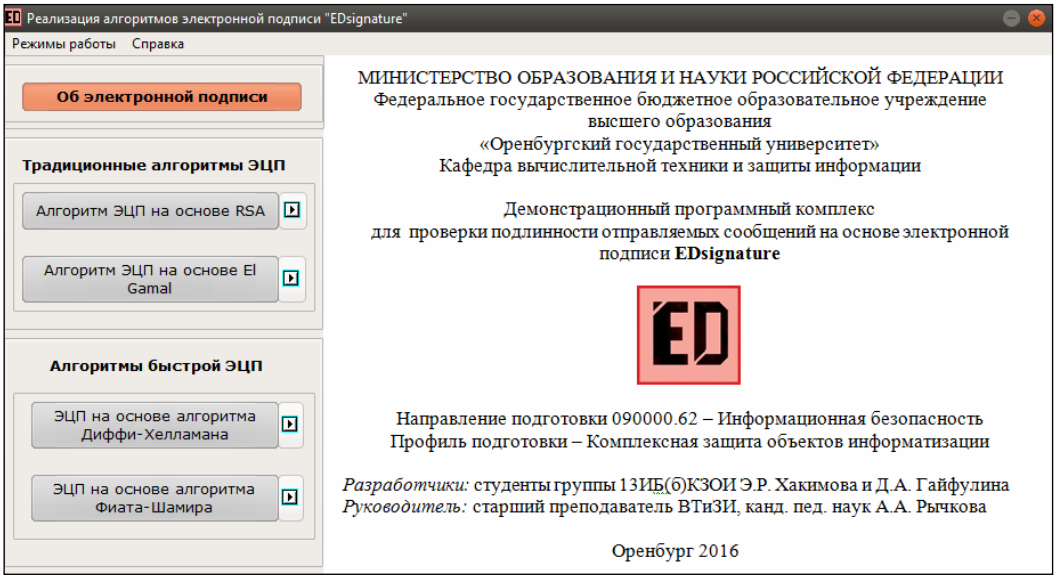

Рисунок 1 – Главное окно программы «EDsignature»

Для выбора определенного алгоритма формирования электронной подписи следует нажать на кнопку на левой панели или на соответствующую строку во всплывающем меню.

При нажатии на кнопку любого алгоритма формирования электронной подписи появляется окно программы, содержащее теорию по данному алгоритму формирования. Данное окно программы для режима формирования электронной подписи на основе алгоритма RSA представлено на рисунке 2.

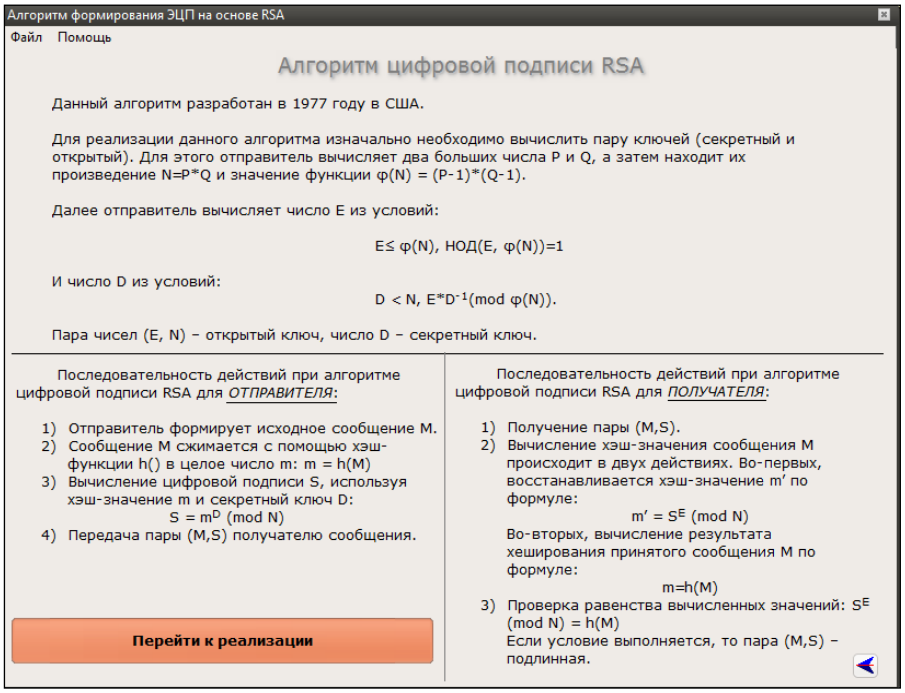

Рисунок 2 – Окно программы «Алгоритм формирования электронной подписи на основе RSA»

Исходными данными для программы являются передаваемое сообщение и криптографический ключ (элементы для формирования ключа).

Для начала работы с программным средством необходимо изначально установить соединение между клиентом и сервером для последующей передачи сообщений и формирования электронной подписи.

Для использования в учебном процессе в программе представлена реализация следующих алгоритмов:

ЭЦП на основе алгоритма RSA. Формирование ключей производится на основе введенных параметров p, q которые должны быть простыми. Пара чисел (e, n) – открытый ключ, число d – секретный ключ. Формирование ЭЦП отправляемого сообщения основано на применении асимметричного метода RSA, где в качестве ключей используются параметры {e, n} – являющиеся закрытыми ключами шифрования. На выходе получают ЭЦП, представленную в виде значения чисел {M,S}, которые передаются получателю. Клиент производит проверку ЭЦП полученного сообщения на основе асимметричного метода RSA, где в качестве ключей используются параметры {d, n} – являющиеся открытыми ключами шифрования, переданными клиенту сервером. На выходе получают строку расшифрованного хэша сообщения, который впоследствии сравнивается с вычисляемым хэшем полученного сообщения. По результатам сравнения делается вывод о подлинности отправителя.

ЭЦП на основе алгоритма El Gamal. Для реализации данного алгоритма изначально необходимо вычислить пару ключей с использованием больших простых целых чисел P, G и X. Число Y – закрытый ключ, X – открытый ключ. Сервер производит формирование ЭЦП отправляемого сообщения на основе асимметричного метода Эль Гамаль, с использованием в качестве входных параметров отправляемого сообщения и ключа Y. На выходе получают ЭЦП, представленную в виде значения чисел {a, b}, которые передаются получателю. Клиент производит проверку ЭЦП полученного сообщения на основе асимметричного метода Эль Гамаль, где в качестве ключей используются параметр X. На выходе получают строку расшифрованного хэша сообщения, который впоследствии сравнивается с вычисляемым хэшем полученного сообщения. По результатам сравнения делается вывод о подлинности отправителя.

Быстрая ЭЦП на основе алгоритма Диффи-Хеллмана. Изначально происходит генерация ключа. Пользователь выбирает случайный секретный ключ x и вычисляет открытый ключ y с использованием генератора абелевой группы G. Сервер производит формирование быстрой ЭЦП отправляемого сообщения на основе алгоритма Дифии-Хеллмана, входными параметрами является отправляемое сообщение и ключ x. На выходе получают быструю ЭЦП, представленную в виде значения чисел {M, S}, которые передаются получателю. Клиент производит проверку ЭЦП полученного сообщения на основе метода Диффи-Хеллмана, где в качестве ключей используются параметр

y. На выходе по результатам сравнения принимается решение о подлинности отправителя.

Быстрая ЭЦП на основе алгоритма Фиата-Шамира. До начала создания подписи происходит генерация ключей. В качестве секретного ключа выбирается последовательность s=(s1,…,sk), состоящий из случайных чисел si. На основе закрытого ключа считается открытый ключ: формируется последовательность v = (v1,…,vk). Далее сервер производит формирование быстрой ЭЦП отправляемого сообщения на основе алгоритма Фиата-Шамира, входными параметрами является отправляемое сообщение и ключевая последовательность s. На выходе получают быструю ЭЦП, представленную в виде значения чисел {M, S}, которые передаются получателю. Клиент производит проверку ЭЦП полученного сообщения на основе метода Фиата-Шамира, где в качестве ключей используется открытая последовательность v. На выходе по результатам сравнения принимается решение о подлинности отправителя [3-7].

При выборе любого из предложенных алгоритмов результатом выполнения программы будет являться вывод сообщения о подтверждении или отклонении подлинности отправителя. На рисунке 3 представлено окно программы при подтверждении подлинности отправителя.

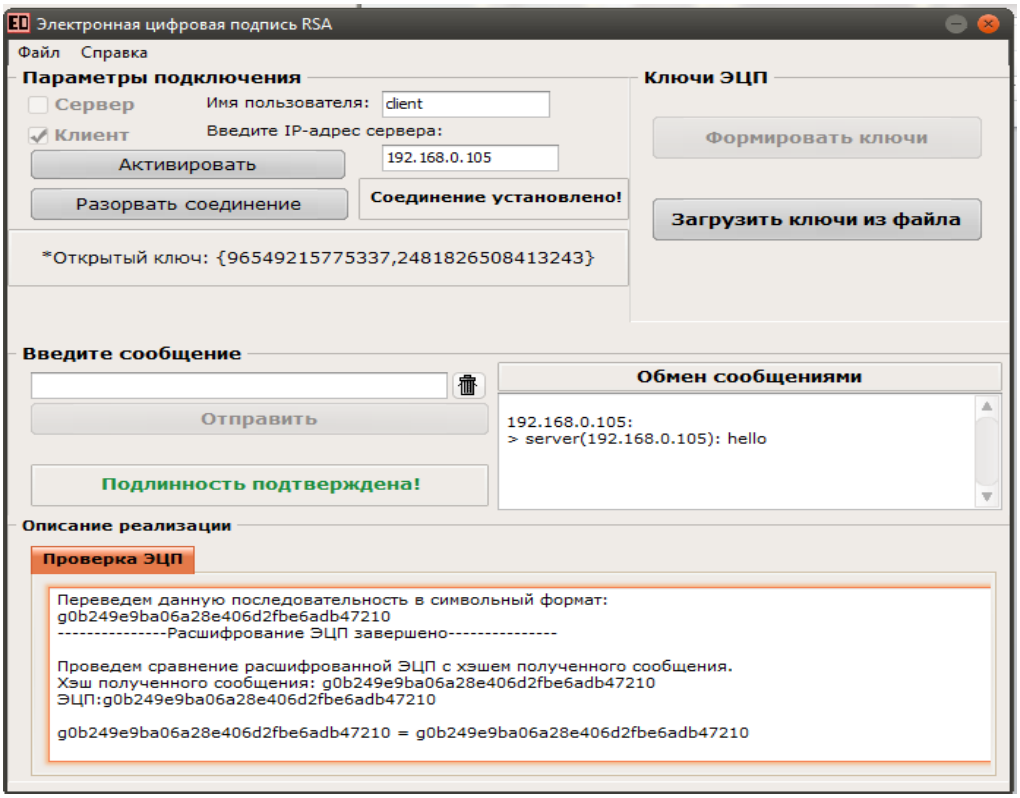

Рисунок 3 – Подтверждение подлинности отправителя сообщения

В результате выполнения лабораторной работы с помощью разработанной прикладной программы «Исследование криптографических методов формирования электронной подписи» будущие бакалавры по

информационной безопасности самостоятельно изучают существующие алгоритмы электронной подписи, проводят сравнительный анализ быстродействия выбранных методов, делают выводы, подготавливают отчет о проделанной работе. Активное вовлечение студентов в процесс разработки авторских прикладных программ учебного назначения, полученные в ходе выполнения лабораторных работ с применением таких средств, знания и умения способствуют формированию необходимых профессиональных компетенций.

Список литературы

1. Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата): Приказ от 1 декабря 2016 г. № 1515 // Зарегистрирован в Минюсте России 20.12.2016 № 44821/

2. Гайфулина, Д.А. Исследование криптографических методов формирования электронной подписи : прикладная программа / Д.А. Гайфулина, Э.Р. Хакимова, А.А. Рычкова. – Оренбург.: УФЭР. – 2016. - №1332.

3. Ветров, Ю.В. Криптографические методы защиты информации в телекоммуникационных системах: учеб. пособие / Ю.В. Ветров, С.Б. Макаров - Спб.: Изд=во Политехн. ун-та, 2010. - 174 с. - ISBN 978-5-7422-3025-0.

4. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. / Н.А. Молдовян - СПб.: БХВ-Петербург, 2010. - 304 с. - ISBN 978-5-9775-0585-7.

5. Рычкова, А.А. Разработка и применение прикладных программ учебного назначения для организации самостоятельной работы студентов / А.А. Рычкова : сборник научных статей Всероссийской научно-методической конференции «Университетский комплекс как региональный центр образования, науки и культуры»; Оренбургский гос. ун-т.. – Оренбург: ООО ИПК «Университет», 2014. – С. 3082-3088.

6. Рычкова, А.А. Основы криптографии : мультемедийное учебное пособие / Т.Н. Шалкина, В.В. Запорожко, А.А. Рычкова. - М.: ОФАП. - 2008. - №10602.

7. Тимошин П.А, Перспективы развития и использования систем электронной цифровой подписи / П.А. Тимошин - Прикладная информатика, вып. №2(8) - М.:ЛитРес, 2014. - С.12-26. - ISBN 978-5-4573-8888-8.