

Topic: ECC DH Key Exchange

$E_p(a, b)$: Elliptical curve

$$y^2 = (x^3 + ax + b) \text{ mod } p$$

Say G is point on the elliptic curve whose order is large value n . (Note: Order is order of element in group over $E_p(a, b)$ with '+' operator.)

Alice

- (1) Select $n_A < n$
- (2) Calculate $P_A = n_A * G$ (P_A : Public)

Defined over Points (Scalar Multiplication)

Bob

- (1) Select $n_B < n$
- (2) Calculate public $P_B = n_B * G$

- Alice sends P_A to Bob
- Bob sends P_B to Alice
- Alice Computes $K = n_A * P_B$
- Bob Computes $K = n_B * P_A$

Alice

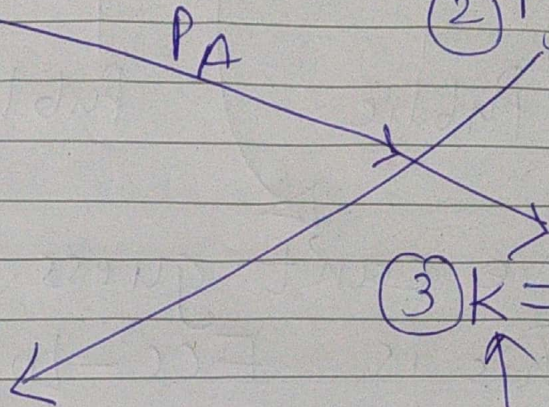
Bob

① $n_A < n$ (select)

① $n_B < n$ (select)

② $P_A = n_A * G$

② $P_B = n_B * G$



③ $K = n_B * P_A$

Secret key

③ $K = n_A * P_B$

Secret key

Verify: $n_A * P_B = n_B * P_A$

LHS = $n_A * P_B$

$= n_A * n_B * G$

RHS = $n_B * P_A$

$= n_B * n_A * G$

$= n_A * n_B * G$

∴ $\boxed{LHS = RHS}$

Note: G, P_A, P_B are Public
 n_A, n_B are Private

★ If Eve gets P_A (Public) i.e.

$$P_A = n_A * G$$

\uparrow \uparrow
 Public Public

Eve can't guess this easily
 → This is Ecc-Logarithm problem

→ It is Difficult when order of elements are Large enough.

★ If Eve gets n_A somehow then she can compute

$$k = n_A * P_B$$

\uparrow \uparrow
 (If Eve knows this) Public

Secret key is revealed in this case.

Simple Example (Try during Lab)

Date _____
Page _____

Ex:

$$E_p(a, b) = E_{257}(0, -4)$$

i.e. $y^2 = (x^3 - 4) \text{ MOD } 257$

Say $\kappa = (2, 12) \in E_{257}(0, -4)$

Bob's private $n_B = 101$

$$\begin{aligned} \therefore P_B &= n_B \cdot \kappa \\ &= 101(2, 12) \\ &= (197, 167) \end{aligned}$$

Alice's private $n_A = 97$

$$\begin{aligned} P_A &= n_A \cdot \kappa \\ &= 97(2, 12) \end{aligned}$$

$$= \boxed{} \leftarrow \text{Find}$$

$$K = n_A * P_B$$

$$= 97 * P_B$$

$$= 97(197, 167)$$

$$K = n_B * P_A$$

$$= 101 * P_A$$

Verify that both are same