✓ modPow $u = v^{e} \bmod m$ ← $(2^{255}-19)$

✓ modInverse $u = v^{m-2} \bmod m$ → m2 ✓

---

sk (256 bits) —SHA512→ a | .... | b

a: &0xF8 → 11111000 clear lowest 3 bits; 31: &0x7F → 01111111 clear highest bit, |0x40 → 01000000 set 2nd highest bit; b → prefix

a (256 bits) little-endian

priv. key → but with highest bit clear, 2nd highest set, lowest 3 cleared → 256 − 1 − 1 − 3 → 251 effective bits

$A = a \cdot B$ pub key $(\bmod m)$

→ exponent always byte array

→ point addition multiplier byte array

Sign $r = SHA512(prefix \,||\, M)$ little-endian

$r \leftarrow r \bmod L$

$R = r \cdot B \pmod m$ → encode

$k = SHA512(R \,||\, A \,||\, M) \bmod L$

$S = (r + k \cdot a) \bmod L$ byte arrays

$B = (X, Y, Z, T)$ Point

A → encode

$x = X \cdot Z^{-1} \bmod m$

$y = Y \cdot Z^{-1}$

$Z^{m-2} \bmod m$

---

recover x-coordinate:

$xx = (y \cdot y - 1) \cdot (d \cdot y \cdot y + 1)^{-1} \bmod m$

$x = xx^{(m+3)/8} \bmod m$

$2^{\frac{m-1}{4}} \bmod m$ const

if (x * x − xx mod m != 0) x = (x * I) mod m

if (x mod 2 != 0) x = m − x