С.А. Педя
Научный руководитель: к.т.н. Е.Е. Канунова
Муромский институт (филиал) Владимирского государственного университета
Владимирская обл., г. Муром, ул. Орловская, д.23

Электронно-цифровая подпись на основе RSA

В современном мире информационные технологии проникли в большинство сфер деятельности человека, что привлекло за собой широкое распространение электронных документов, которые применяются наряду с бумажной документацией, а иногда даже заменяют её. Как и бумажные документы, электронные нуждаются в защите от подделок, существует необходимость подтверждать их подлинность.

Для подтверждения подлинности используется электронно-цифровая подпись — реквизит электронного документа, предназначенный для его защиты от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе [1].

Одним из успешных методов для создания электронно-цифровых подписей на сегодняшний день является метод, в основе которого лежит криптографический алгоритм ассиметричного шифрования RSA. В соответствии с ним в ходе исследовательской деятельности была разработана программа, позволяющая создавать электронно-цифровую подпись документов, что говорит об актуальности разработки в настоящее время. Алгоритм приложения включает в себя следующие этапы:

1. По алгоритму RSA генерируются открытый и закрытый ключи, их можно сохранить в файлы. Для получения ключей генерируются простые числа p и q; вычисляется N = p * q; функция Эйлера — φ(N) = (p - 1) * (q-1); подбирается e взаимно простое с результатом функции Эйлера; находится d, мультипликативно обратное e по модулю φ(N) — d * e = 1 mod φ(N). Пара (e, N) является открытым ключом, а (d, N) закрытым ключом.
2. Получение хэш-кода документа с помощью алгоритма MD5.
3. Получение электронно-цифровой подписи путем шифрования хэш-кода документа с использованием закрытого ключа по формуле: $c = m^d \mathrm{mod} N$, где m — блок шифруемого хэш-кода.

Проверяется электронно-цифровая подпись открытым ключом (e, N) с помощью формулы $r = c^e \mathrm{mod} N$, где r – расшифрованный хэш-код. Если хэш-код документа m совпадает с расшифрованным хэш-кодом электронно-цифровой подписи r, то документ является подлинным. С помощью данных ключей можно подписывать любые документы, однако, закрытый ключ нужно хранить в строжайшем секрете

Разработка позволяет не только генерировать новые электронно-цифровые подписи, но и использовать имеющиеся, с помощью которых осуществляется защита документов, придание им юридической силы, а также идентификация их владельца.

Литература

1 Федеральный закон от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи" Система ГАРАНТ: http://base.garant.ru/184059/1/#block_1#ixzz44W7tyAjK

2 Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - Москва: ДМК Пресс, 2008.- 448 с.