ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ С ОТКРЫТЫМ КЛЮЧОМ

А.К. Фролов, Д.Н. Шарый
Научные руководители – Матюшков В.Е. – д-р техн. наук, профессор;
Алексеев В.Ф. – канд.техн.наук, доцент
Белорусский государственный университет информатики и радиоэлектроники

Электронная цифровая подпись (ЭЦП) позволяет подтвердить авторство электронного документа (будь то реальное лицо или, например, аккаунт в криптовалютой системе). Подпись связана как с автором, так и с самим документом с помощью криптографических методов, и не может быть подделана с помощью обычного копирования [1].

В настоящие время широко применяется электронная подпись основанная на асимметричном шифровании с открытым ключом. В Республике Беларусь действует стандарт СТБ 34.101.45-2013 "Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых". Им определяются алгоритмы электронной цифровой подписи, которые предназначены для контроля целостности и подлинности сообщений, алгоритмы транспорта ключа. Автор сообщения использует свой личный ключ для выработки электронной цифровой подписи, а связанный с личным ключом открытый ключ используется другими сторонами для проверки электронной цифровой подписи. Алгоритмы выработки и проверки электронной цифровой подписи построены по схеме Шнорра. При выполнении алгоритмов используются вычисления в группе точек эллиптической кривой над конечным простым полем. В стандарте определяются алгоритмы генерации и проверки параметров, описывающих искомую группу. Определены также алгоритм генерации пары ключей (личного и открытого) и алгоритм проверки открытого ключа. Стандарт применяется при разработке средств криптографической защиты информации, в том числе средств электронной цифровой подписи и шифрования [2].

На практике алгоритмы с открытыми ключами недостаточно эффективны для подписания больших документов. Для экономии времени протоколы цифровой подписи нередко используют вместе с хэш-функциями. Хэш-функция — функция, осуществляющая преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом [3]. Шифрование выполняется в прямом направлении. Указания по шифрованию открыты, каждый может зашифровать сообщение. Закрытый ключ делает дешифрование таким же простым, как и шифрование. При этом заметно возрастает скорость и, так как вероятность получить для двух различный документов одинаковое 160-битное значение хэш-функции составляет только один шанс из 2^{160}, можно безопасно приравнять подпись значения хэш-

функции и подпись документа. Также, подпись может быть отделена от документа и значительно уменьшаются требования к объему памяти получателя, в котором хранятся документы и подписи. Архивная система может использовать этот протокол для подтверждения существования документов, не храня их содержания [4].

На рисунке 1 показан алгоритм подписания и проверки электронной цифровой подписи документа.

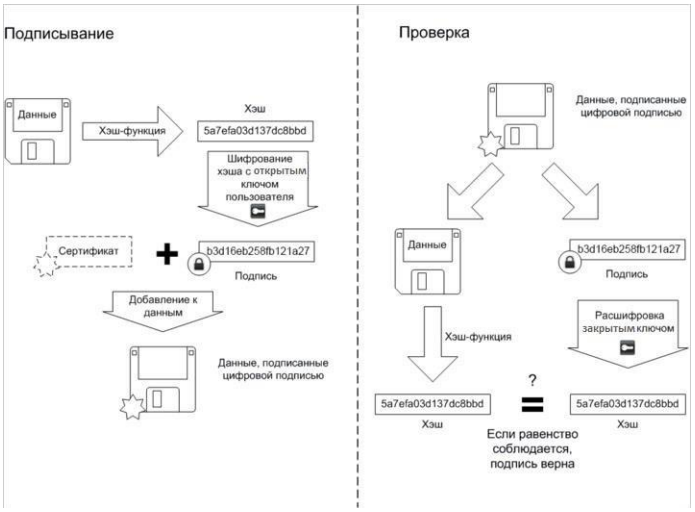

Рис. 1 — Алгоритм подписания и проверки ЭЦП

Асимметричное шифрование с открытым ключом базируется на следующих принципах:

— генерируется открытый и закрытый ключи так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. При этом механизм генерации является общеизвестным;

— надёжные методы шифрования, позволяющие зашифровать сообщение открытым ключом так, чтобы расшифровать его можно было только закрытым ключом. Механизм шифрования является общеизвестным;

— владелец ключей никому не сообщает закрытый ключ, но делает открытый ключ общеизвестным.

Если необходимо передать зашифрованное сообщение владельцу ключей, то отправитель должен получить открытый ключ. Отправитель шифрует свое сообщение открытым ключом получателя и передает его получателю (владельцу ключей) по открытым каналам. При этом расшифровать сообщение не может никто, кроме владельца закрытого ключа [5].

В результате можно обеспечить надёжное шифрование сообщений, сохраняя ключ расшифровки секретным для всех - даже для отправителей сообщений.

Библиографический список

1. Электронная подпись [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Электронная_подпись.

2. СТБ 34.101.45-2013. Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых [Текст]. — Взамен СТБ П 34.101.45-2011; введ. 2014-01-01. — Минск: Госстандарт. — 42 с.

3. Хеш-функция [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Хеш-функция.

4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2002. — 816 с. — 3000 экз.

5. Криптосистема с открытым ключом [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Криптосистема_с_открытым_ключом.