8.3. Алгоритм цифровой подписи на основе эллиптических кривых ECDSA

Алгоритм ECDSA (Elliptic Curve Digest Signature Algorithm) принят в качестве стандартов ANSI X9F1 и IEEE P1363.

Создание ключей:

1. Выбирается *эллиптическая кривая* $E_p(a,b)$. Число точек на ней должно делиться на большое целое n.
2. Выбирается точка $P \in E_p(a,b)$.
3. Выбирается случайное число $d \in [1, n-1]$.
4. Вычисляется $Q = d \times P$.
5. Закрытым ключом является d, открытым ключом – (E, P, n, Q).

Создание подписи:

1. Выбирается случайное число $k \in [1, n-1]$.
2. Вычисляется $k \times P = (x_1, y_1)$ и $r = x_1 \pmod n$.

Проверяется, чтобы r не было равно нулю, так как в этом случае подпись не будет зависеть от закрытого ключа. Если $r = 0$, то выбирается другое случайное число k.

3. Вычисляется $k^{-1} \bmod n$
4. Вычисляется $s = k^{-1}(H(M) + dr) \pmod n$

Проверяется, чтобы s не было равно нулю, так как в этом случае необходимого для проверки подписи числа $s^{-1} \bmod n$ не существует. Если $s = 0$, то выбирается другое случайное число k.

Подписью для сообщения M является пара чисел (r,s).

Проверка подписи:

1. Проверить, что целые числа r и s принадлежат диапазону чисел [0, n-1]. В противном случае результат проверки отрицательный, и подпись отвергается.
2. Вычислить $w = s^{-1} \pmod n$ и H(M)
3. Вычислить $u_1 = H(M)\, w \pmod n$, $u_2 = rw \pmod n$
4. Вычислить $u_1P + u_2Q = (x_0, y_0)$, $v = x_0 \pmod n$
5. Подпись верна в том и только том случае, когда $v = r$.