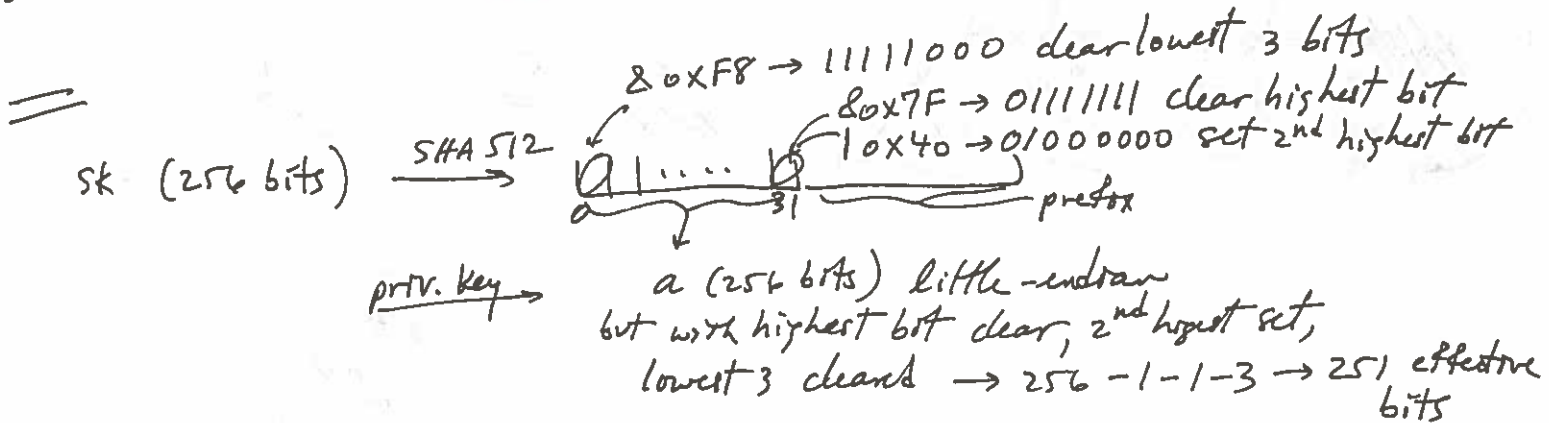


✓ mod Pow $\mu = v^e \bmod m \leftarrow (2^{255} - 19)$

✓ mod Inverse $\mu = v^{m-2} \bmod m$



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

Sign $r = \text{SHA512}(\text{prefix} \parallel M)$ little-endian

$r \leftarrow r \bmod L$

$R = r \cdot B \pmod{m} \rightarrow \text{encode}$

$k = \text{SHA512}(R \parallel A \parallel M) \bmod L$

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

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

$A \rightarrow \text{encode}$

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

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

$z \bmod m$

recover x-coordinate:

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

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

if $(x^2 + x - xx \bmod m \neq 0) \quad x = (x + 1) \bmod m$

if $(x \bmod 2 \neq 0) \quad x = m - x$

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