Exercise 12.3.4

Consider ECDSA on the elliptic curve $\boldsymbol{E(Z_{17}) : y^2 = x^3 + 2x + 2}$ with $\boldsymbol{G = (5,1), n = 19}$ and $\boldsymbol{s_k = d = 5}$. Let $\boldsymbol{M}$ be a message with $\boldsymbol{hash(M)}$ = 8. Sign $\boldsymbol{M}$ and compute the public key $\boldsymbol{p_k = (p, a, b, n, G, B)}$.

SOLUTION

From the definition: $E(Z_p) : y^2 = x^3 + ax + b$ so $p = 17, a = 2, b = 2$. We need to compute B.

$$B = d \cdot G = 5G(5,1)$$

Compute it using $P + Q = R$ formula.

$x_3 = \lambda^2 - x_1 - x_2$ $\qquad\qquad$ $\lambda = \frac{3x_1^2+a}{2y_1}\ (P = Q)$

$y_3 = -(\lambda x_3 + \varphi)$ $\qquad\qquad$ $\varphi = y_1 - \lambda x_1$

1) Compute $2G = G + G \rightarrow G(5,1) + G(5,1) = R(x_3, y_3)$

$$\lambda = \frac{3 \cdot 5^2 + 2}{2} = 77 \cdot 2^{-1} mod\ 17 = 77 \cdot (-8) mod\ 17 = 13$$

$$\varphi = 1 - 13 \cdot 5 = \ -64\ mod\ 17 = 4$$

$$x_3 = 169 - 5 - 5 = 159\ mod\ 17 = 6$$

$$y_3 = -(13 \cdot 6 + 4) = -82\ mod\ 17 = 3$$

$$2G = (6,3)$$

2) Compute $4G = 2G + 2G \rightarrow 2G(6,3) + 2G(5,1) = R(x_3, y_3)$

$$\lambda = \frac{3 \cdot 6^2 + 2}{2 \cdot 3} = 110 \cdot 6^{-1} mod\ 17 = 110 \cdot (3) mod\ 17 = 7$$

$$\varphi = 3 - 7 \cdot 6 = \ -39\ mod\ 17 = 12$$

$$x_3 = 49 - 12 = 37\ mod\ 17 = 3$$

$$y_3 = -(7 \cdot 3 + 12) = -33\ mod\ 17 = 1$$

$$4G = (3,1)$$

3) Compute $5G = 4G + G \rightarrow 4G(3,1) + G(5,1) = R(x_3, y_3)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1 - 1}{5 - 3} = 0$$

$$\varphi = 1 - 0 \cdot 3 = \ 1$$

$$x_3 = -3 - 5 = 9$$

$$y_3 = -1 = 16$$

$$5G = (9,16)$$

So, $B = 5G(9,16)$ and $\boldsymbol{p_k = \big(17, 2, 2, 19, (5,1), (9,16)\big)}$.

To sign M follow the algorithm:

1) Choose a random integer $k = 4 < n$
2) Compute $R = kG = 4G = (3,1) \rightarrow r = 3$
3) Compute $s = (hash(M) + d \cdot r) \cdot K^{-1}(mod\, n)$

$$s = (8 + 5 \cdot 3) \cdot 4^{-1}\, mod\ 19 =$$
$$= 23 \cdot 5\, mod\ 19 = 1$$

So $\boldsymbol{sign_{sk}(M) = (r, s) = (3, 1)}$.