Волков Дмитрий Алексеевич
магистрант
Павлова Светлана Михайловна
канд. пед. наук, канд. пед. наук
Муромский институт (филиал)
ФГБОУ ВО «Владимирский государственный
университет им. А.Г. и Н.Г. Столетовых»
г. Муром, Владимирская область

ОБЗОР И АНАЛИЗ МЕТОДИКИ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ СЕКРЕТА ФИАТА – ШАМИРА

Аннотация: *в статье проведен обзор метода аутентификации. Представлен сравнительный анализ алгоритмов с нулевым разглашением, сделаны выводы по проделанной работе.*

Ключевые слова: *криптография, аутентификация, нулевое разглашение, секрет Фиата – Шамира.*

Данная работа посвящена обзору и анализу методов аутентификации, реализуемого в клиент-серверных приложениях для защиты информации на примере алгоритма с нулевым разглашением секрета Фиата – Шамира.

В ходе выполнения данной работы необходимо выполнить следующие задачи: обзор метода аутентификации с нулевым разглашением, проведение сравнительного анализа методов с нулевым разглашением, сформулировать результаты исследований.

Аутентификация – это проверка соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации, в простейшем случае – с помощью имени входа и пароля.

В ходе исследования был рассмотрен следующий метод:

Алгоритм Фиата – Шамира. Основной идеей является сложность извлечения квадратного корня по составному модулю, который включает не менее двух

больших простых множителей [2]. При этом считается, что разложение этих множителей неизвестно. Доказывающим происходит выбор двух простых чисел (преимущественно больших) p и q и вычисляется модуль $n = p * q$. Затем в качестве своего личного секретного ключа выбирается случайное число s, такое, что $1 \leq s \leq n-1$, и вычисляется значение $y = s^2 \bmod n$. (Это делается для того, чтобы доказывать проверяющему, то что он знает квадратный корень из y.) Значение y, которое объявляется всем участникам протокола, играет роль открытого ключа в смысле его использования для проверки того, что доказывающий знает s.

Алгоритм протокола состоит из z-кратного повторения раундов, содержащих следующие шаги:

1. Доказывающим выбирается число k, которое удовлетворяет условию $1 \leq k \leq n-1$. Далее происходит вычисление значения $u = k^2 \bmod n$, называемое фиксатором, и это значение отправляется проверяющему. (Число k играет роль разового секретного ключа, это применяется для обеспечения защиты и личного секретного ключа от разглашения при направлении ответа, зависящего от s.).

2. Проверяющий отправляет доказывающему равновероятный случайный бит r ($r = 1$ или $r = 0$).

3. Доказывающий производит вычисление значение $w = k * s^r \bmod n$ и отправляет его проверяющему.

При выполнении равенства $w^2 = u * y^r \bmod n$, проверяющий считает ответ верным.

Вероятность правильного прохождения раунда нарушителем равна 2^{-1}, следовательно, пройти проверку и выдать себя за пользователя, знающего секрет, возможно лишь с вероятностью 2^{-z} [1].

Для сравнительного анализа были выбранные следующие критерии:

Вычислительные затраты и предвычисления – число модульных умножений для обоих сторон.

Требования к памяти – необходимое количество памяти для записи ключей.

Гарантии безопасности – защита от злоумышленника, пытающегося получить доступ к секретной информации.

Кроме вышеупомянутого алгоритма Фиата-Шамира, для сравнения выбраны алгоритмы Гуилоу-Куйсквуатера и Шнорра[3]:

1. Вычислительные затраты. Менее требовательным к вычислительным затратам является алгоритм Фиата-Шамира, для него необходимо от 11 до 20 шагов. Далее идет алгоритм Шнорра, порядка 30 шагов. Заключает список алгоритм Гуилоу-Куйсквуатера с количеством шагов равным 60. Эти данные получены при kt=20 и размере n в 512 бит. Так же можно отметить, что неоптимизированный алгоритм RSA требует порядка 768 шагов.

2. Предвычисления. По совокупности вычислений проверяющей и доказывающей стороны данные алгоритмы приблизительно одинаковы. Алгоритм Шнорра имеет меньше вычислений у доказывающей стороны, из-за необходимости выполнения всего лишь одного модульного умножения (возвести в степень можно в ходе выполнения предвычислений), но у проверяющей стороны требуется большие вычисления, чем в алгоритмах Фиата-Шамира и Гуилоу-Куйсквуатера.

3. Требования к памяти и коммуникационные затраты. В алгоритме Гуилоу-Куйсквуатера имеется возможность снизить требования к необходимой памяти и часть коммуникационных затрат. В других рассматриваемых алгоритмах данная возможность отсутствует.

4. Гарантии безопасности. Все вышеупомянутые алгоритмы способны обеспечить эффективное противодействие злоумышленнику, так как основываются на сложных математических операциях. Алгоритм Фиата-Шамира требует извлечения из числа корня по составному модулю, Гуилоу-Куйсквуатера основывается на невозможности получения из числа v корней по составному модулю, Шнорра требует вычисление дискретного логарифма по модулю простого числа.

Запищим результаты сравнения в сводную таблицу:

Таблица 1

Результаты сводная таблица сравнения.

Алгоритм	Вычислительные затраты	Предвычисления	Требования к памяти	Гарантии безопасности
Фиата-Шамира	+	+–	–	+

Гуилоу-Куйск-вуатера	–	+–	+	+
Шнорра	+–	+–	–	+

В результате сравнения, алгоритм Фиата-Шамира является наилучшим вариантом, т.к. требованиями к памяти на текущий момент развития ЭВМ можно пренебречь.

В результате проведенного исследования было выяснено, что выбранный метод аутентификации, основанный на алгоритме с нулевым разглашением секрета Фиата-Шамира является безопасным для защиты конфиденциальной информации. Так же, в ходе анализа были рассмотрены различные алгоритмы с нулевым разглашением секрета и выявлено, что выбранный алгоритм наиболее оптимальный для ряда основных критериев.

Список литературы

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

2. Протокол Фиата – Шамира // Википедия: свободная энцикл. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Протокол_Фиата_-_Шамира (дата обращения: 20.09.2017).

3. Сравнение протоколов с нулевым разглашением // Cryptowiki: энциклопедия теоритической и прикладной криптографии [Электронный ресурс]. – Режим доступа: http://cryptowiki.net/index.php?title=Доказательства_с_нулевым_разглашением_знания (дата обращения: 17.09.2017).