Elliptic Curve: Adding pt to itself

$$x_R = \lambda^2 - x_P - x_Q \mod p$$

$$y_R = \lambda(x_P - x_R) - y_P \mod p$$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \mod p \text{ if } P \neq Q$$

$$\Rightarrow \lambda = \frac{3x_P^2 + a}{2y_P} \mod p$$

$y^2 = x^3 + ax + b$

$4a^3 + 27b^2 \neq 0 \mod p$

Example

Curve: $E_{23}(1,1)$ $\quad y^2 = (x^3 + x + 1) \mod 23$

(a, b, p)

$E_p(a,b)$

$P = (13, 7)$ Calculate $2P = (P+P)$

$$\lambda = \frac{3 \cdot 13^2 + 1}{2 \cdot 7} \mod 23$$

$$= (3 \cdot 8 + 1)(14^{-1}) \mod 23$$

$169 - 115 = 54$

$54 - 46 = 8$

$23 = 1 * 14 + 9$

$14 = 1 * 9 + 5$

$9 = 1 + 5 + 4$

$5 = 1 * 4 + 1$

$5 - 1 + 4 = 1$

$5 - (9 - 5) = 1$

$2 \cdot 5 - 1 \cdot 9 = 1$

$2(14 - 9) - 1 \cdot 9 = 1$

$2 \times 14 - 3 \times 9 = 1$

$2 \times 14 - 3(23 - 14) = 1$

$5 \times 14 - 3 \times 23 = 1$

$14^{-1} \equiv 5 \mod 23$

$= (25)(5) \mod 23$

$= 2(5)$

$= 10$

$x_R = \lambda^2 - x_P - x_Q$ ($Q = P$ here)

$= 10^2 - 13 - 13$

$= 100 - 26$

$= 74 \mod 23$

$= \boxed{5}$

$y_R = (\lambda(x_P - x_R) - y_P) \mod p$

$= (10(13-5) - 7) \mod 23$

$= (10 \times 8 - 7) \mod 23$

$= 73 \mod 23$

$= (4)$ $(5, 4)$

$P = (13, 7)$ $2P = (5, 4)$

Elliptic Curve DH

Pick Curve $C(p, a, b)$
Pick generator point g.
] Public

Alice pick X_A calculates $0 \leq X_A < p$

$V_{1A} = X_A \times g \Longrightarrow$ to Bob

V_{1A}: pt; X_A: num; g: pt

Bob pick X_B calculate $0 < X_B < p$

$V_B = X_B \times g \Longrightarrow$ to Alice

Alice gets V_{1B} calculate is

$Key = X_A \times V_{1B}] = X_A \times X_B \times g$

Bob gets V_{1A} calculates

$Key = X_B \times V_{1A} = X_B \times X_A \times g$