Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Система цифровых денег

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Беззуба Дмитрия Владимировича

Научный руководитель

доцент, к.ф.-м.н. _____ А.В. Жаркова

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

Со времён создания Интернета всё больше и больше людей было привлечено удобствами, которые он предоставляет. Интернет соединил миллионы людей по всему свету и дал бизнесу возможность предоставлять свои продукты, даже если продавец находится в тысяче километров от покупателя. С течением времени Интернет стал неотъемлемой частью повседневной жизни, каждый год создаётся всё больше и больше сервисов, раскрывающих весь потенциал интернета. Один из таких сервисов – цифровые или электронные деньги, которые позволяют людям вести свой бизнес в интернете, они выступают заменой обычным купюрам и монетам, так как те не пригодны для ведения торговли через Интернет.

Наличные деньги нужно постоянно носить с собой, они способствуют распространению микробов, люди могут их украсть у вас. Чеки и кредитные карточки уменьшили количество наличных денег, оборачивающихся в обществе, но полное удаление наличных денег фактически невозможно из-за интересов некоторых влиятельных групп лиц. Чеки и кредитные карточки можно проследить, вы не можете скрыться от того, кому дали деньги. [1]

С другой стороны, чеки и кредитные карточки позволяют людям вторгаться в вашу личную жизнь как никогда прежде. Вы никогда не допустили бы, чтобы полиция всю жизнь ходила за вами по пятам, но полицейские могут проследить ваши финансовые операции. Они могут видеть, где вы покупаете газ, где вы покупаете еду, кому вы звоните по телефону – всё это не отрываясь от своих мониторов. Люди должны уметь защитить свою анонимность, чтобы защитить свои личные тайны.

К счастью, существуют протоколы, которые позволяют использовать заверенные, но неотслеживаемые сообщения, которыми можно пользоваться в качестве цифровых денег.

Целью данной дипломной работы является разработка и реализация системы цифровых денег.

Для достижения поставленной цели требуется решить следующие задачи:

- рассмотреть протоколы работы цифровых денег;
- изучить необходимые алгоритмы и протоколы для реализации системы.

Дипломная работа состоит из введения, 6 разделов, заключения, списка использованных источников и 3 приложений. Общий объём работы – 137 страниц, из них 52 страницы – основное содержание, включая 17 рисунков и список использованных источников из 16 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

1) Основные определения

В первом разделе приведены понятия и определения, которые понадобятся нам при рассмотрении протоколов и алгоритмов, которые будут использоваться в разрабатываемой системе.

2) Функции шифрования

Функции шифрования необходимы как для безопасного обмена сообщениями в системе, так и для реализации некоторых частей протокола цифровых денег. В этом разделе мы рассмотрим основные виды алгоритмов шифрования.

В подраздел 2.1 «Асимметричное шифрование» рассматриваются 2 алгоритма асимметричного шифрования – криптосистема RSA в подразделе 2.1.1 и криптосистема Эль-Гамаля в подразделе 2.1.2, описывается их применение в разрабатываемой системе.

В подразделе 2.2 «Симметричное шифрование» рассматриваются 2 государственных стандарта шифрования. В подразделе 2.2.1 рассматривается стандарт США – алгоритм AES. В подразделе 2.2.2 рассматривается российский стандарт шифрования данных ГОСТ Р 34.12-2015.

3) Функции хэширования

В третьем разделе рассматриваются криптостойкие функции хэширования, которые будут необходимы для безопасной реализации некоторых протоколов, использованных в протоколе цифровых денег.

В подразделе 3.1 рассматривается семейство хэш-функций SHA, которое является стандартом в США. В подразделе 3.2 описывается российский стандарт – функция хэширования ГОСТ Р 34.11-2012.

4) Вспомогательные протоколы

В четвёртом разделе рассматриваются некоторые протоколы, которые будут использованы нами при реализации протокола цифровых денег.

Использование этих протоколов позволяет достичь важных свойств цифровых денег, таких как анонимность, независимость, неотслеживаемость.

В разделе 4.1 описывается протокол вручения битов, рассматриваются некоторые из его реализаций и выбирается более подходящая для нас.

В разделе 4.2 описывается протокол разделения секрета, рассматриваются две его реализации и выбирается более подходящая для нас.

В разделе 4.3 описывается идея протокола слепой подписи и рассматривается её реализация, основанная на криптосистеме RSA.

В разделе 4.4 рассматривается протокол разрезать и выбирать.

В разделе 4.5 описывается протокол цифрового конверта, который мы будем использовать для безопасного обмена сообщениями в системе.

5) Цифровые деньги

В пятом разделе речь идёт непосредственно об алгоритмах цифровых денег. В разделе 5.1 «Общие сведения» описываются преимущества цифровых денег, вводятся некоторые классификации протоколов, описываются основные свойства.

В разделе 5.2 «Протоколы работы цифровых денег» рассматриваются четыре протокола цифровых денег – от базового до усложненного. Описываются плюсы и минусы каждого из них, рассказывается про уязвимости в протоколах. В конце выводится протокол, который будет нами использован при реализации нашей системы.

6) Программная реализация протокола цифровых денег

Автором была разработана и реализована система цифровых денег, позволяющая производить анонимные и неотслеживаемые платежи с использованием протокола, описанного в разделе 5.2. В системе применяется алгоритмы RSA и ГОСТ Р 34.12-2015 для безопасного обмена сообщениями, хэш функция ГОСТ Р 34.11-2012 и ряд вспомогательных криптографических протоколов.

Продукт написан на языке программирования Java версии 8, состоит из серверной и клиентской части. В разделе подробно раскрыто описание работы

приложения, описаны типичные действия пользователя системы, приведены снимки экрана, иллюстрирующие процесс взаимодействия пользователя с разработанной системой.

Завершается работа приложениями, а именно:

- приложение А «Листинг программы-банка»;
- приложение Б «Листинг программы-клиента»;
- приложение В «Листинг общего модуля».

ЗАКЛЮЧЕНИЕ

С развитием сети Интернет люди всё больше стали нуждаться в сервисах, с помощью которых можно тратить и зарабатывать деньги через сеть. Существующие способы оплаты с помощью банковских карт не могут удовлетворить потребности пользователей, которым нужна анонимность при совершении операций. В связи с этим стремительно изучается тема цифровых денег, разрабатываются алгоритмы, которые обладают различными наборами свойств, чтобы удовлетворить все нужды пользователей.

В ходе дипломной работы были рассмотрены некоторые алгоритмы симметричного и асимметричного шифрования, протоколы вручения битов, разделения секрета, слепой подписи, протокол разрезай и выбирай а так же протоколы заверенных, анонимных и неотслеживаемых цифровых денег. В результате проделанной работы была разработана и реализована система цифровых денег, в частности с использованием отечественных стандартов шифрования и функции хэширования. В данной платёжной системе можно проводить операции без непосредственного участия банка, а покупатель анонимен вплоть до момента его мошенничества, которое всегда будет обнаружено банком.

Таким образом, все поставленные задачи были полностью решены, цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Шнайер, Б. Прикладная криптография : протоколы, алгоритмы, исходные тексты на языке Си [Электронный ресурс] / Б. Шнайер. М. : Триумф, 2003. 815 с. Загл. с экрана. Яз. рус.

2 Салий, В. Н. Криптографические методы и средства защиты информации : учеб. пособие [Электронный ресурс] / В. Н. Салий. Саратов, 2015. 43 с. Загл. с экрана. Яз. рус.

3 Мао, В. Современная криптография: теория и практика [Электронный ресурс] / В. Мао. М. : Издательский дом «Вильямс», 2005. 768 с. Загл. с экрана. Яз. рус.

4 Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ (действующая редакция, 2016). Документ опубликован не был. Доступт из справочной правовой системы Консультант Плюс.

5 Бауэр, Ф. Расшифрованные секреты. Методы и принципы криптологии [Электронный ресурс] / Ф. Бауэр. М. : Мир, 2007. 550 с. Загл. с экрана. Яз. рус.

6 Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии [Электронный ресурс] / О. Н. Василенко. М. : МЦНМО, 2003. 328 с. Загл. с экрана. Яз. рус.

7 Основы криптографии : учеб. пособие [Электронный ресурс] / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. М. : Гелиос АРВ, 2002. 480 с. Загл. с экрана. Яз. рус.

8 Ленг, С. Алгебра [Электронный ресурс] / С. Ленг. М. : Мир, 1968. 572 с. Загл. с экрана. Яз. рус.

9 Ишмухаметов, Ш. Т. Математические основы защиты информации : учебно-методическое пособие [Электронный ресурс] / Ш. Т. Ишмухаметов, Р. Х. Латыпов, Р. Г. Рубцова. Казань, 2014. 95 с. Загл. с экрана. Яз. рус.

10 ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)

[Электронный ресурс]. URL: https://tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 30.11.2016). Загл. с экрана. Яз. рус.

1 ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режим работы блочных шифров [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) [Электронный ресурс]. URL: https://www.tc26.ru/standard/gost/GOST_R_3413-2015.pdf (дата обращения: 02.12.2016). Загл. с экрана. Яз. рус.

12 Баричев, С. Г. Основы современной криптографии : учеб. пособие [Электронный ресурс] / С. Г. Баричев, Р. Е. Серов. М. : Горячая Линия – Телеком, 2006. 152 с. Загл. с экрана. Яз. рус.

13 ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Электронный ресурс] // AltEll [Электронный ресурс] : IT Innovation & Security. URL: http://www.altell.ru/legislation/standards/gost-34.10-2012.pdf (дата обращения: 05.12.2016). Загл. с экрана. Яз. рус.

14 ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования [Электронный ресурс] // Спецремонт [Электронный ресурс]. URL: http://specremont.su/pdf/gost_34_11_2012.pdf (дата обращения: 05.12.2016). Загл. с экрана. Яз. рус.

15 The Overview of E-cash: Implementation and Security Issues [Электронный ресурс] // Global Information Assurance Certification Paper [Электронный ресурс]. URL: https://www.giac.org/paper/gsec/1799/overview-e-cash-implementation-security-issues/103204 (дата обращения: 17.09.2016). Загл. с экрана. Яз. англ.

16 How to make a mint: the cryptography of anonymous electronic cash [Электронный ресурс] // National Security Agency Office of Information Security Research and Technology [Электронный ресурс]. URL:

http://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm (дата обращения: 19.09.2016). Загл. с экрана. Яз. англ.