ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ НА ОСНОВЕ СХЕМЫ ШНОРРА

А.В. ИВАШКЕВИЧ, Е.Д. СТРОЙНИКОВА

В настоящее время основу обеспечения безопасности электронного документооборота составляют системы электронной цифровой подписи (ЭЦП). Системы ЭЦП основаны на криптографических алгоритмах. Одним из таких алгоритмов является алгоритм К. Шнорра. Его надежность основана на практической неразрешимости определенного частного случая задачи вычисления дискретного логарифма. Современные методы решения этой задачи имеют приблизительно ту же эффективность, что и методы решения задачи факторизации; в связи с этим предлагается использовать ключи длиной от 512 до 1024 бит. Большая часть вычислений, нужных для генерации подписи и независящих от подписываемого сообщения, может быть выполнена на стадии предварительных вычислений. Эти вычисления могут быть выполнены во время простоя и не влияют на скорость подписания. Следует заметить, что при одинаковом уровне безопасности длина подписей для схемы Шнорра короче, чем для схем RSA и Эль Гамаля. Из практических соображений длина параметров системы, используемых в алгоритме аутентификации, может быть уменьшена: вскрытие за несколько секунд невозможно. Схема Шнорра является одной из наиболее эффективных и теоретически обоснованных схем ЭЦП. На ее основе построен стандарт Республики Беларусь СТБ 1176.2-99, южнокорейские стандарты KCDSA и EC-KCDSA.

Поставленной целью была разработка программного модуля аутентификации пользователей и электронной цифровой подписи на основе алгоритма Шнорра. Для этого были использованы алгоритмы генерации больших псевдопростых чисел с заданной длиной ≈2160 и ≈21024, возведения в степень по модулю, формирования параметров схемы аутентификации, формирования параметров схемы ЭЦП для файла, проверки аутентичности пользователя, проверки ЭЦП файла. На основании алгоритмов был разработан программный продукт с использованием среды Microsoft Visual Studio 2010 и языка программирования C#. Разработанное программное средство позволит значительно сократить время, затрачиваемое на оформление сделки и обмен документацией, усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов, гарантировать достоверность документации, разграничить доступ пользователей в компьютерной сети, минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена, построить корпоративную систему обмена документами.