Шардин Тимофей Олегович
магистрант, лаборант
Павлова Светлана Михайловна
канд. пед. наук, доцент
Муромский институт (филиал)
ФГБОУ ВО «Владимирский государственный
университет им. А.Г. и Н.Г. Столетовых»
г. Муром, Владимирская область

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АЛГОРИТМА RSA В ПРОТОКОЛЕ РУКОПОЖАТИЯ

Аннотация: *в работе представлен метод реализации защищенного канала передачи информации, основанного на протоколе рукопожатия с использованием криптосистемы RSA, являющийся безопасным для защиты конфиденциальной информации.*

Ключевые слова: *передача данных, защищенный канал связи, информационное взаимодействие, ассиметричные алгоритмы шифрования.*

В настоящее время Интернет – открытая информационная среда. По технологическим причинам большинство трафика пересылается открытым образом, что дает злоумышленнику в некоторых случаях получать конфиденциальную информацию. Поэтому разработчики программного обеспечения принимают меры по защите передаваемых данных путем создания защищенного канала связи.

На практике, процесс передачи информации через защищенный канал связи связан с использованием протоколов [1], основанных на различных криптосистемах. В ходе исследования был рассмотрен следующий метод:

Протокол рукопожатия – криптографический протокол, основанный на симметричном взаимном обмене информацией между участниками по схеме запрос – ответ [2].

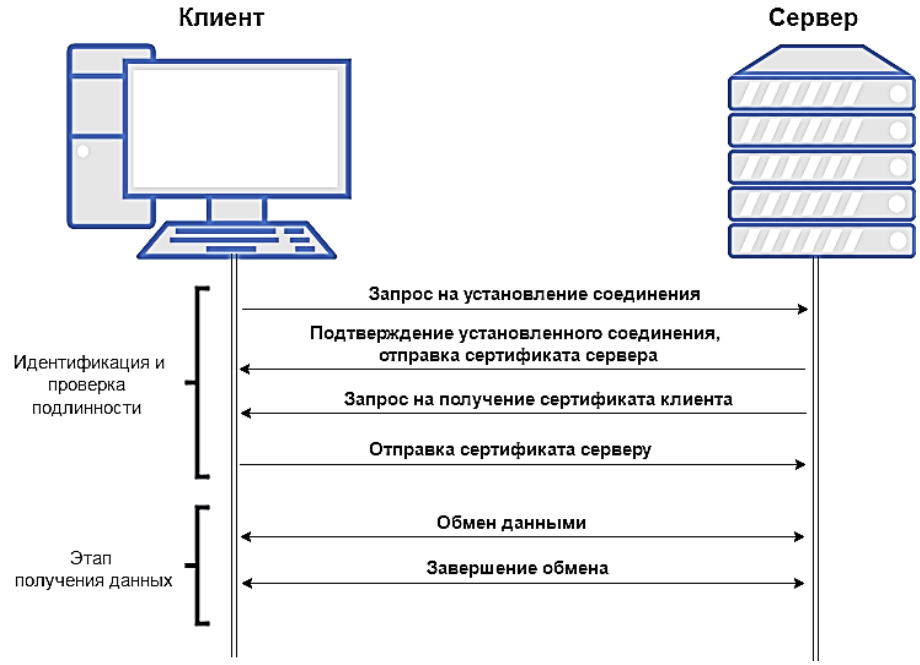

Рис. 1. Схема работы протокола рукопожатия

При использовании криптосистемы RSA в данном протоколе позволяет участникам обмена изначально использовать необходимые параметры для безопасной передачи информации. RSA – асимметричный алгоритм, у которого ключ шифрования не совпадает с ключом дешифровки. Закрытый ключ находится в тайне, а открытый ключ можно передавать любым способом. Открытый и закрытый ключи каждого участника обмена образуют согласованную пару, так как они являются взаимно обратными.

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 данное решение для безопасного обмена информацией в различных клиент-серверных приложениях [3]. Стоит отметить, что протокол рукопожатия имеет аналоги: SSL сертификат и электронно-цифровую подпись (ЭЦП).

Проведем анализ этих алгоритмов с использованием криптосистемы RSA по следующим критериям:

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

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

3. Криптостойкость метода – позволяет оценить, обладает ли данный алгоритм достаточной способностью противостоять криптоанализу.

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

В результате анализа были выявлены следующие достоинства данного метода, приведенные в таблице 1:

Таблица 1

Результаты анализа

Вид	Требование к материальным затратам	Использование центров сертификации	Криптостойкость метода (алгоритм RSA)	Простота использования метода в приложениях
Протокол рукопожатия	Не требует материальных затрат	Не требует центров сертификации	Обладает высокой криптостойкостью	Обладает простотой при использовании в приложениях
SSL сертификат	Требует материальные затраты	Требует центра сертификации	Обладает высокой криптостойкостью	Требует дополнительного программного обеспечения
ЭЦП	Требует материальные затраты	Требует центра сертификации	Обладает высокой криптостойкостью	Обладает простотой при использовании в приложениях

Математическая модель алгоритма RSA, используемая в протоколе рукопожатия:

1. Берутся два простых числа «p» и «q» большой длины.

2. Затем числа перемножаются.

$$n = p \times q, \quad (1)$$

где «n» – называется модулем.

3. Потом вычисляется функция Эйлера по следующей формуле

$$f(n) = (p-1) \times (q-1), \quad (2)$$

4. Выбирается такое число «e» (открытая экспонента), которое будет являться взаимно простым с f(n) (т.е. «d» и f(n) должны иметь лишь один общий делитель, равный 1).

5. Ищется число «d» (закрытая экспонента), мультипликативно-обратное к числу «e» по модулю f (n).

Процесс шифрования происходит следующим образом: есть пара чисел (e, n), которые образуют открытый ключ, тогда шифрование будет представляться следующим образом.

$$C = M^e \times (\mathrm{mod}\, n), \quad (3)$$

где M – то, что шифруем.

Процесс дешифрования: есть пара чисел (d, n), которые образуют закрытый ключ, тогда дешифрование будет представляться следующим образом

$$M = C^{\mathrm{d}} \times (\mathrm{mod}\, n), \quad (4)$$

где C – зашифрованное сообщение.

Данное описание математической модели, можно представить следующим образом (рис. 2).

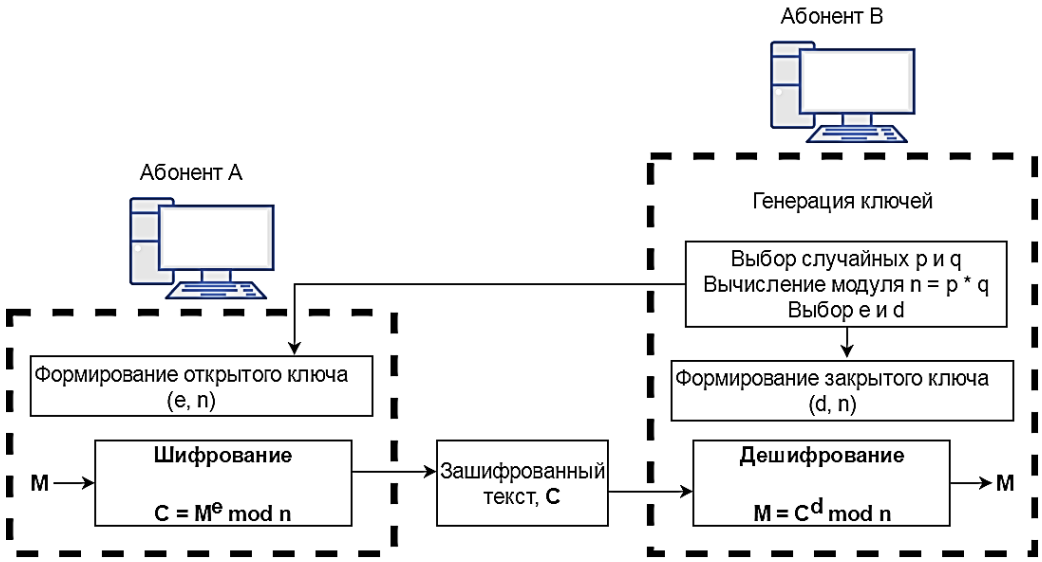

Рис. 2. Математическая модель алгоритма RSA в протоколе рукопожатия

По результатам исследования было выяснено, что выбранный метод для реализации 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 прост в использовании при этом обладая высокой криптостойкостью.

Список литературы

1. Молдовян А.А. Протоколы аутентификации с нулевым разглашением секрета / А.А. Молдовян, Д.Н. Молдовян, А.Б. Левина. – СПб.: Университет ИТМО, 2016. – 55 с.

2. Протокол SSL/TLS [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/studies/courses/14248/1285/lecture/24227?page=3

3. Водолазский В. Коммерческие системы шифрования: основные алгоритмы и их реализация. Ч. 1 // Монитор. – 1992. – №6–7. – С. 14–19.

4. Воеводин В.В. Параллельные вычисления / В.В. Воеводин [и др.]. – СПб.: БХВ-Петербург, 2002. – Р. 608.