

Kacper Łasocha



ECDSA

1. Calculate $e = \text{HASH}(m)$, where HASH is a cryptographic hash function
2. Let z be the L_n leftmost bits of e , where L_n is the bit
3. Select a cryptographically secure random integer k
4. Calculate the curve point $(x_1, y_1) = k \times G$.
5. Calculate $r = x_1 \bmod n$. If $r = 0$, go
6. Calculate $s = k^{-1}(z + rd_A) \bmod n$
7. The signature is the pair (r, s) .

$(x_1, y_1) = k \times G$

