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 одновременного обмена секретными сообщениями

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Кошелевой Ирины Юрьевны

Научный руководитель

доцент, к.ф.-м.н. _____ А. В. Жаркова

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В. Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии – ровесница истории человеческого языка. С широким распространением письменности криптография стала формироваться как самостоятельная наука.

Бурное развитие криптографических систем произошло в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Криптографические методы защиты информации в автоматизированных системах могут применяться как для защиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа запоминающих устройствах, так и для сокрытия информации, передаваемой между различными элементами системы по линиям связи. Криптографическое преобразование как метод предупреждения несанкционированного доступа к информации имеет многовековую историю. В настоящее время разработано большое количество различных методов шифрования, созданы теоретические и практические основы их применения. Подавляющие число этих методов может быть успешно использовано и для сокрытия информации.

Целью дипломной работы является разработка и реализация приложения, с помощью которого пользователи в локальной сети смогут одновременно обмениваться секретами.

Для достижения поставленной цели требуется решить следующие задачи:

1) изучить протокол одновременного обмена секретами;

2) рассмотреть необходимые алгоритмы и протоколы для его построения и реализации.

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 137

страниц, из них 52 страницы – основное содержание, включая 35 рисунков и 5 таблиц, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Во введении ставится цель дипломной работы: разработка и реализация приложения, с помощью которого пользователи в локальной сети смогут одновременно обмениваться секретами. Для достижения поставленной цели требуется решить следующие задачи: изучить протокол одновременного обмена секретами, рассмотреть необходимые алгоритмы и протоколы для его построения и реализации.

В разделе 1 «Необходимые определения» приводятся некоторые определения, используемые в работе: шифрование, расшифрование, симметричные и асимметричные шифры, хэш-функция, криптографическая хэш-функция, хэш-код, функция сжатия, криптографический протокол и другие. [1–6]

Раздел 2 «Необходимые алгоритмы» состоит из двух подразделов, в которых содержится описание алгоритмов шифрования и хэширования.

Подраздел 2.1 «Шифрование» состоит из 2 подразделов, которые описывают работу симметричных и асимметричных алгоритмов шифрования.

В подразделе 2.1.1 «Симметричные шифры» даются общие сведения о симметричных шифрах и рассматривается шифр «Магма», входящий в национальный стандарт РФ ГОСТ Р 34.12-2015. В рамках данного подраздела приводятся определенные в отечественном стандарте ГОСТ Р 34.12-2015 обозначения, преобразования и алгоритмы развертывания ключа, шифрования и расшифрования. [1, 7–11]

В подразделе 2.1.2 «Асимметричные шифры» даются общие сведения об асимметричных шифрах, рассматриваются следующие алгоритмы: алгоритм Евклида нахождения наибольшего общего делителя двух целых чисел, алгоритм нахождения обратного по модулю элемента. Также в данном подразделе приводятся необходимые для работы шифрсистемы RSA алгоритмы генерации пары ключей (открытого и закрытого), шифрования и расшифрования. [2, 3, 7, 12]

Подраздел 2.2 «Хэширование» состоит из двух подразделов, в которых даются общие сведения об алгоритмах хэширования и рассматривается алгоритм хэширования ГОСТ Р 34.11-2012.

В подразделе 2.2.1 «Об алгоритмах хэширования» определяется область применения криптографических хэш-функций, дается определение лавинного эффекта и перечисляются часто используемые алгоритмы хэширования. [7]

В подразделе 2.2.2 «Алгоритм хэширования ГОСТ Р 34.11-2012» приводятся определенные в отечественном стандарте ГОСТ Р 34.11-2012 значения параметров, обозначения, преобразования, формула вычисления значения функции сжатия и алгоритм вычисления хэш-функции с длиной хэш-кода 256 бит. [5, 7, 13, 14]

Раздел 3 «Некоторые развитые протоколы» состоит из двух подразделов, в которых содержится описание протоколов передачи с забыванием и одновременного обмена секретами.

В подразделе 3.1 «Передача с забыванием» рассматривается протокол передачи с забыванием, необходимый для обмена ключами между пользователями при реализации протокола одновременного обмена секретами. [2, 15]

В подразделе 3.2 «Одновременный обмен секретами» рассматривается протокол одновременного обмена секретами, необходимый для одновременного обмена сообщениями между пользователями в реализованном приложении.

Допустим, Алиса знает секрет A, а Боб – секрет B. Алиса собирается сообщить Бобу A, если он расскажет ей B. Боб хочет сообщить Алисе B, если она расскажет ему A. Следующий протокол позволит Алисе и Бобу одновременно обменяться секретами.

1) Алиса шифрует свой секрет случайным ключом симметричного шифрования и посылает его Бобу.

2) Алиса создает n пар ключей симметричного шифрования. Первый

ключ каждой пары генерируется случайным образом, а второй представляет собой XOR первого ключа и ключа шифрования сообщения.

3) Алиса шифрует сообщение-заглушку каждым из своих $2n$ ключей.

4) Алиса посылает Бобу всю пачку шифрованных сообщений, проверяя, что он знает, какие сообщения какими половинами каких пар являются.

5) Боб шифрует свой секрет случайным ключом симметричного шифрования и посылает его Алисе.

6) Боб создает n пар ключей симметричного шифрования. Первый ключ каждой пары генерируется случайным образом, а второй представляет собой XOR первого ключа и ключа шифрования сообщения.

7) Боб шифрует сообщение-заглушку каждым из своих $2n$ ключей.

8) Боб посылает Алисе всю пачку шифрованных сообщений, проверяя, что она знает, какие сообщения какими половинами каких пар являются.

9) Алиса и Боб посылают друг другу все пары ключей, используя протокол передачи с забыванием. То есть Алиса посылает Бобу независимо для каждой из n пар ключей либо ключ, использованный для шифрования левого сообщения, либо ключ, использованный для шифрования правого сообщения. Боб делает то же самое. Они могут посылать свои половинки по очереди или сначала один может послать все n, а потом другой – это не имеет значения. Теперь и у Алисы, и у Боба есть по одному ключу из каждой пары, но никто не знает, какие из половинок получил партнер.

10) Алиса и Боб расшифровывают те половинки сообщений, которые могут, и убеждаются, что расшифрованные сообщения правильны.

11) Алиса и Боб посылают друг другу первые биты всех $2n$ ключей симметричного шифрования.

12) Алиса и Боб повторяют этап 11 для вторых битов всех $2n$ ключей симметричного шифрования, затем третьих битов и так далее, пока все биты всех ключей симметричного шифрования не будут переданы.

13) И Алиса, и Боб расшифровывают оставшиеся половины пар сообщения и выполняют XOR для любой пары ключей, чтобы получить ключи, которыми зашифрованы оригинальные сообщения. [2]

В разделе 4 «Некоторые существующие мессенджеры» рассматриваются некоторые из существующих корпоративных мессенджеров для локальной сети, а именно Lan Messenger [16], Winsent Messenger [17], HipChat [18].

В разделе 5 «Программная реализация» описывается разработанная и реализованная в рамках данной дипломной работы система одновременного обмена секретами. Для функционирования данной системы в ней реализованы алгоритмы шифрования «Магма» из отечественного стандарта ГОСТ Р 34.12-2015 и RSA, отечественный алгоритм хэширования ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит, криптографический протокол одновременного обмена секретами. Данная система состоит из двух программ: программа, выполняющая роль сервера, и программа, выполняющая роль клиента. Программы написаны на языке программирования C++ и скомпилированы в среде Qt Creator. [19, 20]

Программа Server.exe, выполняющая роль сервера, является консольным приложением. В данной программе осуществлено хранение списка зарегистрированных в системе пользователей. Для каждого пользователя хранится его имя в системе, хэш-код пароля, вычисленный согласно ГОСТ Р 34.11-2012, число попыток для входа в систему, а также указанный при регистрации пользователя адрес электронной почты. Также для каждого пользователя хранятся список его собеседников, список пользователей, которым был выслан запрос на добавление в собеседники, и список удаленных собеседников. Перечисленные данные хранятся в текстовых файлах, которые при запуске/закрытии сервера шифруются/расшифровываются с помощью шифра «Магма». В качестве ключа шифрования используется хэш-код длиной 256 бит, вычисленный согласно ГОСТ Р 34.11-2012, от пароля, вводимого при каждом запуске сервера, при этом для надёжности пароль можно периодически менять. При регистрации и восстановлении паролей пользователей в программе

генерируется код, который отправляется на указанный адрес электронной почты. Также в программе поддерживается список пар пользователей, осуществляющих одновременный обмен секретами, позволяющий этим пользователям обмениваться сообщениями друг с другом. Предполагается, что данная программа будет установлена на одном из компьютеров в локальной сети и запущена до запуска первой программы-клиента.

Программа Messenger.exe, выполняющая роль клиента, позволяет пользователю регистрироваться в системе, изменять сохраненный в системе пароль, осуществлять вход в систему, добавлять новых или удалять уже существующих пользователей, а также обмениваться сообщениями с другими пользователями, добавленными в список собеседников. Обмен сообщениями между пользователями осуществляется с помощью криптографического протокола одновременного обмена секретами. В рамках данного раздела приводится подробное описание работы пользователя в данной программе, иллюстрируемое большим количеством снимков экрана.

В заключении содержатся основные результаты проделанной работы.

В списке использованных источников приводятся 20 наименований.

В приложении А «Основной листинг программы-сервера» приведены исходные коды основных классов программы Server.exe.

В приложении Б «Основной листинг программы-клиента» приведены исходные коды основных классов программы Messenger.exe.

ЗАКЛЮЧЕНИЕ

Значение криптографии в современном обществе трудно переоценить. Новая информационная инфраструктура создает новые опасности для информации. Однако и криптография не стоит на месте, теперь она стала доступна широким массам пользователей. При помощи широкодоступных алгоритмов шифрования пользователи могут добиться безопасности передачи своих данных.

В ходе дипломной работы был изучен специальный криптографический протокол одновременного обмена секретами, а также необходимые для его реализации шифр «Магма» из национального стандарта РФ ГОСТ Р 34.12-2015, асимметричная шифрсистема RSA, протокол передачи с забыванием. В результате проделанной работы на базе указанных алгоритмов и протоколов было разработано и реализовано приложение, с помощью которого пользователи в локальной сети могут отправлять друг другу сообщения только при их одновременной передаче.

Разработанная система одновременного обмена секретами может быть использована в случае, когда требуется возможность обмена сообщениями между пользователями только при их одновременной передаче. Поиск в сети Интернет программ, которые бы поддерживали одновременный обмен секретами, не дал результатов.

Таким образом, все поставленные задачи были полностью решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Салий, В. Н. Криптографические методы и средства защиты информации [Электронный ресурс] : учеб. пособие / В. Н. Салий // Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского [Электронный ресурс]. 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: 22.11.2017). Загл. с экрана. Яз. рус.

2 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. М. : ТРИУМФ, 2003. 816 с.

3 Основы криптографии: учеб. пособие [Электронный ресурс] / А. П. Алферов [и др.]. 2-е изд. М. : Гелиос АРВ, 2002. 480 с. Загл. с экрана. Яз. рус.

4 Баричев, С. Г. Основы современной криптографии [Электронный ресурс] / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов // ИКТ [Электронный ресурс] : информационно-коммуникационные технологии в образовании. М. : Горячая линия – Телеком, 2006. 152 с. URL: http://www.ict.edu.ru/ft/002447/crypto1-3.pdf (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

5 ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования [Электронный ресурс] // docs.cntd.ru [Электронный ресурс] : электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/gost-r-34-11-2012 (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

6 Салий, В. Н. Лекции по дисциплине «Криптографические методы защиты информации» / В. Н. Салий. Саратов, 2016.

7 Российские криптографические стандарты [Электронный ресурс] // dom8a.ru [Электронный ресурс]. URL: http://dom8a.ru/seminar-

ib/05.06.2014/kazemskiy/paper.pdf (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

8 ГОСТ 28147-89 [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/ГОСТ_28147-89 (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

9 ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры [Электронный ресурс] // StandartGOST.ru [Электронный ресурс] : бесплатные ГОСТы и магазин документов. URL: http://standartgost.ru/g/ГОСТ_Р_34.12-2015 (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

10 О введении новых криптографических стандартов, разработанных с участием ИнфоТеКС [Электронный ресурс] // infotecs [Электронный ресурс]. URL: https://infotecs.ru/about/press-centr/news/produkty_i_resheniya/o_vvedenii_novykh_ kriptograficheskikh_standartov_razrabotannykh_s_uchastiem_infoteks_25.06.2015.html (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

11 ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров [Электронный ресурс] // docs.cntd.ru [Электронный ресурс] : электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200121984 (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

12 Петров, А. А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А. А. Петров. М. : ДМК, 2000. 448 с. Загл. с экрана. Яз. рус.

13 ГОСТ Р 34.11-2012 [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/ГОСТ_Р_34.11-2012 (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

14 Стандарт функции хеширования ГОСТ Р 34.11-2012 [Электронный ресурс] // IB-Bank.ru [Электронный ресурс] : отраслевой портал. URL: https://glossary.ib-bank.ru/solution/1086 (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

15 Забывчивая передача [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Забывчивая_передача (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

16 LAN Messenger [Электронный ресурс] // SourceForge [Электронный ресурс] : [сайт]. URL: https://sourceforge.net/projects/lanmsngr/ (дата обращения: 22.11.2017). Загл. с экрана. Яз. англ.

17 Winsent Messenger [Электронный ресурс] // WinSent [Электронный ресурс] : instant lan messenger. URL: www.winsent.ru (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

18 HipChat [Электронный ресурс] // Atlassian [Электронный ресурс]. URL: https://ru.atlassian.com/software/hipchat (дата обращения: 22.11.2017). Загл. с экрана. Яз. рус.

19 Qt [Электронный ресурс] // Qt [Электронный ресурс] : [сайт]. URL: http://doc.qt.io/ (дата обращения: 22.11.2017). Загл. с экрана. Яз. англ.

20 SMTP Service Extension for Authentication [Электронный ресурс] // IETF [Электронный ресурс]. URL: http://www.ietf.org/rfc/rfc2554.txt (дата обращения: 22.11.2017). Загл. с экрана. Яз. англ.