МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
(СГУ)

Кафедра теоретических основ компьютерной безопасности и криптографии

Анонимные кредитные карты

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Пантелеева Романа Игоревича

Научный руководитель
доцент, к. ф.-м. н. _____ А. В. Жаркова
18.01.2019 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
18.01.2019 г.

Саратов 2019

ВВЕДЕНИЕ

Криптография – наука о методах преобразования информации в целях ее защиты от незаконных пользователей [1].

Современная криптография является областью знаний, связанной с решением таких проблем безопасности информации, как конфиденциальность, целостность и аутентификация. Достижение этих требований безопасности информационного взаимодействия и составляет основные цели криптографии [2].

Например, работа в областях деятельности, в которых используется оперативный обмен данными, возможна только если обеспечена безопасность обмена данными через открытые сети. Применение криптографии позволяет эффективно решить эту проблему. Наиболее распространенным криптографическим средством, обеспечивающим безопасность связи, является шифрование [3].

Шифрование представляет собой сокрытие информации от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней. Пользователи называются авторизованными, если у них есть соответствующий ключ для расшифрования информации. Вся сложность заключается в том, как реализовать весь этот процесс. Целью любой системы шифрования является максимальное усложнение получения доступа к информации неавторизованными лицами, даже если у них есть зашифрованный текст и известен алгоритм, использованный для шифрования. Пока неавторизованный пользователь не обладает ключом, секретность и целостность информации не нарушается.

Независимо от способа реализации для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

1) знание алгоритма шифрования не должно снижать криптостойкости системы;

2) зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

3) шифр должен быть стойким даже в случае, если нарушителю известно достаточно большое количество исходных данных и соответствующих им зашифрованных данных;

4) число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку;

5) незначительное изменение ключа или исходного текста должно приводить к существенному изменению вида зашифрованного текста;

6) структурные элементы алгоритма шифрования должны быть неизменными;

7) длина шифрованного текста должна быть равной длине исходного текста;

8) дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

9) не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

10) любой ключ из множества возможных должен обеспечивать равную криптостойкость [4].

Одной из областей применения криптографических систем является использование анонимных кредитных карт, а именно системы, которая полностью сохраняет анонимность клиента и скрывает личность клиента и его покупки от банка, в котором он ведет счет, а также скрывает банк от организации, в которой клиент совершает покупки.

Целью настоящей работы является изучение протокола анонимных кредитных карт, в результате чего требуется написать программное обеспечение для банков, организаций и клиентов на основе данного протокола.

В процессе работы необходимо выполнить следующие задачи:

1) изучить основные положения системы анонимных кредитных карт;

2) изучить алгоритмы и протоколы, необходимые для защиты данных в системе;

3) разработать и реализовать программный продукт, позволяющий организовать систему анонимных кредитных карт.

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 4 приложений. Общий объем работы – 110 страниц, из них 59 страниц – основное содержание, включая 72 рисунка, список использованных источников из 22 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе «Необходимые определения» приводятся необходимые определения, а именно: открытый текст, шифр, шифрование, криптограмма, расшифрование, ключ в соответствии с [5], симметричная криптосистема, криптосистема с открытым ключом в соответствии с [6], электронная подпись в соответствии с [7], аутентификация, полная система вычетом по модулю n, группа, кольцо, поле в соответствии с [8–11], функция Эйлера в соответствии с [12], хэш-функция в соответствии с [13].

В разделе 2 «Об анонимных кредитных картах» рассматривается формирование системы анонимных кредитных карт. Описывается применение анонимных кредитных карт на примере карт швейцарского банка Swiss Bankers Travel Card и Интеркарт в соответствии с [14] и пример офшорной карты Payeer в соответствии с [15]. Рассматривается система анонимных кредитных карт в соответствии с [16, 17]. Приводятся обозначения, используемые в протоколах. Описывается процесс создания и назначения коробки с двойной блокировкой (double-locked box). В подразделе, посвящённом протоколам, сначала описываются сущности, участвующие в протоколе. Затем согласно [16] подробно рассматривается протокол коробки с двойной блокировкой (double-locked box), протокол взаимодействия банка с банком (bank-to-bank протокол), протокол взаимодействия клиента с банком (customer-to-bank протокол) и протокол анонимных кредитных карт.

В разделе 3 «Алгоритмы блочного шифрования» рассматриваются примеры блочных шифров и их описание. Сначала приводится определение блочного шифра, описывается общая схема блочного шифрования. Описываются симметричные и асимметричные системы шифрования в соответствии с [5, 9, 18]. Далее подробно рассматриваются симметричный алгоритм AES в соответствии с [19] и блочный шифр «Кузнечик» в соответствии с [20], который входит в национальный стандарт РФ ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации.

Блочные шифры». Также изучается режим простой замены работы блочных шифров согласно национальному стандарту ГОСТ Р 34.13–2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» [21]. При программной реализации для симметричного шифрования выберем рассмотренный блочный шифр «Кузнечик» из национального стандарта РФ с режимом простой замены работы блочных шифров из соответствующего стандарта.

В разделе 4 «Асимметричное шифрование» приводится определение открытого шифрования и описываются примеры протоколов асимметричного шифрования: схема RSA согласно [22] и способ Эль-Гамаля согласно [12]. При программной реализации для асимметричного шифрования была выбрана схема RSA, так как она используется в большом числе криптографических приложений и включена во многие стандарты.

В разделе 5 «Программное обеспечение для анонимных кредитных карт» описывается разработанный и реализованный в ходе проделанной работы комплекс программ, предназначенный для функционирования системы клиентов, банков и организаций в рамках протокола анонимных кредитных карт. Программы написаны на языке Java и для их запуска необходима среда Intellij Idea. Также для реализации базы данных использовались технологии JDBC. Для общего доступа к базе данных с различных машин для каждой программы база данных размещена на сервере. Технологии и API для данной работы имеет сервер Heroku. Использованная база данных – postgresql. Также для реализации технологии отправки электронной почты использовались технологии mail-api.

В работе приводится описание программы администратора по регистрации банков в системе. Рассматривается интерфейс программы и различные сценарии работы, включая обработку неверного ввода информации. Также описываются действия, которые должен выполнить администратор, и изменения в базе данных, которые происходят после регистрации банка. Листинг программы для регистрации банков приведен в приложении А.

Описывается программа администратора по регистрации в системе организаций. Так же присутствует описание последовательности действий, которые должен выполнить администратор, и изменения в базе данных после регистрации организации. Фрагмент листинга программы для регистрации организаций приведен в приложении Б.

Описывается клиентское приложение на основе протокола анонимных кредитных карт. Приводится описание последовательности действий, которые должен выполнить пользователь для успешной регистрации в системе, описывается процесс входа в систему и то, какие действия может выполнить пользователь в данном приложении. Присутствует описание окна меню программы, окна регистрации, окна входа в систему, окна личного кабинета пользователя, окна регистрации пользователя в банках, окна пополнения счета и окна оплаты покупок. Фрагмент листинга программы клиента приведен в приложении В.

В приложении Г «SQL код для создания базы данных» приводится листинг по созданию таблиц баз данных.

ЗАКЛЮЧЕНИЕ

Система анонимных кредитных карт используется для разграничения и защиты личной информации клиентов, чтобы никто не смог связать личность клиента и его покупки.

В данной работе был изучен протокол анонимных кредитных карт и его составляющих, рассмотрены криптографические алгоритмы и протоколы, необходимые для защиты данных в системе.

В результате проделанной работы было разработано и реализовано программное обеспечение для взаимодействия банков, клиентов и магазинов с помощью анонимной кредитной карты. Для шифрования информации внутри данного протокола был использован базовый алгоритм шифрования «Кузнечик», определенный национальным стандартом Российской Федерации ГОСТ Р 34.12–2015 с режимом простой замены согласно национальному стандарту Российской Федерации ГОСТ Р 34.13–2015; для асимметричного шифрования используется система RSA. Программы были написаны на языке программирования Java с использованием различных технологий для работы с электронной почтой и базами данных. В качестве базы данных использовалась postgresql.

Результаты работы могут быть использованы для создания защищенной банковской системы, где клиентам будут выдаваться кредитные карты, которые они смогут использовать для оплаты покупок, при этом их личность будет засекречена.

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

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Нечаев, В. И. Элементы криптографии. Основы теории защиты информации [Электронный ресурс] / В. И. Нечаев. М. : Высшая школа, 1999. 109 с. Загл. с экрана. Яз. рус.

2 Основы криптографии : учеб. пособие, 2-е изд., испр. и доп. [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.

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

4 Баричев, С. Г. Основы современной криптографии [Электронный ресурс] / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. М. : ДИАЛОГ-МИФИ, 2011. 175 с. URL: http://www.ict.edu.ru/ft/002447/crypto1-3.pdf (дата обращения: 07.09.2018). Загл. с экрана. Яз. рус.

5 Салий, В. Н. Криптографические методы и средства защиты информации [Электронный ресурс] : учеб. пособие / В. Н. Салий. Саратов, 2017. 43 с. URL: https://www.sgu.ru/sites/default/files/textdocsfiles/2017/10/18/saliy_v.n._kriptograficheskie_metody_i_sredstva_zashchity_informacii.pdf (дата обращения: 07.09.2018). Загл. с экрана. Яз. рус.

6 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер. М. : Триумф, 2003. 806 с.

7 Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» [Электронный ресурс] // КонсультанПлюс [Электронный ресурс] : надёжная правовая поддержка. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 14.12.2018). Загл. с экрана. Яз. рус.

8 Смарт, Н. Криптография [Электронный ресурс] / Н. Смарт. М. : ТЕХНОСФЕРА, 2015. 529 с. Загл. с экрана. Яз. рус.

9 Ростовцев, А. Г. Теоретическая криптография [Электронный ресурс] / А. Г. Ростовцев, Е. Б. Маховенко. СПб. : АНО НПО «Профессионал», 2005. 480 с. Загл. с экрана. Яз. рус.

10 Винберг, Н. Б. Курс алгебры [Электронный ресурс] / Н. Б. Винберг. М. : Факториал Пресс, 2001. 544 с. Загл. с экрана. Яз. рус.

11 Лидл, Р. Конченые поля [Электронный ресурс] / Р. Лидл, Г. Нидеррайтер. М. : Мир, 1988. 430 с. Загл. с экрана. Яз. рус.

12 Молдовян, Н. А. Теоретический минимум и алгоритмы цифровой подписи [Электронный ресурс] : учеб. пособие / Н. А. Молдовян. СПб. : БХВ-Петербург, 2010. 304 с. Загл. с экрана. Яз. рус.

13 Чудеса хэширования [Электронный ресурс] // Kaspersky lab [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/the-wonders-of-hashing/3633/ (дата обращения: 14.12.2018). Загл. с экрана. Яз. рус.

14 Анонимные банковские карты швейцарских банков [Электронный ресурс] // Ваш личный банкир [Электронный ресурс]. URL: https://www.yourprivatebankers.com/anonimnye-bankovskie-karty/ (дата обращения: 06.01.2019). Загл. с экрана. Яз. рус.

15 Анонимная банковская карта – как получить и воспользоваться [Электронный ресурс] // Мониторинг и блог о проектах [Электронный ресурс]. URL: https://www.iqmonitor.ru/bank/anonimnaya-karta.html (дата обращения: 06.01.2019). Загл. с экрана. Яз. рус.

16 Androulaki, E. An anonymous credit card system [Электронный ресурс] / E. Androulaki, S. Bellovin // Proc. of 6th International Conference on Trust, Privacy & Security in Digital Business. 2009. 12 p. URL: https://www1.cs.columbia.edu/~smb/papers/ACC_TrustBus09.pdf (дата обращения: 08.10.2018). Загл. с экрана. Яз. англ.

17 Low, S. H. Anonymous credit cards and its collusion analysis [Электронный ресурс] / S. H. Low, N. F. Maxemchuk, S. Paul // IEEE/ACM Transactions of Networking. 1996. V. 4, is. 6. P. 809–816. URL: https://authors.library.caltech.edu/8583/1/LOWieeeacmtn96.pdf (дата обращения: 12.10.2018). Загл. с экрана. Яз. англ.

18 Фергюсон, Н. Практическая криптография [Электронный ресурс] / Н. Фергюсон, Б. Шнайер; пер. издательский дом «Вильямс». М. : Диалектика, 2004. 432 с. Загл. с экрана. Яз. Рус.

19 Панасенко, С. П. Алгоритмы шифрования. Специальный справочник [Электронный ресурс] / С. П. Панасенко. СПб. : БХВ-Петербург, 2009. 576 с. Загл. с экрана. Яз. рус.

20 ГОСТ Р 34.12–2015. Криптографическая защита информации. Блочные шифры [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) [Электронный ресурс] : [сайт]. URL: http://wwwold.tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 12.10.2018). Загл. с экрана. Яз. рус.

21 ГОСТ Р 34.13–2015. Криптографическая защита информации. Режимы работы блочных шифров [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) [Электронный ресурс] : [сайт]. URL: http://wwwold.tc26.ru/standard/gost/GOST_R_3413-2015.pdf (дата обращения: 12.10.2018). Загл. с экрана. Яз. рус.

22 Грушо, А. А. Анализ и синтез криптоалгаритмов [Электронный ресурс] : курс лекций / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. М., 2000. 110 с. Загл. с экрана. Яз. рус.