7.3. Стандарт цифровой подписи DSS

Для создания *цифровой подписи* используется алгоритм *DSA* (Digital Signature Algorithm). В качестве хэш-алгоритма стандарт предусматривает использование алгоритма SHA-1 (Secure Hash Algorithm).

DSS использует алгоритм, который разрабатывался для использования только в качестве *цифровой подписи*.

DSS основан на трудности вычисления дискретных логарифмов и базируется на схеме, первоначально представленной ElGamal и Schnorr.

Существует три параметра, которые являются открытыми и могут быть общими для большой группы пользователей.

160-битное простое число q, т.е. $2^{159} < q < 2^{160}$.

Простое число p длиной между 512 и 1024 битами должно быть таким, чтобы q было делителем (p - 1), т.е. $2^{L-1} < p < 2^{L}$, где $512 < L < 1024$ и (p-1)/q является целым.

$g = h^{(p-1)/q} \bmod p$, где h является целым между 1 и (p-1) и g должно быть больше, чем 1,10.

Зная эти числа, каждый пользователь выбирает закрытый ключ и создает открытый ключ.

Закрытый ключ отправителя

Закрытый ключ x должен быть числом между 1 и (q-1) и должен быть выбран случайно или псевдослучайно.

x - случайное или псевдослучайное целое, $0 < x < q$.

Открытый ключ отправителя

Открытый ключ вычисляется из закрытого ключа как $y = g^x \bmod p$. Вычислить y по известному x довольно просто. Однако, имея открытый ключ y, вычислительно невозможно определить x, который является дискретным логарифмом y по основанию g.

$y = g^x \bmod p$

Случайное число, уникальное для каждой подписи.

k - случайное или псевдослучайное целое, $0 < k < q$, уникальное для каждого подписывания.

Подписывание

Для создания подписи отправитель вычисляет две величины, r и s, которые являются функцией от компонент открытого ключа (p, q, g), закрытого ключа пользователя (x), хэш-кода сообщения H (M) и целого k, которое должно быть создано случайно или псевдослучайно и должно быть уникальным при каждом подписывании.

$r = (g^k \bmod p) \bmod q$

$s = [\ k^{-1} (H (M) + xr)\ ] \bmod q$

Подпись = (r, s)

Проверка подписи

Получатель выполняет проверку подписи с использованием следующих формул. Он создает величину v, которая является функцией от

компонент общего открытого ключа, открытого ключа отправителя и хэш-кода полученного сообщения. Если эта величина равна компоненте r в подписи, то подпись считается действительной.

$w = s^{-1} \bmod q$

$u_1 = [\, H(M)\, w \,] \bmod q$

$u_2 = r\, w \bmod q$

$v = [\, (g^{u1}\, y^{u2}) \bmod p \,] \bmod q$

подпись корректна, если $v = r$.