Elliptic Curve Diffie-Hellman (ECDH) key exchange

→ It is a variant of Diffie-Hellman key exchange algorithm using Elliptic Curve Cryptography. (ECC).

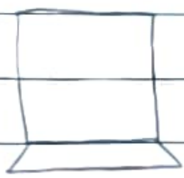
Global Public Elements

$E_q(a,b)$ - Elliptic Curve

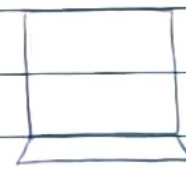
G - point on the Elliptic curve whose order is large value n.

- $G(x, y)$.

Alice



Bob



Key generation by Alice

Select Private key $\boxed{n_A}$

$n_A < n$

Calculate Public Key P_A

$\boxed{P_A = n_A \times G}$

Calculation of shared secret key by Alice

$\boxed{K = n_A \times P_B}$

exchanging public key

Key generation by Bob

$\boxed{n_B}$ Private key

$n_B < n$

Public key P_B

$\boxed{P_B = n_B \times G}$

shared secret key by Bob

$\boxed{K = n_B \times P_A}$

→ This shared secret key can be directly used for encryption or decryption <u>or</u> this shared secret key can be used to compute new key from secret key and that new derived key can be used for symmetric encryption / decryption.

Example ①:

Find the shared secret key for the Elliptic Curve $E_{11}(1,1)$ with a point on the curve (4,6) and the private keys of users A and B are 2 and 4 respectively.

⟹ Given data:

$E_{11}(1,1) \rightarrow p = 11$

$a = 1$

$b = 1$

$G = (4,6)$

$n_A = 2$

$n_B = 4$

→ Global Public Elements

$E_{11}(1,1)$ - Elliptic Curve

$G = (4,6) \in E_{11}(1,1)$

→ User A | User B

Private key $n_A = 2$ | $n_B = 4$

Calculate Public Key

$P_A = n_A \times G$
$= 2(4,6)$
$= (6,6)$

$P_B = n_B \times G$
$= 4(4,6)$
$= (0,10)$

→ for 2(4,6)

since P = Q,

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(4)^2+1}{2(6)} \pmod{11}$$

$$= \frac{49}{12} \pmod{11}$$

$$= 49 \times 12^{-1} \bmod 11$$

$$= 49 \times 1 \pmod{11}$$

$\therefore \lambda = 5$

$$x_3 = \lambda^2 - x - x \pmod p$$

$$= 5^2 - 4 - 4 \pmod{11}$$

$$= 17 \bmod 11$$

$\therefore x_3 = 6$

$$y_3 = \lambda(x - x_3) - y \pmod p$$

$$= 5(4-6) - 6 \pmod{11}$$

$$= -16 \bmod 11$$

$\therefore y_3 = 6$

$2P = 2(4,6) = (x_3, y_3)$

$\therefore 2(4,6) = (6,6)$

→ for 4(4,6)

Since $4P = 2P + 2P$ and $2P = (6,6)$

$$= \underbrace{(6,6) + (6,6)}_{P = Q}$$

$$\lambda = \frac{3x^2 + a}{2y} \pmod{p}$$

$$= \frac{3(6)^2 + 1}{2(6)} \pmod{11}$$

$$= \frac{109}{12} \pmod{11}$$

$$= 109 \times 12^{-1} \pmod{11}$$

$$= 109 \times 1 \pmod{11}$$

$$\therefore \lambda = 10$$

$$X_3 = \lambda^2 - x - x \pmod{p}$$

$$= 10^2 - 6 - 6 \pmod{11}$$

$$= 88 \bmod 11$$

$$\therefore X_3 = 0$$

$$Y_3 = \lambda(x - x_3) - y \pmod{p}$$

$$= 10(6 - 0) - 6 \pmod{11}$$

$$= 54 \bmod 11$$

$$\therefore y_3 = 10$$

$$\therefore 4P = (x_3, y_3) = (0, 10)$$

→ User A

User B

$n_A = 2$

$n_B = 4$

$P_A = 2(4,6)$
$= (6,6)$

$P_B = 4(4,6)$
$= (0,10)$

exchanging public keys

Calculation of shared secret key

$K = n_A \times P_B$
$= 2(0,10)$
$= (3,8)$

$K = n_B \times P_A$
$= 4 \times (6,6)$
$= (3,8)$.

→ for $2(\overset{x}{0}, \overset{y}{10})$
since $P = Q$,

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(0)^2 + 1}{2(10)} \pmod{11}$$

$$\doteq \frac{1}{20} \pmod{11}$$

$$= 1 \times 20^{-1} \bmod 11$$

$$= 9^{-1} \bmod 11$$

$\therefore \lambda = 5$

NOTE: $A^{-1} \bmod B$ if $A > B$ then find $(|A-B|)^{-1} \bmod B$

$[A^{-1} \bmod B = (|A-B|)^{-1} \bmod B]$

→ $20^{-1} \bmod 11 = 9^{-1} \bmod 11$

∴ find M.I. of $9 \bmod 11$

Q	A	B	R	T_1	T_2	$T = T_1 - T_2 Q$
1	11	9	2	0	1	-1
4	9	2	1	1	-1	5
2	2	1	0	-1	5	9
	1	0		$\boxed{5}$	9	

$\therefore 20^{-1} \bmod 11 = 9^{-1} \bmod 11 = 5$

$X_3 = \lambda^2 - x - x \pmod p$
$= 5^2 - 0 - 0 \pmod{11}$
$= 25 \bmod 11$
$\therefore X_3 = 3$

$Y_3 = \lambda(x - x_3) - y \pmod p$
$= 5(0-3) - 10 \pmod{11}$
$= (-15-10) \bmod 11$
$= -25 \bmod 11$
$= -14 \bmod 11 = -3 \bmod 11$
$\therefore Y_3 = 8$

$\therefore 2P = 2(0,10) = (x_3, y_3) = (3,8)$

$\therefore \boxed{K = (3,8)}$

$\rightarrow$ for $4(6,6)$

$$4P = 2P + 2P$$

$\therefore 4(6,6) = 2(6,6) + 2(6,6)$

$\rightarrow$ already computed

$2(6,6) = (0,10)$

$\therefore 4(6,6) = (0,10) + (0,(10))$

$= 2(0,10)$

$\rightarrow$ already computed

$2(0,10) = (3,8)$

$\therefore 4(6,6) = 2(0,10) = (3,8)$

$\therefore \boxed{K = (3,8)}$