CIS 3362 11/3/25

Elliptic Curves

$y^2 \equiv (x^3 + ax + b) \bmod p$, $p \in$ Prime

↳ refer to this curve as $E_p(a,b)$.

$E_{23}(1,1) \rightarrow y^2 \equiv (x^3 + x + 1) \bmod 23$

Rule for valid curve: $4a^3 + 27b^2 \neq 0 \pmod p$

1) Additive Identity, O, $P + O = P$

2) $P = (x,y)$, $-P = (x,-y) = (x, p-y)$

$P + (-P) = O$

3) $P + Q = R$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \bmod p$$

mod Inverse

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p$$

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

4) $P + P$ then $\lambda = \frac{3x_P^2 + a}{2y_P} \bmod p$

mod Inverse

For Cryptography, we will repeatedly add a point P to itself. So before we look at the cryptoscheme, let's look at what happens when we a point P over and over again!

With modexpo a prime there was an "order" to each base - the smallest exponent you had to raise it to, to obtain 1, the multicative identity element. For a generator, g, the order was always $p-1$. ($\phi(p)$, $p \in$ Prime.)

For elliptic curves, the order isn't exactly a particular value, but it's even + around p.

In our example with curve $E_{23}(1,1)$ and point $(3,10)$, the order is 28.

$P = (3,10)$ and $Q = 2P = (7,12)$ and cycle size of P is 28, then Q's cycle size is 14. $14 \times (2P) = 28P = O$.

The cycle size of point kP, $k \in \mathbb{Z}^+$

$$= \frac{ord(P)}{gcd(k, ord(P))}$$

, other points with the same cycle size are ones where $gcd(k, ord(P)) = 1$

P, 12P, 18P
2P, 4P, 6P, ... 28P

$9P = (0,1)$

$+$

$13P = (1,7)$

$22P = (12,19)$

$\begin{array}{r} 28 \\ 3 \\ \hline 84 \end{array}$

$Ord(P) = 28$ what is $85P? = (P)$

$85 \equiv 1 \mod 28$ $= (3,10)$

Diffie - Hellman

Public key is $E_p(a,b)$ point G on curve with a large order. (min pos int n for which $nG = O$ is large!), n = order of curve

Alice $\overset{\text{secret}}{\uparrow}$ $n_A < n$ send $n_A \cdot G$ on curve to Bob

Bob secret $n_B < n$ send $n_B \cdot G$ on curve to Alice

Alice receive $n_A(n_B \cdot G)$ then multiply by

Bob will receive $n_B(n_A \cdot G)$ then multiply by

For elliptic curves, it's easy to multiply $k \cdot G$ but given $k \cdot G$ it's hard to determine k.

Public sees both $n_A \cdot G$ and $n_B \cdot G$ but can't calculate the shared key of

$\underbrace{n_A \cdot n_B \cdot G}_{\text{numbers pt.}}$ =] Idea: take 512 least significant bits of x coordinate to be secret shared key.

Something Similar to El-Gamal

Public Elements: $E_p(a,b)$ and G, $n = ord(G)$.

Alice make her own keys so anyone can send a message to Alice.

Alice choose $n_A < n$ as her private key.

Alice computes $P_A = n_A \cdot G$, Alice's public key

Bob to send message M, does this.

1. Choose $k < n$ (doesn't share w/anyone.)
2. Computes $k \cdot G$. This will be $C_1 = k \cdot G$
3. Bob takes $M + k \cdot P_A$ ← Alice's Public key

POINT

$C_2 = M + k \cdot P_A$

Alice receives $C_1 = k \cdot G$, $C_2 = M + k \cdot P_A$

$= M + k \cdot n_A \cdot G$

To recover

1. Alice computes $T = n_A \cdot C_1 = n_A \cdot k \cdot G$
2. Alice recovers $M = C_2 - T$.

$= M + k \cdot n_A \cdot G - n_A \cdot k \cdot G$

SAME

$= M$

Roughly speaking about $\frac{1}{2}$ of all x values have 2 matching y values as solutions, these are known as quadratic residues. Because so many x's have solutions, we can embed the ~~answer~~ message in bits of x.

$$y^2 = c \mod p$$

Does this have a solution for y?

We can answer this question quickly.