Шардин Т.О.
Научный руководитель: к.т.н., доцент каф. ФПМ А.В. Астафьев
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: tima.shardin@mail.ru

Обзор и анализ методов защищенной передачи данных на примере протокола рукопожатия с использованием криптосистемы RSA

В настоящее время Интернет – открытая информационная среда. И не только в плане свободы информации, но и в плане несанкционированного доступа к этой информации. По различным историческим и технологическим причинам, большинство трафика, передаваемого разными способами по Интернету, пересылается открытым образом. То есть злоумышленник, подключившийся к каналу передачи данных, сможет беспрепятственно считывать данные, передаваемые пользователем и получаемые им из Интернета. И если содержимое сообщения в тематическом форуме не всегда заслуживает секретности, то номер кредитной карты – напротив, нуждается в хорошей защите. Поэтому разработчики программного обеспечения принимают меры по защите передаваемых данных, тем самым защищая их от злоумышленников. Зачастую это реализуется путем создания защищенного канала передачи данных. В связи с этим анализ, разработка новых и совершенствование существующих методов защищенной передачи информации является актуальной научно-технической задачей.

Объект исследования в данной работе – протокол рукопожатия с использованием криптосистемы RSA, предмет исследования – использование протокола рукопожатия в клиент-серверных приложениях для защиты передаваемых данных.

Целью исследования является обзор и анализ метода защищенного канала передачи данных, реализуемого в клиент-серверных приложениях для защиты информации на примере протокола рукопожатия с использованием криптосистемы RSA.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор метода защищенной передачи информации.
2. Анализ выбранного метода.
3. Результаты исследования.

Обзор метода защищенной передачи информации. На практике, процесс передачи информации через защищенный канал связи зачастую связан с использованием протоколов, основанных на различных криптосистемах. Большинство специалистов сделали вывод, что наилучшие результаты достигаются при использовании, в процессе передачи данных, открытого и закрытого ключа для идентификации клиента или сервера.

В ходе исследования был рассмотрен следующий метод:

Протокол рукопожатия – криптографический протокол, основанный на симметричном взаимном обмене информацией между участниками по схеме запрос – ответ [1]. При использовании криптосистемы RSA в данном протоколе позволяет участникам обмена изначально использовать необходимые параметры для безопасной передачи информации. RSA относится к так называемым асимметричным алгоритмам, у которых ключ шифрования не совпадает с ключом дешифровки. Закрытый ключ находится в тайне, а открытый ключ можно сообщать кому угодно или даже публиковать его. Открытый и закрытый ключи каждого участника обмена образуют согласованную пару в том смысле, что они являются взаимно обратными [2]. Злоумышленнику, перехватившему значение открытого ключа, потребуется большое количество времени или вовсе будет невозможно вычислить пару простых чисел для дальнейшего подбора закрытого ключа, при условии, что простые числа при генерации пары ключей изначально были большими. Тем самым это позволяет использовать данную систему для безопасного обмена информацией в клиент-серверных приложениях [3].

Анализ методов защищенной передачи информации. Для анализа были выбранные следующие критерии:

Требование к материальным затратам – позволяет оценить, рентабелен ли данный метод при разработке приложения, требуется ли материальные затраты для поддержания алгоритма.

Использование центров сертификации – позволяет оценить, необходимо ли дополнительно прибегать к использованию подтверждения подлинности ключей с помощью электронно-цифровой подписи.

Криптостойкость метода – позволяет оценить, обладает ли данный алгоритм достаточной способностью противостоять криптоанализу. Это один из важных критериев, так как при недостаточной или низкой криптостойкости, использование алгоритма для защиты информации между участниками обмена нецелесообразно.

Простота использования алгоритма – позволяет оценить, понятна ли работа для пользователя, работающего с интерфейсом алгоритма.

В результате анализа были выявлены следующие достоинства данного метода, приведенные в таблице:

Таблица 1 – Результаты анализа

Вид	Требование к материальным затратам	Использование центров сертификации	Криптостойкость метода	Простота использования алгоритма
Протокол рукопожатия с криптосистемой RSA	Не требует материальных затрат	Не требует центров сертификации	Обладает высокой криптостойкостью при использовании большой длины ключа (большие простые числа)	Обладает простотой при использовании в приложениях

Результаты исследования. В результате проведенного исследования было выяснено, что выбранный метод защищенного канала передачи информации, основанного на протоколе рукопожатия с использованием криптосистемы RSA является безопасным для защиты конфиденциальной информации. Данный метод обладает рядом преимуществ, а именно: выгоден по экономическим соображениям (затраты минимальные или их вовсе нет), не требует дополнительных центров сертификации, что позволяет использовать его любому лицу, а также простота в использовании.

Литература

1. Цифровые SSL сертификаты [Электронный ресурс] // Habrahabr.ru : интернет портал URL: https://habrahabr.ru/company/tuthost/blog/150433 (дата обращения: 28.03.2016).

2. RSA [Электронный ресурс] // Википедия : свободная энцикл. URL: https://ru.wikipedia.org/wiki/RSA (дата обращения: 28.10.2016).

3. Молдовян А.А., Молдовян Д.Н., Левина А.Б. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ СЕКРЕТА - Санкт-Петербург: СПб: Университет ИТМО, 2016. - 55 с. - экз.