Pick large prime, p, $p \equiv 3 \bmod 4$ and pick a, b $4a^3 + 27b^2 \not\equiv 0 \bmod p$

let $p = 512 + 64 = 576$ bits, to encode a block size of 512 bits.

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

To make my public keey I need to find a pt on the curve!

1) Plug in a random x to RHS

let $c = x^3 + ax + b$

Question does $y^2 \equiv c \bmod p$ have any solutions? (0, 1 or 2), usually 0 or 2, 1 sol iff $c = 0 \bmod p$.

if 0 → we skip + try again

if 2 → find a solution for y!

Legendre Symbol =

$\left(\frac{c}{p}\right) = 1$ if $\exists y \in \mathbb{Z} \mid y^2 \equiv c \bmod p$ $p \in$ Prime $\wedge c \neq 0$.

$\left(\frac{c}{p}\right) = -1$ if $\nexists y \in \mathbb{Z} \mid y^2 \equiv c \bmod p$

$\left(\frac{c}{p}\right) = 0$ if $c = 0$.

Euler figured out that $\left(\frac{c}{p}\right) = c^{\frac{p-1}{2}} \bmod p$

Note: from Fermat we know if $\gcd(c, p) = 1$

$c^{p-1} \equiv 1 \bmod p$

We know that for all c above $c^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$

If $y^2 \equiv c \mod p$ has solution, what are the values of y that work?

$$y \equiv c^{\frac{p+1}{4}} \mod p$$

$\frac{p+1}{4}$ is only an integer iff $p+1 \equiv 0 \mod 4$, $p \equiv 3 \mod 4$

why is this the answer?

$$y \times y = c^{\frac{p+1}{4}} \times c^{\frac{p+1}{4}} = c^{\frac{p+1}{2}}$$

$$= c^{\frac{p-1}{2}+1} = c^{\frac{p-1}{2}} \times c^1 \equiv 1 \times c \equiv c \mod p$$

if $p \in$ Prime $\wedge$ $p \equiv 3 \mod 4$ $\wedge$ $c^{\frac{p-1}{2}} \equiv 1 \mod p$, then $y_1 = c^{\frac{p+1}{4}}$ is sol to $y^2 = c$.

$y_2 = p - y_1$

Public components: prime p, ints a, b

CURVE $E_p(a,b)$

Alice picks private key n_A

POINT I generated G

Public key $n_A \times G = P_A$

Bob to send Message. Let M be 512 bits.

$p = 576$ bits

$X =$ [64 bits open] | [least 512 bits] OR [counter]

M

Note 10 bits would be enough

While (not done) {

1. fill 64 msb randomly

Cause there's 1024 possible strings to try!

2. Run Legendre Symbol test to see
   Calc $c = x^3 + ax + b \bmod p$
   See if c is a quadratic residue

Prob bc $\left(\frac{1}{2}\right)^{1024}$ mine crazy

3. If c is a quadratic residue, calculate y and break out.

}

$\left(\frac{1}{2}\right)$ Bob gets M encoded as point

$M_p = (x, y)$.

pick secret k. (int)

$C_1 = k \times P_A$ ($= n_A \times G$) $C_2 = M_p + k \times P_A$ ($= n_A \times G$)

When Alice receives C_1, C_2

she computes $C_2 - C_1 = M$

$= M_p + \underbrace{k \times n_A \times G}_{\text{numbers}} - \underbrace{(k \times n_A \times G)}_{\text{numbers}}$

$= M_p$

Goal

1. Pick $p \equiv 3 \bmod 4 \sim 10^6$
2. Get a, b valid
3. Generate point $(x, y) = G$
4. Pick secret n_A, $P_A = n_A \times G$
5. Encode 16-bit message w/ 4 mod bits, see if we can "send it"

$p = 1792267$ $\quad q = 1173956$

$b = 88656$