3.2.3. Алгоритм цифровой подписи DSA

Алгоритм DSA (Digital Signature Algorithm – алгоритм цифровой подписи) был предложен Национальным институтом стандартов и технологий в августе 1991. Данный алгоритм вместе с криптографической хеш-функцией SHA-1 является частью DSS (Digital Signature Standard – стандарт цифровой подписи) − криптографического стандарта электронной цифровой подписи, используемой в США. DSA основан на трудности вычисления дискретных логарифмов и базируется на схеме, первоначально представленной Эль-Гамалем и Шнорром.

Алгоритма цифровой подписи DSA состоит в следующем. Сначала необходимо получить секретный и открытый ключи, для этого выполнить следующие действия:

1. Выбрать большое простое число q.

2. Выбрать простое число p такое, что q является делителем $(p-1)$.

3. Подобрать число g такое, что для него верно $g = h^{(p-1)/q} \bmod p$, где h − некоторое произвольное число из интервала $(1, p-1)$, и при этом $g>1$. В большинстве случаев значение $h = 2$ удовлетворяет этому требованию.

4. Закрытый ключ отправителя x выбирается случайно из интервала $(0, q)$.

5. Открытый ключ вычисляется из закрытого ключа по формуле:

$$y = g^x \bmod p. \tag{3.5}$$

Вычислить y по известному x довольно просто (используя алгоритм быстрого возведения в степень). Однако, имея открытый ключ y, вычислительно невозможно определить x, который является дискретным логарифмом y по основанию g.

Открытой информацией являются значения p, q и y, закрытой – x. При этом значения p и q могут быть общими для группы пользователей, а значеие y и x – для каждого свое.

Подпись сообщения выполняется по следующему алгоритму:

1. Получаем хеш-образ исходного сообщения $h(M)$. При использовании формулы 3.2 вычисления необходимо выполнять по модулю числа q.

2. Выбирается случайное число k из $(0, q)$, уникальное для каждого подписи.

3. Вычисляется значение r и s по формулам:

$$\begin{aligned} r &= (g^k \bmod p) \bmod q, \\ s &= k^{-1}(h(M)+x*r) \bmod q. \end{aligned} \tag{3.6}$$

4. Если одно из полученных значений r или s будет равно 0, то необходимо повторить вычисления для другого значения k. Иначе, подписью будет пара значений (r, s).

Таким образом сообщение с подписью будет иметь вид $\{M, r, s\}$.

Для того чтобы проверить подлинность подписи, сначала из полученного сообщения $\{M', r, s\}$вычисляется хеш-образ $h(M')$, после чего находят значение v, используя формулы 3.7. Подпись признается подлинной, если $v = r$.

$$\begin{aligned} w &= s^{-1} \bmod q, \\ u_1 &= h(M)*w \bmod q, \\ u_2 &= r*w \bmod q, \\ v &= (g^{u1}*y^{u2} \bmod p) \bmod q. \end{aligned} \qquad (3.7)$$

Приведем пример данного алгоритма подписи. Возьмем приведенное выше сообщение "БГУИР", хеш-образ которого равен 93. Далее сгенерируем открытый и закрытый ключи для создания подписи. Для этого выберем случайные простые числа q и p, пусть они будут равны соответственно 107 и 643. Как видно $p-1$ (642) делится на q (107) без остатка. Тогда число будет g равно 64. Далее выберем случайное число x = 45, которое будет секретным ключом и храниться в секрете, и вычислим для него открытый ключ по формуле 3.5: $y = = g^x \bmod p = 64^{45} \bmod 643 = 181$. Значение y является открытой информацией.

Вычислим цифровую подпись для сообщения. Для этого возьмем его хеш-образ $h(M)$ = 93, сгенерируем случайное число k = 31, и вычислим r, s по формулам 3.6:

$$r = (g^k \bmod p) \bmod q = (64^{31} \bmod 643) \bmod 107 = 36,$$

$$s = k^{-1}(h(m) + x*r) \bmod q = \frac{1}{31}(93 + 45*36) \bmod 107 = 31^{\varphi(q)-1}*1713 \bmod 107 = 38.$$

Так как оба полученных значения r и s не равны 0, то подпись будет равна паре значений (36, 38). И отправляемое сообщение будет иметь вид: {БГУИР, 36, 38}.

Для проверки подлинности подписи получатель выполняет следующие действия. Сначала он вычисляет хеш-образ сообщения "БГУИР", которое равно 93. Далее вычисляет значение v по формулам 3.8.

$$\begin{aligned} w &= s^{-1} \bmod q = 38^{105} \bmod 107 = 31, \\ u_1 &= h(M)*w \bmod q = 93*31 \bmod 107 = 101, \\ u_2 &= r*w \bmod q = 36*31 \bmod 107 = 46, \\ v &= (g^{u1}*y^{u2} \bmod p) \bmod q = (64^{101}*181^{46} \bmod 643) \bmod 107 = 36. \end{aligned}$$

Так как $r = v$ (36 = 36), то подпись является подлинной.

Задание для выполнения лабораторной работы №3

1. Изучить теоретический материал по лабораторной работе.