ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.056.55

Сравнительный анализ алгоритмов электронной подписи

М.В. Ступина, А.Н. Илющенко
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Аннотация. В настоящее время все больше внимания уделяется информационным технологиям, активно используемым в деятельности государственных и муниципальных органов власти, разного вида организаций и самих граждан. К таким информационным технологиям, в частности, относятся системы электронного документооборота. Их растущая популярность приводит к необходимости внедрения в информационные системы (ИС) средств электронной подписи. Проблема такого внедрения заключается в совместимости всех элементов ИС, криптографической стойкости зашифрованных данных, возможности дальнейшей масштабируемости системы. Цель статьи — поиск оптимального алгоритма для реализации электронной подписи в информационной системе с целью упрощения взаимодействия организаций и их клиентов. Для этого проведен сравнительный анализ алгоритмов цифровой подписи и определен оптимальный на сегодняшний день.

Ключевые слова: электронная подпись, криптографические алгоритмы, электронный документооборот.

Comparative Analysis of Electronic Signature Algorithms

Mariya V Stupina, Anastasiya N Ilyushchenko
Don State Technical University, (Rostov-on-Don, Russian Federation)

Abstract. Currently, more and more attention is paid to information technologies that are actively used in the activities of state and municipal bodies, various types of organizations and by citizens themselves. Such information technologies, in particular, include electronic document management systems. The growing popularity of electronic document management systems leads to the need to introduce electronic signature tools into information systems(IS). The problem lies in the compatibility of all the elements of the IS, the cryptographic strength of the encrypted data, the possibility of further scalability of the system. The article objective is to find the optimal algorithm for implementing an electronic signature in an information system in order to simplify the interaction of organizations and their customers. The article provides a comparative analysis of digital signature algorithms and the optimal one for today is determined.

Keywords: electronic signature, cryptographic algorithms, electronic document management.

Введение. Высокую заинтересованность в применении такой инновации, как система электронного документооборота, можно объяснить введением карантина из-за пандемии коронавируса. Многим службам и организациям пришлось отказываться от бумажных вариантов документов, возникла необходимость в привлечении к работе удаленных сотрудников, которые применяют электронные варианты документов, занимаются их обработкой и пересылкой. Данные предпосылки и вызвали необходимость активного развития системы электронного документооборота.

Широкое применение инструментов электронной системы привело к необходимости гарантировать защиту данных, которые применяют в таких операциях. На сегодня одним из эффективных видов обеспечения безопасности является электронная цифровая подпись (ЭЦП), которая подтверждает юридический вес документа.

На основании положений, прописанных в Федеральном законе «Об информации, информационных технологиях и о защите информации», такая подпись определяется как данные, представленные в электронном виде, которые прикрепляются к иным данным (также в электронном варианте), и используется для идентификации личности, которая удостоверяет подписываемые сведения [1]. Сегодня электронная подпись становится все более популярной по причине ее практичности и имеющихся достоинств. В первую очередь, данная подпись — это полный аналог ручного исполнения подписи, ее применяют для подтверждения

официального документа даже в качестве печати, используют в любых организациях, с ее введением значительно упростился документооборот у физических лиц, которым теперь нет необходимости выстаивать длинные очереди в тех или иных учреждениях.

В связи с преимуществами использования электронного документооборота (ЭДО) возникает потребность во внедрении средств электронной подписи в информационные системы организаций. И здесь может возникнуть проблема, которая заключается в совместимости всех элементов информационной системы, криптографической стойкости зашифрованных данных, возможности дальнейшей масштабируемости системы. Поэтому так важно найти оптимальный алгоритм для реализации электронной подписи в информационной системе.

Основная часть. Сравнительный анализ алгоритмов электронной цифровой подписи. Цифровые подписи работают через два взаимно аутентифицирующих криптографических ключа (открытого и закрытого), создаваемых при помощи асимметричного алгоритма шифрования. Лицо, создающее цифровую подпись, использует закрытый ключ для шифрования данных, связанных с подписью. Единственный способ расшифровать эти данные — использовать открытый ключ подписавшего. На сегодняшний день наиболее распространенными последовательностями с открытым доступом стали RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm) и ECDSA (Elliptic Curve Digital Signature Algorithm) [2]. В настоящее время применяется и российский норматив цифровой подписи, представленный в виде ГОСТ Р 34.10-94.

Начальный вариант ЭЦП — это система RSA, которая разрабатывалась в 1977 году в одном из американских институтов на основании математической модели. Подобное шифрование типа с открытым ключом достаточно широко применяется многими продуктами, представленными на рынке цифровых технологий в качестве эффективной защиты. Вышеупомянутая система является блочным шифром, в котором открытый и шифрованный текст представляются целыми числами из диапазона от 0 до n-1, где n может быть различным. Высокая степень защиты при применении данного алгоритма обоснована трудностями распределения на множители больших чисел, а именно на необходимости раскрыть скрытый ключ, опираясь на открытый ключ, потому что для этого потребуется решить задачу о существовании делителей целого числа.

Самые безопасные системы обладают 1024-битовыми и большими числами. Минус ЭЦП данной системы — это то, что при определении модуля и ключей следует провести проверку множества дополнительных пунктов. Если не выполнить любое из данных дополнительных условий, станет возможной подделка подписи той личностью, которая выявляет отсутствие выполнения данного требования. К недостаткам можно также отнести и необходимость реализации множества операций при вычислении, которые больше в среднем на 25 % вычислительных расходов, требуемых при применении прочих технологий цифровой подписи на фоне аналогичной степени безопасности. Также отметим, что система RSA может быть подвержена мультипликативным атакам.

Алгоритм цифровой подписи (DSA) относится к стандарту для цифровых подписей. Он был введен в 1991 году Национальным институтом стандартов и технологий (США). Алгоритм DSA использует уникальные математические функции для создания цифровой подписи, состоящей из двух 160-битных чисел, которые получены из дайджестов сообщений и закрытого ключа. DSA используют открытый ключ для аутентификации подписи, но процесс аутентификации является более сложным по сравнению с RSA. Степень его безопасности основывается на невозможности нахождения решения для конкретной ситуации определения дискретного логарифма. Длина подписи в системе DSA равна 320 бит, что меньше, чем в системе RSA.

ECDSA — один из вариантов DSA-алгоритма. Это алгоритм с открытым ключом, с помощью которого формируется электронная подпись, но, в отличие от DSA, он определяется над полем точек эллиптической кривой, а не над полем целых чисел. Методика шифрования в данном случае базируется на применении дискретных логарифмов в наборе точек эллиптической кривой. Сегодня не существует техники или метода, с помощью которых возможно было бы решить данную задачу. Подобная криптосистема обладает преимуществами перед системами DSA: им характерна более высокая степень прочности при одинаковых затратах времени и труда. Данную степень надежности, которая присутствует в системе DSA с 1024 битами, в этой системе можно получить при длине модуля в 160 бит, что говорит о сравнительно меньших программных и аппаратных затратах.

ГОСТ Р 34.10-2012 является отечественным аналогом цифровой подписи, как и предыдущая версия, ГОСТ Р 034.10-2001. Базируется данный алгоритм на расчетах в группе точек эллиптических кривых и обладает конструкцией, которая схожа с системой ECDSA. Этот алгоритм создания и подтверждения цифровой подписи в нашей стране начал функционировать в начале 2013 года. Надежность норматива ГОСТ Р 34.10-2012 основывается на сложности поиска решения задачи определения дискретного полулогарифма в группе точек

эллиптической кривой. При 512-битном хэш-значении трудность взлома современного алгоритма равна 1,16×10^77 [3].

Первым критерием при сравнении алгоритмов является совместимость. Совместимость программ (program compatibility) определяется их предрасположенностью к выстраиванию связей друг с другом даже в составе комплекса программ. Зачастую организации имеют веб-сайт и мобильное приложение в качестве канала взаимодействия с клиентами/пользователями. Таким образом, программная реализация должна поддерживать аналогичный функционал для всех платформ. Например, если выпуск подписи производился на сайте, то подпись и верификация документа возможна в мобильном приложении и наоборот. Наиболее широкую программную реализацию имеют алгоритмы RSA и ECDSA.

Основным критерием при сравнении алгоритмов является длина ключа для достижения определенного уровня криптостойкости. Криптографическая стойкость определяется способностью криптографической последовательности сопротивляться реализации криптографического анализа. Стойким характеризуется тот последовательный шифр, криптоаналитическое вскрытие которого требует от определенной личности иметь в распоряжении огромные вычислительные ресурсы для дешифровки украденных данных, что делает невозможным получить решение задачи или требует потратить на поиск решения слишком много времени, что в итоге сделает решение уже неактуальным и бесполезным, т. к. полученные данные станут устаревшими и неэффективными [4]. На сегодняшний день RSA — это наиболее широко используемый алгоритм асимметричного шифрования, ECDSA не поддерживается так широко. Однако благодаря своей сложности ECDSA безопаснее всех существующих методов взлома. Поскольку ECDSA существует весьма короткий период времени, у хакеров было мало возможностей, чтобы научиться его взламывать. Минимально рекомендуемое значение уровня криптостойкости является 112 бит. Для его достижения при использовании RSA требуется длина ключа, равная 2048 бит, а при использовании ECDSA — всего 224–255 бит [5].

Ценность производительности и масштабируемости — еще одно большое преимущество ECDSA по сравнению с RSA. Адаптивность — качество вычислительной системы, с помощью которого гарантируется прогнозируемое увеличение системных свойств, например, числа поддерживаемых пользователей, скорости реакции, общей производительности и пр., при повышении вычислительной мощности. Низкая скорость вычисления ключей цифровой подписи может существенно понизить производительность системы. В ECDSA применяется достаточно короткий ключ шифрования, который быстрее вычисляется, в связи с чем требуется меньшая аппаратная мощность по сравнению с аналогами. 160-битный ключ ECDSA гарантирует такую степень защиты, как и 1024-разрядный RSA ключ, но определяется до 15 раз быстрее, в зависимости от базы, на которой используется [6]. Более эффективные, в сравнении с RSA, характеристики ECDSA обладают высокой степенью важности в области применения беспроводных устройств, обладающих ограниченными параметрами мощности, памяти и долговечности аккумулятора.

Заключение. К выбору алгоритма для реализации цифровой подписи следует подходить комплексно, учитывая такие факторы, как криптостойкость алгоритма, совместимость взаимосвязанных частей информационной системы и масштабируемость. В ходе данного исследования был проведен анализ наиболее распространенных ассиметричных алгоритмов цифровой подписи. Было выявлено, что алгоритм ГОСТ Р 34.10-2012 недостаточно поддерживается, DSA является предшественником ECDSA, но более уязвимым, RSA и ECDSA более безопасны и поддерживаемы, однако RSA проигрывает ECDSA по скорости вычисления ключей, что делает ECDSA более простым при масштабировании систем. Поэтому применение ECDSA становится наиболее желательным вариантом.

Библиографический список

1. *Об информации, информационных технологиях и о защите информации*. Федеральный закон от 27.07.2006 № 149-ФЗ. КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 30.04.2023).

2. Чуканов, К.В., Чичикин Г.Я. Цифровые подписи. *Вестник науки и образования.* 2018;16-2(52):20–22.

3. Комарова А.В., Менщиков А.А., Коробейников А.Г. Анализ и сравнение алгоритмов электронной цифровой подписи ГОСТ Р 34. 10-1994, ГОСТ Р 34. 10-2001 и ГОСТ Р 34. 10-2012. *Вопросы кибербезопасности*. 2017;1(19):51–55. URL: https://cyberleninka.ru/article/n/analiz-i-sravnenie-algoritmov-elektronnoy-tsifrovoy-podpisi-gost-r-34-10-1994-gost-r-34-10-2001-i-gost-r-34-10-2012 (дата обращения: 25.03.2023).

4. Шурховецкий, Г. Н. Криптостойкость алгоритмов шифрования. *Молодая наука Сибири*. 2018;2(2):84–91.

5. Melina Richardson. *ECDSA vs RSA: Everything You Need to Know*. Cybers Guards. URL: https://cybersguards.com/ecdsa-vs-rsa-everything-you-need-to-know/ (accessed: 26.03.2023).

6. Соколов А.А. Формирования цифровой подписи на основе эллиптических кривых. *Вестник магистратуры*. 2015;6-1(45):25–30. URL: https://cyberleninka.ru/article/n/formirovaniya-tsifrovoy-podpisi-na-osnove-ellipticheskih-krivyh (дата обращения: 26.03.2023).

Об авторах:

Ступина Мария Валерьевна, доцент кафедры «Информационные технологии» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), кандидат педагогических наук, maria_stupina@mail.ru

Илющенко Анастасия Николаевна, магистрант кафедры «Информационные технологии» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), nastia.ttn@gmail.com

About the Authors:

Mariya V Stupina, associate professor of the Information Technologies Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), Cand. Sci. (Pedagogical), maria_stupina@mail.ru

Anastasiya N Ilyushchenko, Master's degree student of the Information Technologies Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), nastia.ttn@gmail.com