ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ ПАРАМЕТРОВ ДЛЯ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ СХЕМ ЭЦП НА ОСНОВЕ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

Куржеевский И.В., Толмачёва Ю.С., Шумкова А.А.
Научный руководитель: Куржеевский И.В.
Академия военно-морских сил им. П.С. Нахимова, Украина
E-mail: kurg_igor@mail.ru

Аннотация — Рассматриваются вопросы повышения криптостойкости алгоритмов электронной цифровой подписи (ЭЦП) на основе задачи дискретного логарифмирования.

1. Введение

Дискретным логарифмированием называется задача обращения функции g^x в некоторой конечной мультипликативной группе G. Для заданных g и a решение x уравнения $g^x = a$ по заданному модулю p называется дискретным логарифмом элемента a по основанию g. Криптостойкость схем ЭЦП на основе задачи дискретного логарифмирования базируется на высокой вычислительной сложности обращения показательной функции [1]. Наибольший общий делитель чисел a и n равен единице. Наименьшее из чисел γ, для которого выполняется сравнение $a^\gamma = 1 \bmod n$, называется показателем, которому число a принадлежит по модулю n. Числа, принадлежащие показателю $\varphi(n)$, где $\varphi(n)$ — функция Эйлера, называются первообразными корнями по модулю n [1].

Для повышения криптостойкости схем ЭЦП на основе задачи дискретного логарифмирования в данной работе авторы предлагают в качестве дополнительных параметров использовать рандомизатор k, генерируемый по алгоритму Нидхема-Шредера [6] и параметр H', представляющий собой хеш-значение от общего секретного ключа пользователей K, сформированного по алгоритму Диффи-Хеллмана [2] и параметров ЭЦП r и S.

2. Основная часть

Для потенциального нарушителя в уравнении генерации подписи присутствуют две неизвестные величины: x и k. В качестве случайного значения k при вычислении параметра r используются значения сеансовых ключей, генерируемых по алгоритму Нидхема-Шредера [1]. Для каждого сеанса связи, абоненты А и В вычисляют значение сеансового ключа по следующей схеме. Пусть в течение некоторого времени абоненты А и В договорились об m-сеансах связи; А и В генерируют m-сеансовых ключей последовательно хешируя m-раз общую для них произвольную информацию (M) $h_1=H(M)$, $h_2=H(h_1),\ldots$, $h_{m-1}=H(h_{m-2})$, $h_m=H(h_{m-1})$, а в качестве сеансовых ключей при передачи сообщений применяют эти вычисленные значения в обратном порядке. В схемах ЭЦП в качестве рандомизатора k используется текущее значение сеансового ключа вычисленное по алгоритму Нидхема-Шредера, что позволит осуществить дополнительную проверку подлинности абонентов А и В.

Для повышения криптостойкости схемы ЭЦП с составным модулем применим также алгоритм Диффи-Хеллмана. Абонентам известны некоторые два числа $g^x = a$ и p', которые не являются секретными и могут быть известны также другим заинтересованным лицам (p' — случайное простое число, g — первообразный корень по модулю p'). Для того чтобы создать секретный ключ, оба абонента генерируют большие случайные числа: абонент А — число a, абонент В — число b. Затем абонент А вычисляет значение: $A' = g^a \bmod p'$ и пересылает его абоненту В, который вычисляет: $B' = g^b \bmod p'$ и передаёт абоненту А. На втором этапе первый абонент на основе имеющегося у него a и полученного по сети B' вычисляет значение

$$B'^a \bmod p' = g^{ab} \bmod p',$$

а второй абонент на основе числа b и полученного числа A' вычисляет значение

$$A'^b \bmod p' = g^{ab} \bmod p'.$$

Абоненты А и В сформировывают общий секретный ключ: $K = g^{ab} \bmod p'$. По уравнению формирования подписи вычисляется S: $kH = xr + S \bmod q'$. К общему секретному ключу K добавляются значения параметров ЭЦП r и S и эта совокупность чисел хешируется. Полученное хеш-значение H' является дополнительным параметром ЭЦП. Подписью под электронным документом в этом случае есть совокупность значений (r, S, H').

3. Заключение

Реализованные на языке объектно-ориентированного программирования *Java* в среде *NetBeans IDE* 7.0.1 алгоритмы ЭЦП на основе задачи дискретного логарифмирования, с использованием одноразового сеансового ключа k, сформированного по алгоритму Нидхема-Шредера и дополнительного параметра H', с помощью алгоритма Диффи-Хеллмана, прошли тестирование на правильность результатов формирования и проверки ЭЦП.

4. Список литературы

[1] Молдовян Н.А. Криптография с открытым ключом. / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. — СПб.: БХВ – Петербург, 2004. — 288 с.
[2] Введение в криптографию / под ред. В.В. Ященко. — М.: ЧеРо, 2000. — 287 с.

THE USE OF ADDITIONAL PARAMETERS TO INCREASE THE CRYPTOGRAFIC OF THE EDS ON THE BASIS OF THE DISCRETE LOGARITHM TASK

Kurzheievskyi I.V., Tolmachova Y.S., Shumkova A.A.
Scientific adviser: Kurzheievskyi I.V.
Naval Academy named after P.S. Nakhimov, Ukraine

Abstract — The questions of the cryptographic improving of algorithms of the electronic digital signature (EDS), based on the problem of a discrete finding the logarithm, are considered.