УДК 681.3

РЕАЛИЗАЦИЯ АЛГОРИТМА СОКРАЩЕНИЯ ПОДПИСИ НА ЯЗЫКЕ JAVA

Радчук Юлия, Ипанов Андрей, Куржеевский Игорь

АВМС им. П.С. Нахимова, Украина

Аннотация

Для верификации электронного документа используют электронно-цифровую подпись (ЭЦП). В целях снижения трудоемкости, времени формирования и проверки подписи, её длину можно сократить, но при этом криптостойкость не изменится.

Abstract

We using digital signature for verification the document. We could reduce the length of signature for reduction the labor and time of create and verification signature, but cryptographic strength of signature will not change.

Введение

Электронная цифровая подпись (ЭЦП) — информация в электронной форме, присоединенная к другой информации в электронной форме (электронный документ) или иным образом связанная с такой информацией. Используется для определения лица, подписавшего информацию (электронный документ). По своему существу электронная подпись представляет собой реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП.

Сокращение длины подписи

Для генерации пары ключей (секретного и открытого) в алгоритмах ЭЦП, используются разные математические схемы, основанные на применении однонаправленных функций. Эти схемы разделяются на две группы. В основе такого разделения лежат известные сложные вычислительные задачи: задача факторизации (разложения на множители) больших целых чисел и задача дискретного логарифмирования. Общая схема ЭЦП, основанная на задаче факторизации:

1. Выбираем 2 взаимно простых больших числа p, q
2. Находим их произведение $n = pq$
3. Определяем функцию Эйлера $\phi(n) = (p-1)(q-1)$
4. Выбираем секретный ключ x, при условии $1 < x < \phi(n)$, НОД$(x, \phi(n)) = 1$
5. Вычисляем открытый ключ y, при условии $y < n$, $yx = 1(mod\ \phi(n)) = 1$
6. Вычисляем хеш-значение (H) сообщения
7. Определяем цифровую подпись: $s = H^d(mod\ n)$

Проверка подписи:

1. Вычисляем m' с помощью открытого ключа y, $m' = s^y(mod\ n)$
2. Если m и m' равны, то подпись s - достоверна.

Общая схема ЭЦП, основанная на задаче дискретного логарифмирования:

1. Выбираем общие параметры: простые числа q', p', p.
2. Вычисляем $\alpha = (2^g) mod\ p$, где $g = (p-1)\ div\ q'$.
3. Создаем закрытый ключ x.
4. Вычисляет открытый ключ $y = (\alpha^x) mod\ p$.
5. Выбирает случайное число k.
6. Вычисляет хеш-значение (H) сообщения.
7. ЭЦП состоит из двух чисел (r, s), находим эти параметры по следующим формулам: $r = (\alpha^k) mod\ p$, $s = (r'k - Hx) mod\ q'$, где $r' = r(mod\ q)$.

Проверяем подпись с помощью равенства $r^{r'} = \alpha^s y^H (mod\ p)$, если условия уравнения выполняются, то подпись достоверна.

Для практического использования можно рекомендовать те из них, которые требуют выполнения проверки и формирования подписи с наименьшей трудоёмкостью, но стойкость которой не ниже сложности задачи дискретного логарифмирования. Заметим также, что уравнение проверки подписи и соответствующее ему уравнение формирования подписи могут быть заданы в различных формах[1].

Уравнение проверки подписи может быть задано в двух вариантах: по модулю p-1 или по модулю некоторого числа q, являющегося делителем числа p-1 и имеющего размер 160 и более бит. Известно, что любой делитель числа p-1 является показателем по модулю простого p. Для любого показателя существуют числа β, не превосходящие p-1, для которых выполняются следующие условия:

1. $\beta^q = 1(mod\ p)$;
2. Все числа $\beta, \beta^1, \beta^2, ..., \beta^q$ являются несравнимыми между собой по модулю p;

Эти условия обеспечивают возможность использования уравнений формирования подписи и по модулю q, который по размеру значительно меньше p, что приводит к получению значений $s<q$. Причем для формирования подписи без знания секретного ключа требуется решить задачу дискретного логарифмирования по модулю p, то есть такое сокращение размера числа s не снижает исходной стойкости системы ЭЦП.

Таким образом, использование уравнения вычисления подписи по модулю делителя числа p-1 позволяет сократить длину одного из параметров подписи, а именно значения s. При этом независимо от длины простого модуля p, последний всегда можно выбирать таким образом, чтобы длина q не превосходила 160-256 бит. Это позволяет сократить длину подписи (s,r) почти в два раза по сравнению со случаем использования уравнения вычисления подписи по модулю p-1. Действительно, значение $r(r < p)$ имеет длину примерно равную длине p, которая по соображениям обеспечения высокой стойкости должна быть около 1000 бит или более. Для указанной длины модуля p при использовании 160-битового показателя q можно оценить, что длина подписи сокращается примерно в 1,7 раза. При этом с целью повышения стойкости ЭЦП можно увеличивать размер модуля p, сохраняя размер показателя q. Стойкость ЭЦП будет определяться только длиной простого числа p и правильностью выбора уравнения проверки подписи.

При выборе варианта с вычислением подписи по модулю q мы будем полагать, что в качестве α выбирается некоторое число, относящееся к показателю q по модулю p, то есть такое число, для которого выполняется соотношение

$$\alpha^q = 1(mod\ \ p),$$

где q является простым делителем числа p-1 требуемого размера. Предполагается, что при формаровании простого числа p обеспечивается наличие делителя, имеющего нужный размер, например 160 или 256 бит. При этом в разложении числа p-1 на множители желательно иметь один из делителей большого размера, существенно превышающего размер q, поскольку наличие большого простого делителя в существенной степени повышает сложность задачи дискретного логарифмирования по модулю p. Существуют различные способы формирования простых чисел, удовлетворяющих этим условиям.

В таблице 1 приводятся приемлимые для применения варианты ЭЦП, заданные уравнениями проверки и формирования подписи.

Таблица 1 - Системы ЭЦП с сокращенной длиной подписи,
где $r' = r(mod\ q)$ и $\alpha^q = 1(mod\ p)$

Уравнение для вычисления s	Уравнение проверки подписи
$r'k = s + hx(mod\ \ q)$	$r^{r'} = \alpha^s y^h (mod\ p)$
$r'k = h + sx(mod\ \ q)$	$r^{r'} = \alpha^h y^s (mod\ p)$
$sk = r' + hx(mod\ \ q)$	$r^s = \alpha^{r'} y^h (mod\ p)$
$sk = h + r'x(mod\ \ q)$	$r^s = \alpha^h y^{r'} (mod\ p)$
$hk = s + r'x(mod\ \ q)$	$r^h = \alpha^s y^{r'} (mod\ p)$
$hk = r' + sx(mod\ \ q)$	$r^h = \alpha^{r'} y^s (mod\ p)$

Для повышения криптостойкости в системы ЭЦП, представленные в таблице 1, авторы предлагают в качестве r' использовать значение некоторой сложной функции F, то есть $r' = F(r)$. Эта функция и её параметры будут браться случайно, в зависимости от ключа. То есть, ключ будет изначально хешироваться и это значение будет ключом к криптографически стойкому генератору псевдослучайной последовательности BBS, который будет генерировать саму функцию и параметры к ней. Сложная функция состоит из следующих простых: полинома, синуса, косинуса, тангинса, арксинуса, арккосинуса, арктангинса, гиперболического синуса, гиперболического косинуса и экспоненты.

Список использованных источников:

1. Молдовян Н.А. Введение в криптосистемы с открытым ключом / Н.А. Молдовян, А.А. Молдовян - СПб.: БХВ-Петербург, 2005. - 288 с.