Министерство образования и науки Российской Федерации

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

Кафедра теоретических основ компьютерной безопасности и криптографии

Система информационного обмена с криптографической защитой информации

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 090102.65 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Краснова Никиты Олеговича

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

Заведующий кафедрой
профессор, к.ф.-м.н. В.Н. Салий

Саратов 2016

ВВЕДЕНИЕ

Общемировые тенденции к расширению контроля над информационной сферой заставляют задуматься, что теперь все наши действия в сети обречены на моментальное обнаружение, а Интернет из свободного пространства превращается в инструмент слежки. Мировой специалист по криптографии и журналист Брюс Шнайер убежден, что спецслужбы проникают внутрь систем криптографического шифрования, встроенных в наши программы передачи сообщений и смартфоны, которыми мы активно пользуемся.

Промышленный шпионаж также является большой проблемой в информационной сфере. Сам по себе сбор информации о конкуренте не запрещен законом, если для этого используются легальные методы. Если же способы добывания информации запрещены законом, то тогда и возникает явление, которое принято называть промышленным шпионажем.

Целью данной дипломной работы является изучение алгоритмов и протоколов, использующихся для криптографической защиты информации, исследование возможностей Java смарт-карт, сравнение различных видов смарт-карт, на основании чего требуется разработать программно-аппаратное средство обмена информации в сети Интернет с криптографической защитой.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

1) Необходимые сведения и протоколы.

Современные системы по безопасному обмену информации должны иметь целый комплекс средств защиты, куда входят, как программные модули, так и аппаратные составляющие.

Подраздел 1.1 «Необходимые определения» знакомит с используемыми в работе сведениями и определениями.

Установление подлинности всех аспектов информационного взаимодействия является важной составной частью проблемы обеспечения достоверности получаемой информации. Этой проблеме посвящен подраздел 1.2 «Аутентификация сторон». Аутентификация позволяет осуществить проверку одной из сторон того, что взаимодействующая с ней сторона – именно та, за которую она себя выдает. Основным средством для проведения аутентификации являются протоколы аутентификации. Широкое распространение при аутентификации получили протоколы на базе ассиметричного шифрования. Существует десятки разновидностей таких протоколов, наиболее известными из которых являются протоколы на основе схемы Фейге-Фиата-Шамира, алгоритмов RSA, Эль-Гамаля, Шнорра. В работе также подробно рассмотрены упрощенная схема аутентификации сторон Фейге-Фиата-Шамира и протокол аутентификации сторон на основе RSA, который в результате был выбран автором для реализации.

Одна из фундаментальных проблем криптографии – безопасное общение по прослушиваемому каналу. Сообщения нужно зашифровывать и расшифровывать, но для этого обеим сторонам нужно иметь общий ключ. Если этот ключ передавать по тому же каналу, то прослушивающая сторона тоже получит его, и смысл шифрования исчезнет. Этой проблеме посвящен подраздел 1.3 «Распределение ключей». В работе рассмотрена схема открытого распределения ключей, предложенная У. Диффи и М. Хеллманом, которая

произвела настоящую революцию в мире шифрования. Протокол Диффи-Хеллмана позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены канал связи. Модификация данного протокола распределения ключей Диффи-Хеллмана под названием MTI позволяет использовать незащищённый от подмены канал связи, поэтому автором решено было реализовывать именно данную схему.

Указанные выше протоколы оперируют с большими целыми неотрицательными числами, а именно используются операции сложения, вычитания, умножения, деления, возведения в степень по модулю. В подразделе 1.4 «Длинная арифметика» представлено описание этих алгоритмов.

С целью защиты информации от непредусмотренных пользователей в работе используется алгоритм шифрования ГОСТ 28147-89, который устанавливает единый алгоритм криптографического преобразования для систем обработки информации в сетях. Описание ГОСТ 28147-89 представлено в подразделе 1.5 «Алгоритм шифрования ГОСТ 28147-89».

2) Смарт-карты.

Подраздел 2.1 «Общие понятия» дает начальное представление о смарт-картах. Смарт-карта представляет собой пластиковую карту, оснащенную встроенной электронной микросхемой, которая, в основном, состоит из микропроцессора (контактного чипа), операционной системы, контролирующего устройства.

Существуют несколько видов смарт-карт, основные из которых: карты-счетчики, карты с памятью, микропроцессорные карт.

Одним из видов микропроцессорных карт являются Java смарт-карты. Этот тип смарт-карт рассматривается в подразделе 2.2 «Java смарт-карты».

3) Некоторые существующие службы обмена сообщениями с шифрованием.

В рамках данной работы были рассмотрены некоторые существующие программные продукты, которые в той или иной степени обеспечивают защиту информации, а именно: программы Bimoid, VIPole, линейка программных продуктов от компании B-labs.

4) Разработанный программный продукт.

В работе любой организации зачастую возникает потребность в обмене конфиденциальной информацией между двумя или более лицами.

Автором было разработано и реализовано программно-аппаратное средство мгновенного обмена сообщениями в сети Интернет с криптографической защитой информации, а именно используется шифрование сообщений с помощью алгоритма ГОСТ 28147-89, применяются протокол аутентификации на основе RSA и протокол MTI распределения ключей. Указанные алгоритмы и протоколы оперируют с большими целыми числами, поэтому автором также была реализована длинная арифметика.

Продукт написан на языке программирования Java и состоит из серверной и клиентской частей. На клиентской части используется аппаратная защита, а именно: устройство чтения смарт-карт ACR38U-I1 или устройство чтения смарт-карт ASEDrive III USB, смарт-карты NXP J2A40.

В разделе 4 «Разработанный программный продукт» подробно раскрыто описание работы приложения, действия администратора системы, приведены снимки экрана, иллюстрирующие процесс взаимодействия пользователя с разработанной системой.

Завершается работа приложениями, а именно:

- приложение А «Листинг программы. Серверная часть» представляет собой программный код серверной части, разработанной системы;
- приложение Б «Листинг программы. Вспомогательные средства» представляет собой программный код вспомогательных средств, помогающих

сгенерировать параметры для протоколов аутентификации и распределения ключей;

- приложение В «Листинг программы. Клиентская часть» представляет собой программный код клиентской части, разработанной системы;
- приложение Г «Листинг программы. Апплет» представляет собой программный код апплета, который загружается в память Java смарт-карты;
- приложение Д «Листинг шаблона скрипта» описывает шаблон, который используется при формировании скрипта для программы GPShell, скрипт применяется для загрузки пользовательских данных в память Java смарт-карты.

ЗАКЛЮЧЕНИЕ

Проанализировав различные алгоритмы и протоколы, использующиеся для криптографической защиты информации, а также рассмотрев возможности некоторых аппаратных средств, можно сделать вывод, что для обеспечения защиты и конфиденциальности информации необходимо применять комплексные подходы, нельзя ограничиваться лишь одним методом или концепцией.

В данной работе были рассмотренны различные программы для безопасного общения и взаимодействия, такие как Bimoid, VIPole, линейка программных продуктов от компании B-labs, изучены отечественный стандарт шифрования ГОСТ 28147-89, алгоритмы длинной арифметики, а также протоколы аутентификации и распределения ключей, использующиеся для криптографической защиты информации, исследованы возможности карт памяти и Java смарт-карт.

В результате проделанной работы было разработано и реализовано программно-аппаратное средство информационного обмена с криптографической защитой информации на основании стандарта шифрования ГОСТ 28147-89 в режиме простой замены, схемы аутентификации сторон RSA, протокола распределения ключей MTI и Java смарт-карт NXP JCOP J2A 2.4.1-40KB.

Таким образом, все поставленные задачи были полностью решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Салий, В. Н. Криптографические методы и средства защиты информации : учеб. пособие [Электронный ресурс] / В. Н. Салий // СГУ – Саратовский государственный университет [Электронный ресурс] : [сайт]. URL: http://www.sgu.ru/sites/default/files/textdocsfiles/2015/11/09/saliy_v.n._kriptograficheskie_metody_i_sredstva_zashchity_informacii.pdf (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

2 Основы криптографии : учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. 2-е изд., испр. и доп. М. : Гелиос АРВ, 2002. 480 с.

3 Виноградов, И. М. Основы теории чисел [Электронный ресурс] / И. М. Виноградов. Загл. с экрана. Яз. рус.

4 Квадратичный вычет [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Квадратичный_вычет (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

5 Факторизация целых чисел [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Факторизация_целых_чисел (дата обращения: 18.10.2015). Загл. с экрана. Яз. рус.

6 Односторонняя функция // Википедия [Электронный ресурс] : свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Односторонняя_функция (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

7 Богомолов, А. М. Алгебраические основы теории дискретных систем / А. М. Богомолов, В. Н. Салий. М. : Наука, Физ.-мат. лит., 1997. 368 с.

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

9 ГОСТ 28147-89 [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] : [сайт]. URL: http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=131282 (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

10 Сеансовый ключ [Электронный ресурс] // Википедия [Электронный ресурс]: свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Сеансовый_ключ (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

11 IP-адрес [Электронный ресурс] // Википедия [Электронный ресурс] : свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/IP-адрес (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

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

13 Маховенко, Е. Б. Теоретико-числовые методы в криптографии: учеб. пособие / Е. Б. Маховенко. М. : Гелиос АРВ, 2006. 320 с.

14 Кнут, Д. Искусство программирования. В 4 т. Т. 2. Получисленные алгоритмы / Д. Кнут. 3-е изд. М. : «Вильямс», 2007. С. 832.

15 Смарт-карты [Электронный ресурс] // ZontCard [Электронный ресурс]. URL: http://www.zontcard.ru/forms_card/smart-karta/ (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

16 GlobalPlatform [Электронный ресурс] // Sourceforge [Электронный ресурс]. URL: http://sourceforge.net/projects/globalplatform/?source=navbar (дата обращения: 12.12.2015). Загл. с экрана. Яз. англ.

17 Bimoid [Электронный ресурс] // Bimoid [Электронный ресурс] : [сайт] URL: http://www.bimoid.com (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

18 VIPole [Электронный ресурс] // VIPole [Электронный ресурс] : [сайт] URL: https://www.vipole.com/ru/ (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

19 Система мгновенных сообщений [Электронный ресурс] // B-labs [Электронный ресурс] : [сайт] URL: http://www.bopup.ru/products/ (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.

20 Bopup Secure Messenger [Электронный ресурс] // Softkey.info [Электронный ресурс] : [сайт] URL: http://www.softkey.info/news/news 796.php?sphid= (дата обращения: 12.12.2015). Загл. с экрана. Яз. рус.