CIS 3362 11/4/2024

- RSA
- El Gamal

} Public Key Cryptosystems

Elliptic Curve Cryptography } This might be preferred to RSA is that the keey size doesn't need to be as big to get the same security.

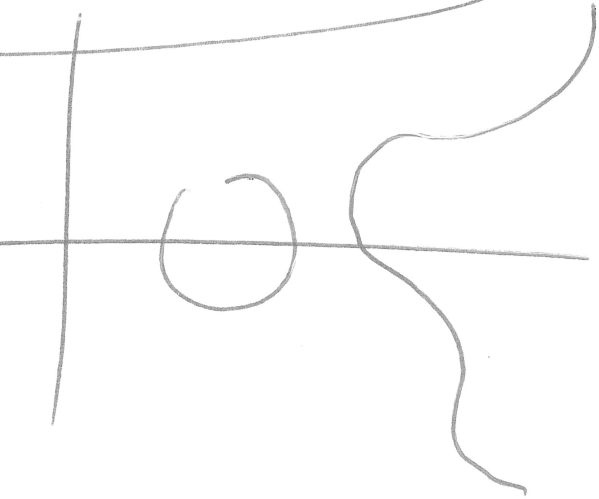
↳ Similar security but faster.

↳ Elliptic Curves

In elliptic curves it's less clear how one would map a binary string or regular text to the plaintext that is an elliptic curve (pt.)

Elliptic Curve in real valued functions

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



$x^3 + 3x^2 + 6x + 2$

$(x+1)^3 = x^3 + 3x^2 + 3x + 1$

$(x+1)^3 + 3x + 1$

$(x+1)^3 + 3(x+1) - 2$

There's no x^2 term because you can take any cubic with an x^2 term and rewrite as an equivalent cubic w/o x^2 term.

But for crypto we usually only deal with ints!

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

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

$$y^2 \equiv (x^3 + x + 1) \bmod 23$$

$$a = 1,\ b = 1,\ p = 23$$

We will refer to this curve as $E_{23}(1,1)$

more generally it's $E_p(a,b)$.

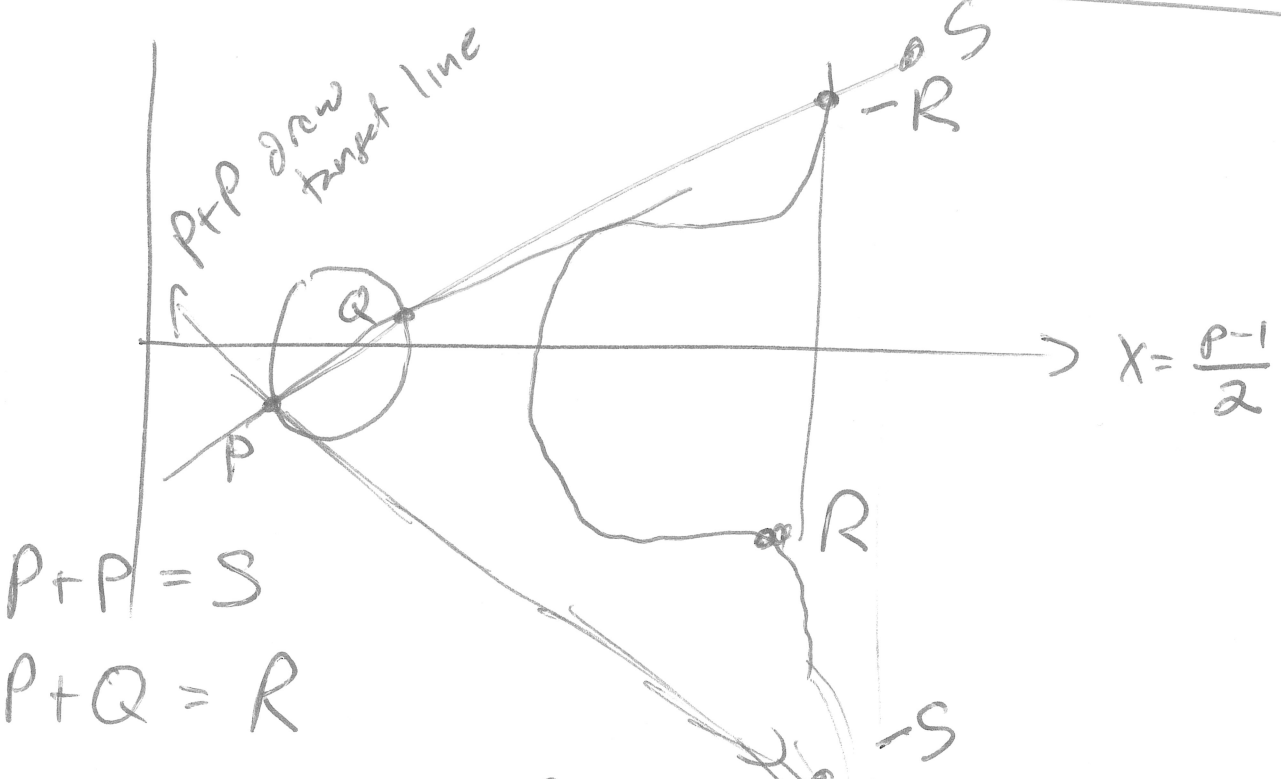
Ultimately some value (x,y) with $0 \le x < p$ $0 \le y < p$ satisfy the equation and some don't.

Usually about p points, give or take a little bit satisfy the equation and are on the elliptic curve.

Some points on $E_{23}(1,1)$: $(1,\underline{7})$, $(1,\underline{16})$ $(3,\underline{0})$, $(3,\underline{13})$, $(4,0)$, $(5,\underline{4})$, $(5,\underline{19})$, ...

We're going to define an operation where we "ADD" points.

Picture of Adding Points on an Elliptic Curve



Draw line btw P and Q. It will hit the curve at a third point. We define this to be $-R$. To get R reflect the point $-R$ about the line $x = \frac{p-1}{2}$.

When you add 2 pts the answer is a third point.

If you keep on adding P+P+P+... you'll eventually get back to P.

HIGH LEVEL IDEA is that we have "Point" generators that allow us to visit the points on the curve in a seemingly random order.

Rules for addition

1. For each point P on E_p curve $P+O=P$, O is additive identity.
2. For each point $P=(x,y)$, $-P=(x,-y)$ under mod $-P=(x, p-y)$. → prime for mod.
   $P+(-P)=O$.
3. Let $P=(x_P,y_P)$, $Q=(x_Q,y_Q)$, We define $R=P+Q$, where $R=(x_R,y_R)$ as follows

   First calculate λ (slope)

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

   if $y_Q - y_P = 20$ and $x_Q - x_P = 5$ then it is valid to say $\lambda = 4$.

   $$\lambda = (y_Q - y_P) \times (x_Q - x_P)^{-1} \bmod p.$$

$20 \times 5^{-1} \bmod 23$

$\equiv 4 \times 5 \times 5^{-1} \bmod 23$

$\equiv 4 \times 1 \bmod 23$

5×20^{-1}

$\equiv 5 \times (4 \times 5)^{-1}$

$\equiv 5 \times 5^{-1} \times 4^{-1}$

$\equiv 4^{-1} \bmod 23$

Calculate x_R, y_R as follows:-

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

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

↳ regular line goes through $-R$ not $+R$.

$y^2 \equiv (x^3 + x + 1) \mod 23$ $\quad a=1, b=1, p=23$

$P = (3,10)$, $Q = (9,7)$
$x_P\ y_P$ $\quad x_Q\ y_Q$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} \mod 23$$

$$\lambda = (-1)(2^{-1}) \mod 23$$

$$\lambda = (-1)(12)$$
$$\equiv -12$$
$$\equiv 11 \mod 23$$

$23 = 11 \times 2 + 1$
$23 - 2 \times 11 = 1$
$-11 \equiv 2^{-1} \mod 23$
$-11 \equiv 12 \mod 23$

$$x_R = (\lambda^2 - x_P - x_Q) = 11^2 - 3 - 9$$
$$= 121 - 12$$
$$= 109 \mod 23$$
$$= \boxed{17 \mod 23}$$

$$y_R = (\lambda(x_P - x_R) - y_P) \mod p$$
$$= 11(3-17) - 10 \mod 23$$
$$= 11(-14) - 10 \mod 23$$
$$\equiv 11 \times 9 - 10 \mod 23$$
$$\equiv 89 \equiv \boxed{20 \mod 23}$$

$$(3,10) + (9,7) = (17,20) \text{ on } E_{23}(1,1)$$

If adding P+P, use this formula for λ:

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

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

$2yy' = 3x^2 + a$

$$\boxed{y' = \frac{3x^2 + a}{2y}}$$

Implicit Diff.

$x_P \; y_P$

$P = (3,10)$ $\boxed{P + P \stackrel{?}{=} (7,12)}$

$$\lambda = \frac{3 \cdot (3)^2 + 1}{2 \times 10} = \frac{28}{20} = \frac{7}{5} = 7(5^{-1}) \mod 23$$

$$= 7(-9) = -63 \equiv 6 \mod 23 \qquad 5^{-1} \equiv -9$$

$$x_R = (\lambda^2 - x_P - x_P) \mod p$$
$$= (6^2 - 3 - 3) \mod 23$$
$$= 30 \equiv \boxed{7 \mod 23}$$

$$y_R = (\lambda(x_P - x_R) - y_P) \mod 23$$
$$= (6(3-7) - 10) = -24 - 10 = -34$$
$$\equiv \boxed{12 \mod 23}$$

$23 = 4 \times 5 + 3$

$5 = 3 + 2$

$3 = 2 + 1$

$3 - 2 = 1$

$2 \times 3 - 1 \times 5 = 1$

$2(23 - 4 \times 5) - 1 \times 5 = 1$

$2 \times 23 - 9 \times 5 = 1$