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

Почтовая служба с подтверждением

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Глотовой Юлии Владимировны

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

В настоящее время передача информации через компьютерную сеть стала обычным делом. В связи с этим возникают проблемы, связанные не только с вмешательством в обмен информацией третьего лица, но и с нечестностью сторон, обменивающихся этой информацией. Например, это может быть отказ одной из сторон от факта получения или отправления сообщения.

Кроме того при обмене данными могут возникнуть такие вопросы, как действительно ли сообщение пришло от конкретного отправителя, не было ли оно подменено или изменено.

Для решения этих и подобных вопросов создано большое количество криптографических протоколов. Обеспечение протоколом таких свойств информации, как доступность, целостность и конфиденциальность, определяет его безопасность. [1]

В данной работе рассматриваются алгоритмы и протоколы, необходимые для обеспечения безопасности почтовых приложений. Будут рассмотрены такие вопросы, как аутентификация сторон и источника данных, обеспечение конфиденциальности и целостности данных, невозможность отказа с доказательством получения сообщения.

Целью данной работы является разработка и реализация почтового приложения, в котором пользователи смогут отправлять друг другу сообщения и файлы, подписывать свои сообщения, а также получать расписку в получении этих сообщений гарантированно раньше, чем получающая сторона сможет их прочитать.

Для достижения поставленной цели требуется решить следующие задачи:

1) рассмотреть протокол электронной почты с подтверждением;

2) изучить необходимые алгоритмы и протоколы для реализации системы.

Дипломная работа состоит из введения, 8 разделов, заключения, списка использованных источников и 6 приложений. Общий объем работы – 137 страниц, из них 61 страница – основное содержание, включая 57 рисунков, список использованных источников из 22 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы «Необходимые определения и обозначения» приведены основные определения и обозначения, которые были использованы в работе. Например, в данном разделе приводятся такие определения, как криптография, хэш-функция, электронная цифровая подпись, эллиптическая кривая. В данном разделе были использованы источники [1–9].

Во втором разделе «Управление ключами» приводятся основные этапы управления ключами, а также обсуждается распределение ключей. В данной главе был сделан вывод об удобстве использования в приложениях с шифрованием большого количества информации гибридных систем, обладающих эффективностью симметричных систем шифрования и легкостью распределения ключей в криптосистемах с открытыми ключами. Гибридная система была использована при реализации почтового приложения в рамках данной дипломной работы. При написании раздела были использованы источники [3, 4, 10].

Третий раздел «Шифрование данных» состоит из двух подразделов: «Симметричные шифры» и «Асимметричные шифры». В первом подразделе приведены общие сведения о симметричных шифрах и подробно рассмотрен отечественный симметричный шифр Магма согласно ГОСТ Р 34.12-2015. Данный алгоритм применяется в реализованном почтовом приложении для обеспечения конфиденциальности при передаче данных по сети. Во втором подразделе приведены общие сведения об асимметричных шифрах, а также подробно рассмотрен алгоритм RSA. Алгоритм RSA применяется в реализованном почтовом приложении для защиты сеансовых ключей симметричного шифрования. При написании раздела были использованы источники [2, 3, 4, 8, 11, 12].

В четвертом разделе «Функции хэширования» приводятся общие сведения о функциях хэширования и подробно рассмотрена отечественная

функция хэширования с длиной результирующего значения 256 бит согласно ГОСТ Р 34.11-2012. В реализованном почтовом приложении она используется для проверки целостности данных, а также для вычисления электронной цифровой подписи согласно ГОСТ Р 34.10-2012. При написании раздела были использованы источники [1, 3, 9, 13, 14].

Пятый раздел «Электронная цифровая подпись» состоит из трех подразделов: «Общие сведения», «Стандарт ГОСТ Р 34.10-2012» и «Генерация эллиптической кривой». В первом подразделе рассмотрены различные подходы к созданию схем цифровой подписи. Во втором подразделе рассмотрена электронная цифровая подпись согласно ГОСТ Р 34.10-2012. Также в ней рассмотрены операции в группе точек эллиптической кривой, определенной над конечным простым полем, с помощью которых в данном стандарте реализуются процессы формирования и проверки электронной цифровой подписи. Электронная подпись на эллиптических кривых согласно ГОСТ Р 34.10-2012 используется в реализации почтового приложения для обеспечения аутентификации источника сообщения. В третьем подразделе рассмотрен алгоритм генерации эллиптической кривой, обладающей комплексным умножением. Комплексное умножение позволяет легко генерировать эллиптические кривые с хорошими криптографическими свойствами. Необходимость рассмотрения алгоритма генерации эллиптической кривой связана с тем, что порядок генерации параметров эллиптической кривой не регламентирован стандартом. Рассмотренный алгоритм был использован при реализации почтового приложения для генерации эллиптической кривой. При написании раздела были использованы источники [1, 5, 6, 7, 9, 15, 16].

В шестом разделе «Аутентификация пользователей» рассмотрены некоторые протоколы аутентификации пользователей. Целью данных протоколов является проверка одной из сторон того, что взаимодействующая сторона – та, за которую себя выдает. При реализации почтового приложения

был выбран протокол, основанный на асимметричном алгоритме шифрования. При написании раздела были использованы источники [1, 3, 14].

Седьмой раздел «Электронная почта с подтверждением» включает подразделы «Передача с забыванием», «Протокол электронной почты с подтверждением» и «Некоторые существующие программные продукты». В данном разделе рассмотрен протокол электронной почты с подтверждением, обеспечивающий в реализованном почтовом приложении невозможность отказа с доказательством получения сообщения. В основу этого протокола положен протокол передачи с забыванием. Описанию этих двух протоколов посвящены первые два подраздела. В третьем подразделе приведен обзор некоторых существующих почтовых приложений. При написании раздела были использованы источники [1, 14, 17, 18, 19, 20].

В восьмом разделе «Программная реализация» описаны три программы, обеспечивающие функциональность реализованного почтового приложения: программа клиента, программа администратора и программа сервера. Программа клиента обеспечивает доступ пользователей к своей почте и работу с ней. Программа администратора позволяет создавать и удалять новых пользователей, а также изменять их ключи. Программа сервера имеет доступ к базе данных, в которой хранится информация о пользователях и их письмах. Программы клиента и администратора подключаются к серверу и получают необходимые для их работы данные. В данном разделе приведены ссылки на источники [21, 22].

ЗАКЛЮЧЕНИЕ

Через электронную почту может передаваться информация разной степени важности. В том числе через нее может передаваться конфиденциальная информация, поэтому очень важно обеспечить безопасность почтового приложения.

В ходе данной работы были изучены специальные криптографические протоколы и алгоритмы, необходимые для обеспечения безопасности почтового приложения.

В результате проделанной работы была разработана и реализована почтовая служба, обеспечивающая возможность пользователям:

– отправлять друг другу сообщения;

– контролировать их целостность с помощью отечественной функции хэширования ГОСТ Р 34.11-2012;

– формировать и проверять электронную цифровую подпись с помощью алгоритмов, определенных в отечественном стандарте ГОСТ Р 34.10-2012;

– гарантированно доказывать получение сообщений или же их отсутствие с помощью реализованного протокола электронной почты с подтверждением.

Для обеспечения конфиденциальности все передаваемые по сети данные шифруются с помощью отечественного блочного шифра Магма, определенного в стандарте ГОСТ Р 34.12-2015.

Для аутентификации пользователей, а также для защиты сеансовых ключей симметричного шифрования, используется алгоритм RSA.

Аутентификация источника данных осуществляется с помощью электронной цифровой подписи на основе эллиптических кривых согласно отечественному стандарту ГОСТ Р 34.10-2012.

Целостность данных проверяется с помощью отечественной функции хэширования с длиной результирующего значения 256 бит согласно ГОСТ Р 34.11-2012.

Для невозможности отказа с доказательством получения сообщения используется протокол электронной почты с подтверждением. В основу этого протокола положен протокол одновременной передачи с забыванием, благодаря которому обеспечивается честность обеих сторон.

Данная почтовая служба может быть использована в качестве корпоративной почты. Как и большинство подобных программных продуктов, данное приложение обеспечивает конфиденциальность и целостность сообщений, а также предоставляет возможность подписи сообщений. Однако в данной программе также реализован протокол электронной почты с подтверждением, гарантирующий, что получатель не сможет прочитать сообщение, не расписавшись в получении.

Таким образом, все поставленные задачи были полностью решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие [Электронный ресурс] / А. В. Черемушкин. М. : Издательский центр «Академия», 2009. 272 с. Загл. с экрана. Яз. рус.

2 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: 09.11.2017). Загл. с экрана. Яз. рус.

3 Алферов, А. П. Основы криптографии: учеб. пособие / А. П. Алферов [и др.]. 3-е изд. М. : Гелиос АРВ, 2002. 480 с.

4 Мао, В. Современная криптография: теория и практика [Электронный ресурс] / В. Мао. М. : Издательский дом «Вильямс», 2005. 763 с. Загл. с экрана. Яз. рус.

5 Ростовцев, А. Г. Теоретическая криптография [Электронный ресурс] / А. Г. Ростовцев, Е. Б. Маховенко. СПб. : НПО «Профессионал», 2004. 478 с. Загл. с экрана. Яз. рус.

6 ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] : [сайт]. URL: http://protect.gost.ru/document.aspx?control=7&id=180151 (дата обращения: 09.11.2017). Загл. с экрана. Яз. рус.

7 Молдовян, Н. А. Криптография. От примитивов к синтезу алгоритмов / Н. А. Молдовян, А. А. Молдовян, М. А. Еремеев. СПб. : БХВ-Петербург, 2004. 228 с.

8 ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК26) [Электронный ресурс] : [сайт]. URL: https://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 09.11.2017). Загл. с экрана. Яз. рус.

9 ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] : [сайт]. URL: http://protect.gost.ru/document.aspx?control=7&id=180209 (дата обращения: 09.11.2017). Загл. с экрана. Яз. рус.

10 Дернова, Е. С. Криптографические протоколы [Электронный ресурс] : учеб. пособие / Е. С. Дернова, Д. Н. Молдовян, Н. А. Молдовян. СПб. : Изд-во СПбГЭТУ «ЛЭТИ», 2010. 100 с. Загл. с экрана. Яз. рус.

11 ГОСТ Р 34.12-2015: чего ожидать от нового стандарта? [Электронный ресурс] // InformationSecurity [Электронный ресурс] : [сайт]. URL: http://www.itsec.ru/articles2/crypto/gost-r-chego-ozhidat-ot-novogo-standarta (дата обращения: 01.12.2017). Загл. с экрана. Яз. рус.

12 ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК26) [Электронный ресурс] : [сайт]. URL: https://www.tc26.ru/standard/gost/GOST_R_3413-2015.pdf (дата обращения: 09.11.2017). Загл. с экрана. Яз. рус.

13 Алгоритм хэширования MD6 [Электронный ресурс] // Sec.ru [Электронный ресурс] : [сайт]. URL: http://daily.sec.ru/publication.cfm?pid=43766 (дата обращения: 01.12.2017). Загл. с экрана. Яз. рус.

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

15 Жданов, О. Н. Применение эллиптических кривых в криптографии [Электронный ресурс] / О. Н. Жданов, Т. А. Чалкин. Красноярск : СибГАУ, 2011. 65 с. Загл. с экрана. Яз. рус.

16 Бабенко, М. Г. Анализ методов скалярного умножения на эллиптической кривой [Электронный ресурс] / М. Г. Бабенко // Молодой ученый [Электронный ресурс]. 2010. № 4. С. 24–28. URL: https://moluch.ru/archive/15/1426/ (дата обращения: 09.11.2017). Загл. с экрана. Яз. рус.

17 Even, S. A Randomized Protocol for Signing Contracts [Электронный ресурс] / S. Even, O. Goldreich, A. Lempel // Communications of ACM [Электронный ресурс]. 1985. № 6. P. 637–647. URL: http://www.lix.polytechnique.fr/~catuscia/teaching/papers_and_books/SigningContracts.pdf (дата обращения: 09.11.2017). Загл. с экрана. Яз. англ.

18 Enhanced email security to keep your data safe [Электронный ресурс] // Hushmail [Электронный ресурс] : [сайт]. URL: https://www.hushmail.com (дата обращения: 01.12.2017). Загл. с экрана. Яз. англ.

19 Secure Email [Электронный ресурс] // Neomailbox [Электронный ресурс] : [сайт]. URL: http://www.neomailbox.com/services/secure-email (дата обращения: 01.12.2017). Загл. с экрана. Яз. англ.

20 Neomailbox: a secure alternative to Gmail [Электронный ресурс] // Nerdbusiness [Электронный ресурс] : [сайт]. URL: https://nerdbusiness.com/blog/neomailbox-gmail-alternative/ (дата обращения: 01.12.2017). Загл. с экрана. Яз. англ.

21 Download Connector/Net [Электронный ресурс] // MySQL [Электронный ресурс] : [сайт]. URL: https://dev.mysql.com/downloads/connector/net/1.0.html (дата обращения: 01.12.2017). Загл. с экрана. Яз. англ.

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