Elliptic Curve Summary

$E_p(a,b)$ is eqn $y^2 = (x^3 + ax + b) \bmod p$

$$4a^3 + 27b^2 \not\equiv 0 \pmod p$$

Rules for adding points

Multiplication is Repeated Addition

kQ represents $\underbrace{Q + Q + \dots + Q}_{k \text{ times}}$

Efficient Calculation

Point add(Point Q, int ktimes) {
  if (ktie == 0) return Origin;
  if (ktimes == 1) return Q;
  if (ktimes % 2 == 0) {
    Point tmp = add(Q, ktimes/2);
    return ~~doubleIt~~ regAdd(tmp, tmp);
  }
  Point R = add(Q, ktimes - 1);
  return regAdd(R, Q);
}

Run time is O(log ktimes * cost of Add)

If I know Q and kQ it's hard to

ECC - ONE METHOD

Public Keys

1. $E_p(a,b)$ (cycle length)
2. G is a point with large order, value n.

User A

Select private key n_A $(n_A < n)$

Calculate Public Key $P_A = n_A \times G$.

Encrypt MSG to send to A:

$$C_m = \{\underbrace{kG}_{C_1}, \underbrace{P_m + kP_A}_{C_2}\}$$

randomly selected (like El-Gamal)

$C_2 =$

Alice receives this $P_m + k(n_A \times G)$

$$C_2 = P_m + n_A(kG)$$

Alice takes C_1 and multiplies it by n_A.
This gives her $k \times n_A \times G$.
Calculates $C_2 - k \times n_A \times G$.

Diffie Hellman Key Exchange

$E_p(a,b)$

G

Alice n_A $P_A = n_A G$

Bob n_B $P_B = n_B G$

$$\text{Alice} \xrightarrow{P_A} \text{Bob} \rightarrow n_B \times P_A = n_B \times n_A \times G$$

$$\text{Alice} \xleftarrow{P_B} \text{Bob}$$

$$\downarrow$$

$$n_A \times P_B = n_A \times n_B \times G$$