Elliptic Curve Diffie-Hellman key exchange

1) For $E_{23}(-2, 15)$, consider the point $G=(4,5)$. Find the shared secret key of user A and user B, where the private key of user A is 3 and user B is 7.

Sol:- Given :- Elliptic curve is $E_{23}(-2, 15)$, i.e, $y^2 = x^3 - 2x + 15$

Here, $a=-2$, $b=15$, $p=23$; $G=(4,5)$

User A private key, $n_A = 3$

User B private key, $n_B = 7$

Find the public key of user A and user B :-

(i) User A public key, $P_A = n_A \times G = 3 \times (4,5)$

3G can calculate as G + G + G. So, first find G + G = 2G

$\therefore 2G = 2 \times (x_1, y_1) = 2 \times (4, 5)$

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3(4)^2 + (-2)}{2 \times 5} = \frac{3(16) - 2}{10} = \frac{46}{10} = \frac{23}{5}$$

$$= 23 \cdot 5^{-1} \pmod{23}$$

$$= 23 \times 14 \pmod{23} \quad [\because 5^{-1} \bmod 23 = 14]$$

$$= 322 \bmod 23$$

$\therefore \boxed{\lambda = 0}$

$x_3 = \lambda^2 - x_1 - x_2 = 0^2 - 4 - 4 = 0 - 8 \pmod{23} = -8 \bmod 23$

$\therefore x_3 = 15$

$y_3 = \lambda(x_1 - x_3) - y_1 = 0(4 - 15) - 5 = 0 - 5 = -5 \bmod 23$

$\therefore y_3 = 18$

$\therefore \boxed{2G = (15, 18)}$

$3G = 2G + G = (15, 18) + (4, 5)$

$\Rightarrow \lambda = 3x_1^2 + a$ $\quad \lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5-18}{4-15} = \frac{-13}{-11} = 13 \cdot 11^{-1} \pmod{23}$

$= (13 \bmod 23) \cdot (11^{-1} \bmod 23)$

$= (13 \cdot 21) \bmod 23 = 273 \bmod 23 = 20$

$\therefore \boxed{\lambda = 20}$

$\therefore x_q = \lambda^2 - x_1 - x_2 = 20^2 - 15 - 4 = 381 \bmod 23 = 13$

$y_q = \lambda(x_1 - x_3) - y_1 = 20(15 - 13) - 18 = 20(2) - 18 = 22$

$\therefore x_q, y_q = (13, 22)$

$\therefore \boxed{3G = (13, 22)} \Rightarrow$ Public key of User A

$\therefore P_A = (13, 22)$

(ii) User B public key, $P_B = n_B \times G = 7 \times (4, 5)$

$7G = G + G + G + G + G + G + G$

Already, we find upto $3G$ then find the values of $4G, 5G, 6G, 7G$

$4G = 3G + G = (13, 22) + (4, 5)$

$\Rightarrow \lambda = \frac{5 - 22}{4 - 13} = \frac{-17}{-9} = 17 \cdot 9^{-1} \pmod{23} = 17 \times 18 \pmod{23}$

$\therefore \boxed{\lambda = 7}$

$x_5 = \lambda^2 - x_1 - x_2 = 7^2 - 13 - 4 = 49 - 17 = 9$

$y_5 = \lambda(x_1 - x_3) - y_1 = 7(13 - 9) - 22 = 28 - 22 = 6$

$\therefore x_5, y_5 = (9, 6)$

$\therefore \boxed{4G = (9, 6)}$

$5G = 4G + G = (9, 6) + (4, 5)$

$\Rightarrow \lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5-6}{4-9} = \frac{-1}{-5} \cdot 5^{-1} \bmod 23 = 14$

$\therefore \boxed{\lambda = 14}$

$\therefore x_6 = \lambda^2 - x_1 - x_2 = 14^2 - 9 - 4 \pmod{23} = 22$

$y_7 = \lambda(x_1 - x_3) - y_1 = 14(9 - 22) - 6 \pmod{23} = 19$

$\therefore \boxed{5G = (22, 19)}$

$6G = 5G + G = (22, 19) + (4, 5)$

$\Rightarrow \lambda = \frac{5-19}{4-22} = \frac{7}{9} = 7 \cdot 9^{-1} \pmod{23} = 11$

$\therefore \boxed{\lambda = 11}$

$x_7 = 11^2 - 22 - 4 \pmod{23} = 3$

$y_7 = 11(22 - 3) - 19 \pmod{23} = 6$

$\therefore \boxed{6G = (3, 6)}$

$7G = 6G + G = (3, 6) + (4, 5)$

$\lambda = \frac{5-6}{4-3} = \frac{-1}{1} = -1 \pmod{23} = 22$

$\therefore \boxed{\lambda = 22}$

$\therefore x_8 = 22^2 - 3 - 4 \pmod{23} = -6 \bmod 23 = 17$

$y_8 = 22(3 - 17) - 6 \pmod{23} = -314 \bmod 23 = 8$

$\therefore \boxed{7G = (17, 8)}$

$\therefore$ User B public key, $P_B = (17, 8)$

Calculate Secret key for user A

$$K = n_A \times P_B$$

$$\Rightarrow K = 3 \times (17, 8)$$

Now, find

$2 \times (17, 8) \Rightarrow \lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3(17)^2 - 2}{2 \times 8} \pmod{23} = 82 \bmod 23$

(x_1, y_1; x_2, y_2)

$\therefore \boxed{\lambda = 21}$

$x_3 = \lambda^2 - x_1 - x_2 = [21^2 - 17 - 17] \pmod{23} = 16$

$y_3 = \lambda(x_1 - x_3) - y_1 = [21(17 - 16) - 8] \pmod{23} = 13$

$\therefore \boxed{2 \times (17, 8) = (16, 13)}$

$3 \times P_B = 2P_B + P_B = (16, 13) + (17, 8)$ (x_1, y_1; x_2, y_2)

$\Rightarrow \lambda = \frac{8 - 13}{17 - 16} = \frac{-5}{1} \pmod{23} = 18$

$\therefore \boxed{\lambda = 18}$

$x_4 = \lambda^2 - x_1 - x_2 = 18^2 - 16 - 17 \pmod{23} = 15$

$y_4 = \lambda(x_1 - x_3) - y_1 = 18(16 - 15) - 13 \pmod{23} = 5$

$\therefore \boxed{K = (15, 5)}$

Compute secret key for user B

$$K = n_B \times P_A = 7 \times (13, 22)$$

To find $7P_A = P_A + P_A + P_A + P_A + P_A + P_A + P_A$

$2P_A = 2 \times (13, 22)$ (x_1, y_1; x_2, y_2) $\Rightarrow \lambda = \frac{3(13)^2 - 2}{2 \times 22} \pmod{23} = 12$

$\therefore \boxed{\lambda = 12}$

$x_3 = 12^2 - 13 - 13 \pmod{23} = 3$

$y_3 = 12(13 - 3) - 22 \pmod{23} = 6$

$\therefore \boxed{2P_A = (3, 6)}$

$3P_A = 2P_A + P_A = (\underset{x_1}{3}, \underset{y_1}{6}) + (\underset{x_2}{13}, \underset{y_2}{22})$

$\Rightarrow \lambda = \frac{22-6}{13-3} = \frac{168}{10_5} = 8 \cdot 5^{-1} \pmod{23} = 20$

$\therefore \boxed{\lambda = 20}$

$x_4 = \{20^2 - 3 - 13\} \pmod{23} = 16$

$y_4 = \{20(3-16) - 6\} \pmod{23} = 10$

$\therefore \boxed{3P_A = (16, 10)}$

$4P_A = 3P_A + P_A = (\underset{x_1}{16}, \underset{y_1}{10}) + (\underset{x_2}{13}, \underset{y_2}{22})$

$\Rightarrow \lambda = \frac{22-10}{13-16} \pmod{23} = 19$

$\therefore \lambda = 19$

$x_5 = \{19^2 - 16 - 13\} \pmod{23} = 10$

$y_5 = \{19(16-10) - 10\} \pmod{23} = 12$

$\therefore \boxed{4P_A = (10, 12)}$

$5P_A = 4P_A + P_A = (\underset{x_1}{10}, \underset{y_1}{12}) + (\underset{x_2}{13}, \underset{y_2}{22})$

$\Rightarrow \lambda = \frac{22-12}{13-10} = \frac{10}{3} = 10 \cdot 3^{-1} \pmod{23} = 11$

$\Rightarrow x_6 = \{11^2 - 10 - 13\} \pmod{23} = 6$

$y_6 = [11(10-6) - 12] \pmod{23} = 9$

$\therefore \boxed{5P_A = (6, 9)}$

$6P_A = 5P_A + P_A = (6, 9) + (13, 22)$
$x_1 \quad y_1 \quad x_2 \quad y_2$

$\Rightarrow \lambda = \frac{22-9}{13-6} \pmod{23} = 15$

$\therefore \lambda = 15$

$\Rightarrow x_7 = [15^2 - 6 - 13] \pmod{23} = 22$

$y_7 = [15(6-22) - 9] \pmod{23} = 4$

$\therefore \boxed{6P_A = (22, 4)}$

$7P_A = 6P_A + P = (22, 4) + (13, 22)$
$x_1 \quad x_2 \quad y_1 \quad y_2$

$\Rightarrow \lambda = \frac{22-4}{13-22} \pmod{23} = 21$

$\therefore \lambda = 21$

$\Rightarrow x_8 = [21^2 - 22 - 13] \pmod{23} = 15$

$y_8 = [21(22-15) - 4] \pmod{23} = 5$

$\therefore 7P_A = (15, 5)$

$\therefore \boxed{K = 7 \times (13, 22) = (15, 5)}$

Scanned By Scanner Go