## 7.4. Отечественный стандарт цифровой подписи ГОСТ 3410

В стандарте *ГОСТ 3410* используется хэш-функция ГОСТ 3411, которая создает хэш-код длиной 256 бит. Это во многом обуславливает требования к выбираемым простым числам p и q:

p должно быть простым числом в диапазоне

$2^{509} < p < 2^{512}$ либо $2^{1020} < p < 2^{1024}$

q должно быть простым числом в диапазоне

$2^{254} < q < 2^{256}$

q также должно быть делителем (p-1).

Аналогично выбирается и параметр g. При этом требуется, чтобы $g^q \pmod p = 1$.

В соответствии с теоремой Ферма это эквивалентно условию в *DSS*, что $g = h^{(p-1)/q} \bmod p$.

Закрытым ключом является произвольное число x: $0 < x < q$

Открытым ключом является число y: $y = g^x \bmod p$

Для создания подписи выбирается случайное число k: $0 < k < q$

Подпись состоит из двух чисел (r, s), вычисляемых по следующим формулам:

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

$s = (k\ H(M) + xr) \bmod q$

Обратим внимание на отличия *DSS* и *ГОСТ 3410*.

1. Используются разные хэш-функции: в *ГОСТ 3410* применяется отечественный стандарт на хэш-функции ГОСТ 3411, в *DSS* используется SHA-1, которые имеют разную длину хэш-кода. Отсюда и разные требования на длину простого числа q: в *ГОСТ 3410* длина q должна быть от 254 бит до 256 бит, а в *DSS* длина q должна быть от 159 бит до 160 бит.
2. По-разному вычисляется компонента s подписи. В *ГОСТ 3410* компонента s вычисляется по формуле: $s = (k\ H(M) + xr) \bmod q$

В *DSS* компонента s вычисляется по формуле: $s = [k^{-1}\ (H(M) + xr)] \bmod q$

Последнее отличие приводит к соответствующим отличиям в формулах для проверки подписи.

Получатель вычисляет

$w = H(M)^{-1} \bmod q$

$u_1 = w\ s \bmod q$

$u_2 = (q-r)\ w \bmod q$

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

Подпись корректна, если $v = r$.

Структура обоих алгоритмов довольно интересна. Заметим, что значение r совсем не зависит от сообщения. Вместо этого r есть функция от k и трех общих компонент открытого ключа. Мультипликативная инверсия k (mod p) (в случае *DSS*) или само значение k (в случае ГОСТ 3410) подается в

функцию, которая, кроме того, в качестве входа имеет хэш-код сообщения и закрытый ключ пользователя. Эта функция такова, что получатель может вычислить r, используя входное сообщение, подпись, открытый ключ пользователя и общий открытый ключ.

В силу сложности вычисления дискретных логарифмов нарушитель не может восстановить k из r или x из s.

Другое важное замечание заключается в том, что экспоненциальные вычисления при создании подписи необходимы только для $g^k \bmod p$. Так как это значение от подписываемого сообщения не зависит, оно может быть вычислено заранее. Пользователь может заранее просчитать некоторое количество значений r и использовать их по мере необходимости для подписи документов. Еще одна задача состоит в определении мультипликативной инверсии $k^{-1}$ (в случае *DSS*). Эти значения также могут быть вычислены заранее.