

Elliptic Curve Cryptography

Tutorial

Suppose two parties A and B agree on ECC $E_{23}(6, 12)$: $y^2 = x^3 + 6x + 12$ along with base-point $P = (7, 12)$. Let G is a cyclic group generated with P of order 29. Assume that A's private key is $n_A = 7$ and B's private key is $n_B = 10$. Let $k = 3$ be a chosen one-time random number in the encryption algorithm.

- Q • Let A wants to send a message $P_m = (11, 11)$ to B by encrypting using the above ECC. Show with detailed calculations that how A finds the ciphertext of message point P_m ?

1) Find B's public key $P_B = n_B P$

$$\begin{aligned}
 &= 10P \\
 &= 10(7, 12) \\
 &= (19, 4)
 \end{aligned}$$

Diagram illustrating the communication process:

```

    graph LR
      A[A] -- "E23(6,12)" --> B[B]
      A -- "nA=7" --> A
      B -- "nB=10" --> B
      Pm[Pm] -- "C" --> Q[?]
  
```

The diagram shows a communication channel between A and B. A is labeled with $\{P=(7,12)\}$ and $E_{23}(6,12)$. B is labeled with $\{n_B=10\}$. A sends a message P_m to B, which is then encrypted into ciphertext C .

$$\begin{aligned}
 10P &= 8P + 2P \\
 &= ? (19, 4)
 \end{aligned}$$

$$\begin{aligned}
 2P &= P + P = (4, 10) \\
 4P &= 2P + 2P = (17, 17) \\
 8P &= 4P + 4P = (16, 8)
 \end{aligned}$$

$$\frac{A}{P_m = (11, 11)}$$

$$C_1 = KP = 3P$$

$$C_2 = P_m + \underline{KP_B} = P_m + 3P_B$$

$$C_1 = 3P = 3(7, 12) = (15, 21)$$

$$C_2 = (11, 11) + 3(19, 4) = (18, 8)$$

$$C = \{C_1, C_2\} = \{(15, 21), (18, 8)\}$$

$$\frac{B}{\{n_B, P_B = n_B P\}}$$

$$\xrightarrow{C} \boxed{P_m = C_2 - n_B C_1}$$

$$\begin{aligned} Q: & A \langle n_A \rangle \\ & B \langle n_B \rangle \end{aligned}$$

Then what is the DH key?

$$\frac{A}{\langle n_A, P_A \rangle}$$

$$\frac{B}{\langle n_B, P_B \rangle}$$

$$\xrightarrow{P_A} \xleftarrow{P_B}$$

$$K_{AB} = n_A P_B$$

$$K_{BA} = n_B P_A$$

$$\boxed{K_{AB} = K_{BA}}$$

$$7P_B = 7(19, 4) = (2, 3)$$