## ★ Elliptic Curve Crypto-System:

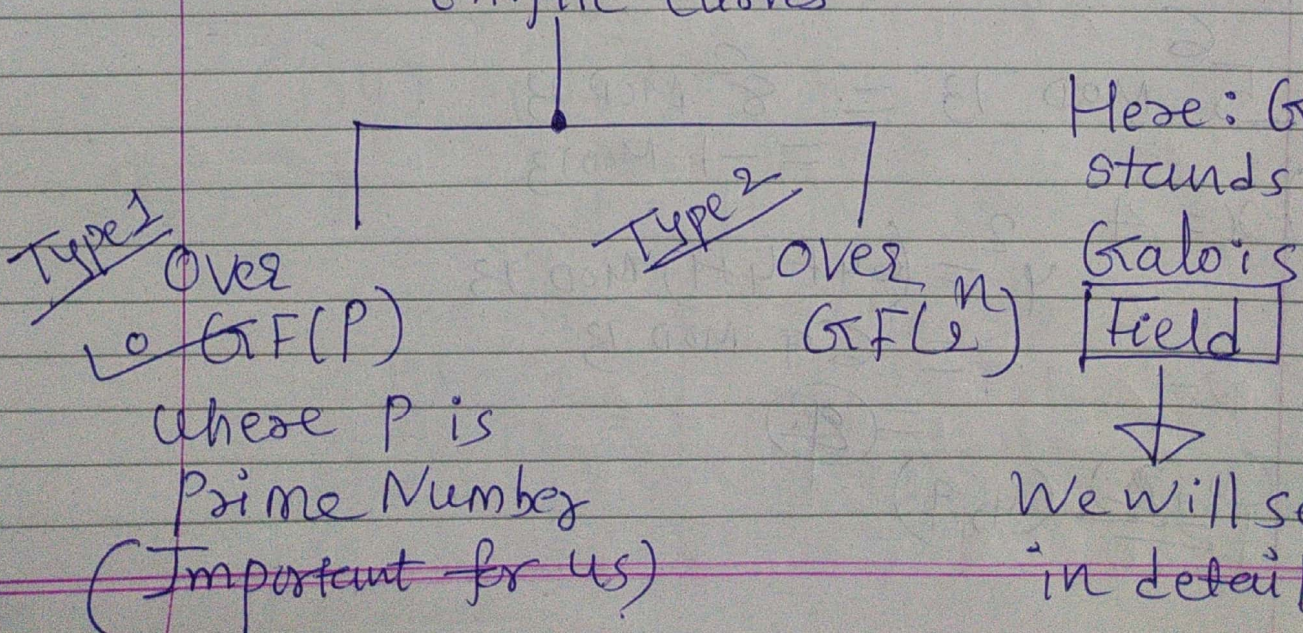
→ Although RSA and Elgamal are asymmetic-key cryptosystems, their security comes with a price, their large keys.

→ Researchers have looked for alternatives that give the same level of security with smaller key sizes.

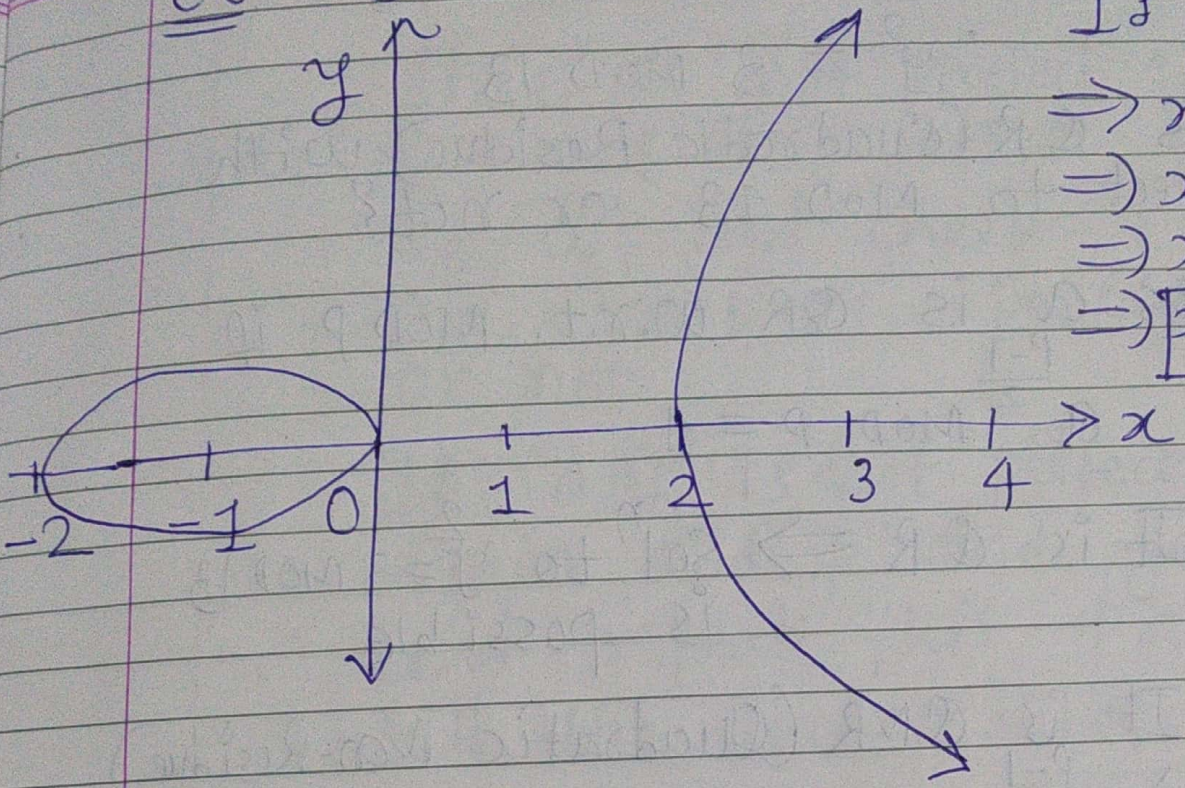
One of the alternative is ECC i.e. Elliptical Curve Cryptography which is based on the theory of elliptic curves.

★ Elliptic curves over real numbers use a special class of elliptic curves of the form

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



E.g. $y^2 = x^3 - 4x$




If $y = 0$

$\Rightarrow x^3 - 4x = 0$

$\Rightarrow x(x^2 - 4) = 0$

$\Rightarrow x(x-2)(x+2) = 0$

$\Rightarrow \boxed{x = 0, 2, -2}$

Ex: Assume that

$$E_p(a,b) = (x^3 + ax + b) \text{ MOD } p$$

where p is prime. a, b are parameters

$E_{13}(1,1) \Rightarrow (x^3 + x + 1) \text{ MOD } 13 = y^2$

i.e. $y^2 = (x^3 + x + 1) \text{ MOD } 13$

(1) $x = 0$, $y^2 = 1 \text{ MOD } 13$

$\therefore y = +1 \text{ MOD } 13$ $\quad y = -1 \text{ MOD } 13 = 12$

$\therefore (0,1)$ $(0,12)$ are two points over $E_{13}(1,1)$

② $x=1 \quad y^2 = (x^3+x+1) \bmod 13$

$\therefore y^2 = 3 \bmod 13$

3 is QR (Quadratic Residue) with respect to MOD 13 or not?

☆ Note: a is QR w.r.t. MOD P if

$a^{\frac{P-1}{2}} \bmod P = 1$

If It is QR $\Rightarrow$ Soln to $y^2 = 3 \bmod 13$ is possible

If It is QNR (Quadratic Non-Residue)

$\Rightarrow a^{\frac{P-1}{2}} \bmod P = -1$ and Soln to $y^2 = 3 \bmod 13$ is not possible

☆ $y^2 = 3 \bmod 13$

$a^{\frac{P-1}{2}} \bmod p = 3^{\frac{13-1}{2}} \bmod 13$

$= 3^6 \bmod 13$

$= (27 \times 27) \bmod 13$

$= 1$

$\Rightarrow a = 3$ is QR (MOD 13)

$\Rightarrow y^2 = 3 \bmod 13$ has two Soln's

☆ How to get soln of $y^2 = a \pmod p$?

If 'a' is not perfect square (4, 16, 9 etc.) then add p to 'a' and check new value i.e. 'a+p' is perfect square or not

If 'a+p' is not perfect square again add 'p' and get 'a+2p' and repeat this process till the $a+kp \leq 69 = 13^2 = p^2$

i.e. $a+kp \leq p^2$

$y^2 = 3 \pmod{13}$

3 is not perfect square

∴ add 13 to 3

i.e. $y^2 = 16 \pmod{13}$

16 is perfect square

$\therefore y = +4 \pmod{13}$ $\quad y = -4 \pmod{13}$

$= 4$ $\quad = 9$

∴ (1, 4), (1, 9) are two other points on the curve $E_{13}(1, 1)$.

③ Put $x=2$

$y^2 = (2^3+2+1) \text{ MOD } 13$

$= 11 \text{ MOD } 13 = a \text{ MOD } p$

$\rightarrow a^{(p-1)/2} \text{ MOD } p = 11^6 \text{ MOD } 13$

$= (11^2 \text{ MOD } 13)^3 \text{ MOD } 13$

$= 4^3 \text{ MOD } 13$

$= 12$

$\equiv -1$

$a^{(p-1)/2} \text{ MOD } p \equiv -1 \text{ Mod } p$

$\Rightarrow a=11$ is QNR w.r.t. MOD P=13

$\Rightarrow$ No soln to $y^2 = 11 \text{ MOD } 13$

④ Put $x=3$

$y^2 = (3^3+3+1) \text{ MOD } 13$

$= 31 \text{ MOD } 13$

$= 5 \text{ MOD } 13$

$= a \text{ MOD } p$

$a^{\frac{p-1}{2}} \text{ MOD } p = 5^6 \text{ MOD } 13$

$= (5^3)^2 = 8^2 \text{ MOD } 13$

$= 12$

$\equiv -1 \text{ MOD } 13$

$\Rightarrow$ No soln!

(5) Put $x=4$,

$$y^2 = (4^3+4+1) \bmod 13$$
$$= 69 \bmod 13$$
$$= 4 \bmod 13$$

↑ Perfect Square

$\therefore y = 2$ $\qquad y = -2 \pmod{13}$

$= 11 \pmod{13}$

$\therefore (4,2)$, $(4,11)$ } are two points over $E_{13}(1,1)$

(6) Put $x=5$

$$y^2 = (5^3+5+1) \bmod 13$$
$$y^2 = 131 \bmod 13$$
$$\therefore y^2 = 1 \bmod 13$$

$\therefore y = 1$ $\qquad y = -1 \pmod{13}$

$= 12$

$\therefore (5,1), (5,12)$ are two points over $E_{13}(1,1)$

(7) Put $x=6$

$$y^2 = (6^3+6+1) \bmod 13$$
$$= 219 \bmod 13$$
$$= 11 \bmod 13$$

$$11^{\frac{13-1}{2}} = 11^6 \bmod 13 = 12 \equiv (-1)$$

$\Rightarrow$ No soln

(8) Put $x=7$

$$y^2 = (7^3+7+1) \bmod 13$$
$$= 351 \bmod 13$$
$$= 0$$

$\therefore (7,0)$ is a point on curve.

(9) Put $x=8$

$$y^2 = (8^3+8+1) \bmod 13$$
$$= 521 \bmod 13$$
$$= 1 \bmod 13$$

$\therefore y = +1$ $\quad y = -1 \bmod 13$

$= 12$

$\therefore (8,1)$ $(8,12)$ are two points over $E_{13}(1,1)$

(10) Put $x=9$

$$y^2 = (9^3+9+1) \bmod 13$$
$$= 739 \bmod 13$$
$$= 11 \bmod 13$$

↳ No sol^n (we have already seen this)

(11) Put $x=10$

$$y^2 = (10^3+10+1) \bmod 13$$
$$= 1011 \bmod 13$$
$$= 10 \bmod 13$$

$10^{\frac{13-1}{2}} = 10^6 \text{ MOD } 13 = (10^2 \text{ MOD } 13)^3 \text{ MOD } 13$

$= 9^3 \text{ MOD } 13$

$= 729 \text{ MOD } 13$

$= 1$

$\Rightarrow$ 10 is QR w.r.t. MOD 13

★ $y^2 = 10$ ✗

$y^2 = 10 + 13 = 23$ ✗

$y^2 = 23 + 13 = 36$ ✓

$y^2 = 36 \text{ MOD } 13$

$\Rightarrow y = +6 \text{ MOD } 13 \quad | \quad y = -6 \text{ MOD } 13$

$= 6 \quad | \quad = 7$

∴ (10, 6) (10, 7) are two points over $E_{13}(1,1)$.

(12) Put $x = 11$

$y^2 = (11^3 + 11 + 1) \text{ MOD } 13$

$= 1343 \text{ MOD } 13$

$= 4 \text{ MOD } 13$

∴ $y = 2 \text{ MOD } 13 \quad y = -2 \text{ MOD } 13$

$= 2 \quad = 11$

∴ (11, 2), (11, 11) are two points over $E_{13}(1,1)$.

(13) Put $x=12$

$$y^2 = (12^3 + 12 + 1) \bmod 13$$
$$= 1741 \bmod 13$$
$$= 12 \bmod 13$$
$$= a \bmod p$$

$$12^{\frac{13-1}{2}} = 12^6 \bmod 13$$
$$= (12 \bmod 13)^6 \bmod 13$$
$$\equiv (-1)^6 \bmod 13$$
$$= 1$$

$\therefore y^2 = 12 \bmod 13$ has two soln's.

$y^2 = 12$ ✗

$y^2 = 12 + 13 = 25$ ✓

$y^2 = 25 \bmod 13$

$\therefore y = +5 \bmod 13$ $\quad y = -5 \bmod 13$

$= 5$ $\quad = 8$

$\therefore \{(12,5), (12,8)\}$ are two points over $E_{13}(1,1)$.

## ★Algo: Pseudo code to find points on an Elliptic Curve

```
EllipticCurve_Points (a, b, p)
{
  x ← 0.
  while (x < p)
  {
    w ← (x^3 + ax + b) MOD p
                          (p-1)/2
Checking for QR ⟶ if (w          MOD p == 1)
    {
      // These are soln's to y^2 = w % p

      → Find √w Mod p and
        -√w Mod p (By adding p to w successively)

      → return √w MOD p, -√w MOD p
    }
                          (p-1)/2
Checking for QNR ⟶ if (w          MOD p == -1)
    { print ("No solution for this")
    }
    x ← x + 1
  }
}
```