Отечественный стандарт цифровой подписи ГОСТ Р 3410-94

Отечественный стандарт цифровой подписи ГОСТ Р3410-94

Используется схема подписи Эль Гамаля, как и в DSS, но другой ее вариант

Используется хэш-функция по ГОСТ Р 34.11 длиной 256 бит

Длина подписи 512 бит

Отечественный стандарт цифровой подписи ГОСТ Р3410-94

Общие для группы пользователей и несекретные параметры

- ***p*** - ***простое*** число в диапазоне: $2^{509} < p < 2^{512}$ либо $2^{1020} < p < 2^{1024}$
- ***q*** - ***простое*** число в диапазоне: $2^{254} < q < 2^{256}$
- число q является делителем числа (p-1)
  $q \mid p-1$
- a - произвольное целое число
  $1 < a < p-1$,
  удовлетворяющее условию $a^q \bmod p = 1$

личный ключ отправителя $0 < x < q;$.

Открытый ключ отправителя $y = a^x \bmod p$

Формирование электронной подписи

Генерируется случайное целое число k в диапазоне $0<k<q$.
Оно является секретным и должно быть уничтожено сразу после выработки подписи

Вычисляют
$r= (a^k \mod p) \mod q$
$s= (xr + kh(M)) \mod q$
.

Подпись сообщения
$r \mod 2^{256}$, $s \mod 2^{256}$

Проверка электронной подписи

Проверка условий:

$0 < s < q$

$0 < r < q$

Если хотя бы одно из этих условий не выполнено, то подпись недействительна

Вычисляют

$v = (h(M_1))^{q-2} \bmod q$

$z_1 = (sv) \bmod q$

$z_2 = ((q-r)\, v) \bmod q$

$u = ((a^{z1}\ y^{z2}) \bmod p) \bmod q$

.

При выполнении условия $r = u$ подпись признается правильной