УДК 681.3.06

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КЛАССИЧЕСКИХ И СПЕЦИАЛЬНЫХ АЛГОРИТМОВ И СХЕМ ЦИФРОВОЙ ПОДПИСИ

© 2017 В. Д. Камакин

Воронежский институт высоких технологий (г. Воронеж, Россия)

В данной работе дан сравнительный анализ классических и специальных алгоритмов и схем цифровой подписи.

Ключевые слова: электронная цифровая подпись, алгоритмы.

Оборот электронных документов в самом простом виде происходит так же, как и бумажный документооборот. Вышестоящая организация рассылает распоряжения и указания нижестоящим. В ответ получает регулярные отчеты и рапорты об исполнении. В свою очередь, нижестоящие организации взаимодействуют между собой, обмениваясь документами, необходимыми для выполняемых ими задач. Контроль и сортировку входящей и исходящей документации, а также передачу получаемых документов для отработки конкретному исполнителю о существляет ответственный сотрудник.

Многие виды документов могут гораздо эффективнее доставляться в электронном виде. Это относится как к нормативным актам (особенно копиям, рассылаемым по списку для ознакомления), так и к формам отчетности. Однако для повсеместного внедрения такой практики необходимо, чтобы пересылаемый документ обладал такой же юридической силой, как и его бумажный аналог. Электронный документ может получить статус полноценного, если будет заверен электронной подписью (ЭП).

В соответствии с законом от 06.04.2011 № 63-ФЗ (ред. от 28.06.2014) «Об электронной подписи», ЭП – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Механизм ЭП работает, используя два криптографических ключа – закрытый и открытый, которые генерирует автор (отправитель) сообщения.

Камакин Виктор Дмитриевич – ВИВТ-АНОО ВО, kam13akin2045@yandex.ru.

Закрытый (секретный) ключ ЭП – это последовательность символов, предназначенная для выработки ЭП и известная только правомочному лицу – владельцу. Он использует этот ключ для создания своей подписи под документом.

Открытый (публичный) ключ ЭП – это общедоступная последовательность символов, предназначенная для проверки электронной подписи отправителя. Открытый ключ позволяет только проверять существующую ЭП, но не позволяет «расписаться» вместо отправителя.

Физическое представление ключей ЭЦП зависит от конкретной системы, поддерживающей использование ЭЦП. Чаще всего ключ записывается в файл, который, в дополнение к самому ключу, может содержать, например, информацию о пользователе – владельце ключа, о сроке действия ключа, а также некий набор данных, необходимых для работы конкретной системы.

Данные о владельце ключа позволяют реализовать «побочную», но важную функцию ЭЦП – установление авторства, поскольку при проверке подписи сразу же становится ясно, кто подписал то или иное сообщение. Обычно программы, осуществляющие проверку ЭЦП, настраиваются так, чтобы результат исполнения появлялся на экране в удобном для восприятия виде и с указанием поставившего ЭЦП пользователя, например, так:

«Подпись файла message.doc верна (Автор: Иванов Иван Иванович)».

Как и для всякой последовательности, существует формула вычисления ЭЦП, которую математически можно представить как:

$$S = f(h(M), Ks),$$

где M – текст сообщения, Ks – секретный ключ, h(M) – функция хэширования.

Согласно приведенной зависимости, для формирования ЭЦП в качестве

исходного значения берется не само сообщение, а его хэш (результат обработки сообщения хэш-функцией). Дело в том, что заверяемый подписью текст может быть абсолютно произвольного размера: от пустого сообщения до многомегабайтного файла, содержащего, например, графическую информацию. Но практически все применяемые алгоритмы вычисления ЭЦП используют для расчета сообщения заранее заданной стандартной длины (например, в отечественном алгоритме ЭЦП ГОСТ Р 34.10-94 этот размер определён равным 32 байтам). Задача хэш-функции – из сообщения произвольной длины вычислить цифровую последовательность нужного размера (скажем, 32 байта).

И хотя задача такой хэш-функции вполне тривиальна, сама функция должна удовлетворять определенным требованиям. Прежде всего, необходимо, чтобы результат (хэш сообщения) однозначно соответствовал исходному сообщению и изменялся при любой модификации последнего, даже самой незначительной. Кроме того, хэш сообщения должен вычисляться таким образом, чтобы для любого сообщения M было бы невозможно подобрать такое сообщение M', для которого h(M) = h(M').

Другими словами, трудоемкость успешного вычисления сообщения M' по известному сообщению M и его хэшу h(M), удовлетворяющего условию h(M') = h(M), должна быть эквивалентна трудоемкости прямого перебора сообщений. Невыполнение этого условия создало бы возможность для злоумышленника подменять сообщения, оставляя их подпись верной.

С другой стороны, очевидно, что хэш будет одинаков для многих сообщений, поскольку множество возможных сообщений существенно больше множества возможных хэш-значений (действительно, количество сообщений безгранично, а количество хэш-значений ограничено числом 2N, где N – длина хэш-значения в битах).

К числу наиболее известных функций хэширования принадлежат следующие.

- Отечественный стандарт ГОСТ Р 34.11-94. Вычисляет хэш-значение размером 32 байта.
- MDx (Message Digest) – семейство алгоритмов хэширования, которые наиболее распространены за рубежом. Например, алгоритм MD5 применяется в последних версиях Microsoft Windows для преобразования пароля пользователя в 16-байтное число.
- SHA-1 (Secure Hash Algorithm) – алгоритм вычисления 20-байтного хэш-значения входных данных. Он также очень широко распространен в мире, преимущественно в сетевых протоколах защиты информации.

Помимо средства для создания ЭЦП, хэш-функции успешно используются для аутентификации пользователей. Существует немало криптографических протоколов аутентификации, основанных на применении хэш-функций.

Асимметричные алгоритмы применительно к ЭП предполагают вычисление в процессе ее создания так называемой хэш-функции (хэш-кода) – последовательности нулей и единиц всегда одной и той же длины (российский закон «Об электронной подписи» задает ее равной 256). И хотя длина хэш-кода документа любого размера, на первый взгляд, не представляется большой, идентичные хэш-коды у разных документов могут встретиться с вероятностью меньшей, чем вероятность совпадения отпечатков пальцев у людей. После этого полученный хэш-код «закрывается» секретным ключом лица, подписывающего документ, и ЭП документа как результат описанного процесса добавляется к его исходному тексту. Оформленный таким образом документ и есть документ, подписанный ЭП. Схематично процедура постановки электронной подписи показана на рисунке. По подписи получатель сообщения может удостовериться, что сообщение отправил именно автор, а не кто-то другой. Кроме того, подписанный таким образом документ уже невозможно изменить.

Проверка ЭП под электронным документом для установления его подлинности выполняется с помощью открытого ключа, парного закрытому, который может распространяться свободно и должен быть доступен любому участнику информационного обмена с владельцем закрытого ключа.

Если коды совпали – подпись верна, тогда документ подлинный. Документ также считается подлинным и является действительным, если при создании ЭП действительно использовался секретный ключ того человека, который должен был подписать электронный документ, и при его пересылке содержимое документа не менялось преднамеренно или случайно (например, из-за помех в канале связи). Все

рутинные операции по генерации и проверке ЭП производятся автоматически специальными криптографическими средствами – подсистемой ЭП.

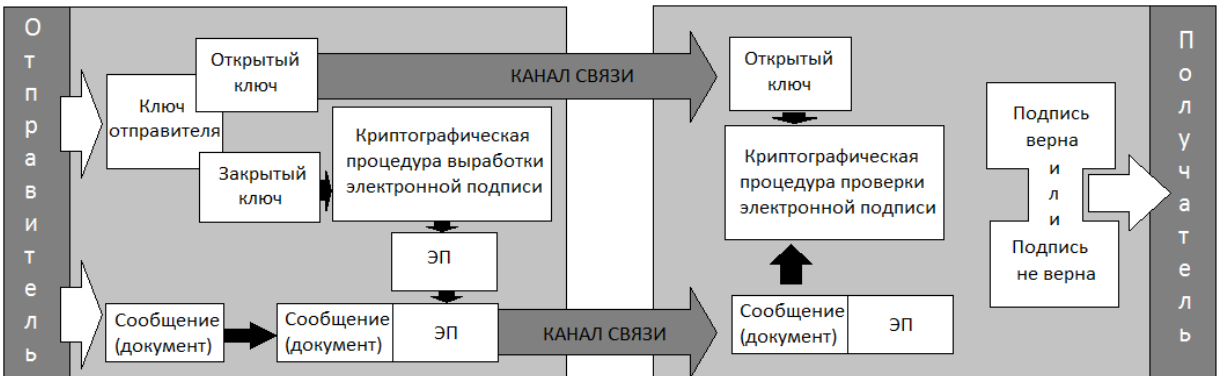

Рисунок. Постановка и проверка ЭП под электронным документом.

Средства создания ЭП могут быть различными. Их правомочность устанавливается законодательно.

Отправитель, кроме подшивки в документ своей ЭП, может еще и зашифровать всё своё сообщение. Соответственно шифрование всего отсылаемого документа и электронная подпись под ним могут применяться отправителем сообщения вместе. Сначала можно подписать документ своим секретным ключом, а потом зашифровать открытым ключом получателя. При этом подпись удостоверяет личность отправителя, а шифрование защищает письмо от чужих глаз.

ЛИТЕРАТУРА

1. Кострова В. Н. Оптимизация распределения ресурсов в рамках комплекса общеобразовательных учреждений / В. Н. Кострова, Я. Е. Львович, О. Н. Мосолов // Вестник Воронежского государственного технического университета. – 2007. – Т. 3. – № 8. – С. 174-176.

2. Преображенский Ю. П. Разработка методов формализации задач на основе семантической модели предметной области / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 075-077.

3. Львович И. Я. Факторы угрозы экономической безопасности государства / И. Я. Львович, А. А. Воронов, Ю. П. Преображенский // Информация и безопасность. – 2006. – Т. 9. – № 1. – С. 36-39.

4. Черников С. Ю. Использование системного анализа при управлении организациями / С. Ю. Черников, Р. В. Корольков // Моделирование, оптимизация и информационные технологии. – 2014. – № 2 (5). – С. 16.

5. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

6. Фомина Ю. А. Принципы индексации информации в поисковых системах / Ю. А. Фомина, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 98-100.

7. Преображенский Ю. П. Информационная безопасность – вызовы современного мира / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2017. – № 2 (21). – С. 60-63.

8. Маричев А. В. Вопросы социальной инженерии в корпоративной информационной безопасности / А. В. Маричев, И. В. Любимов, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2017. – № 2 (21). – С. 64-67.

9. Львович И. Я. Основы информатики / И. Я. Львович, Ю. П. Преображенский, В. В. Ермолова // Воронеж, Издательство: Воронежский институт высоких технологий (Воронеж), 2014. – 339 с.

10. Паневин Р. Ю. Структурные и функциональные требования к программному комплексу представления знаний / Р. Ю. Паневин, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 061-064.

THE COMPARATIVE ANALYSIS OF CLASSICAL AND SPECIAL ALGORITHMS AND SCHEMES OF THE DIGITAL SIGNATURE

© 2017 V. D. Kamakin

Voronezh Institute of High Technologies (Voronezh, Russia)

In the paper the comparative analysis of classical and special algorithms and schemes of the digital signature is given.

Key words: electronic digital signature algorithms.