Elliptic Curve Cryptography

Dr Mukti Padhya

What are Elliptic Curves

$$E = \{(x, y) \mid y^2 = x^3 + ax + b\}$$

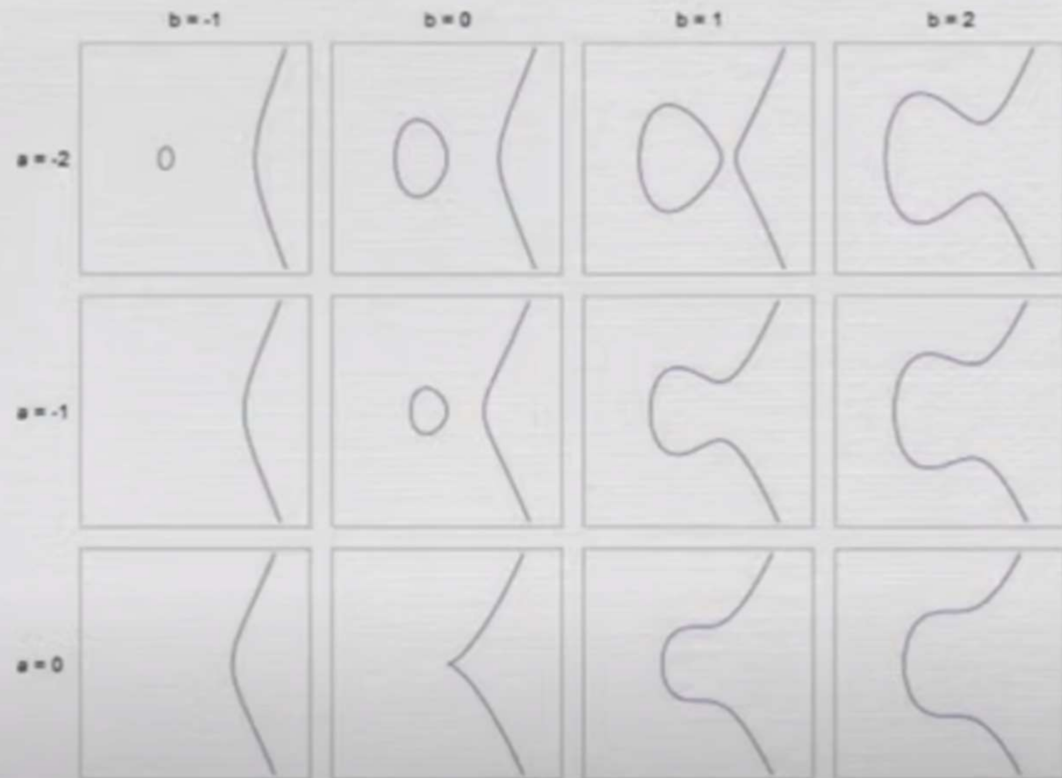
$a, b \in K$

point at infinity: $\mathcal{O}$

$4a^3 + 27b^2 \neq 0$

SOME GRAPHS OF ELLIPTICE CURVES

$\mathbb{R}$



Why Elliptic Curves?

Shorter encryption keys use fewer memory and CPU resources.

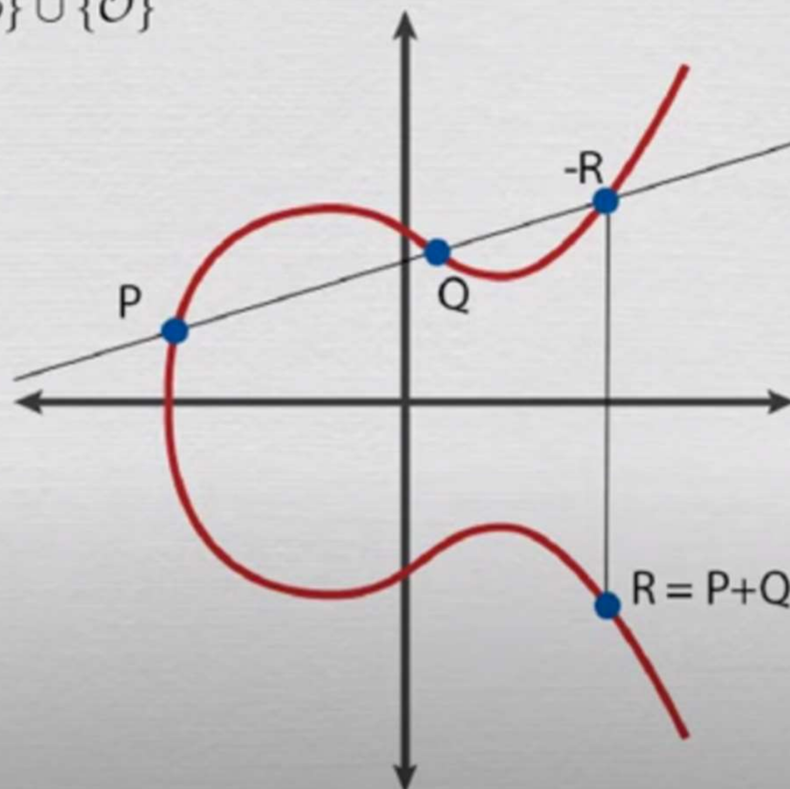
Symmetric Encryption (Key Size in bits)	RSA and Diffie-Hellman (modulus size in bits)	ECC Key Size in bits
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Group Operations

+ ADDITION

point at infinity

Given two points in the set $E = \{(x, y) \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$



P+Q=?

Algebraically

$$s = \frac{y_P - y_Q}{x_P - x_Q}$$

$$x_R = s^2 - (x_P + x_Q)$$

$$y_R = s(x_P - x_R) - y_P$$

Point Doubling

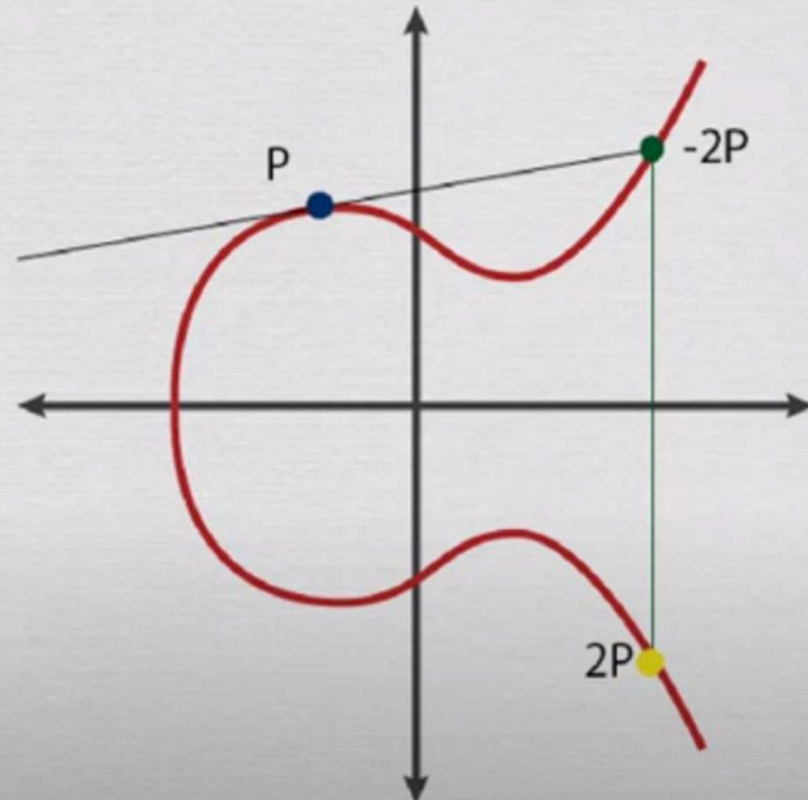
$$P + P = R = 2P$$

Algebraically

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

$$x_R = s^2 - 2x_P$$

$$y_R = s(x_P - x_R) - y_P$$



Scalar Multiplication

$P \in E$

$k \in \mathbb{Z}$

$$Q = kP$$

REPEATED ADDITION

$$Q = P + P + \ldots + P \Big\} \text{ K times}$$

Elliptic Curve Discrete Log Problem

Scalar Multiplication → One Way Function

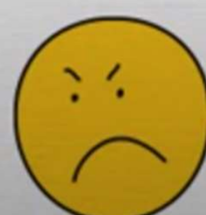
$E(\mathbb{Z}/p\mathbb{Z})$

GIVEN

$Q, P \in E(\mathbb{Z}/p\mathbb{Z})$ Q is a multiple of P

FIND

k such that $Q = kP$



The Base Point (Generator)

$G \in E(\mathbb{Z}/p\mathbb{Z})$ GENERATES A CYCLIC GROUP

$ord(G) = n$ size of subgroup smallest positive integer s.t. $kG = \mathcal{O}$

number of points on the curve

Cofactor: $h = \dfrac{|E(\mathbb{Z}/p\mathbb{Z})|}{n}$

IDEALLY: $h = 1$

Domain Parameters

$$\{p, a, b, G, n, h\}$$

$p:$ field (modulo p)

$a, b:$ curve parameters

$G:$ Generator Point

$n:$ ord(G)

$h:$ cofactor

Elliptic Curce Diffie Hellmann

Bob

Bob picks private key β

$$1 \leq \beta \leq n-1$$

Computes

$$B = \beta G$$

Receives

$$A = (x_A, y_A)$$

Computes

Eve

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

p

a

b

G

n

h

A

B

Alice

Alice picks private key α

$$1 \leq \alpha \leq n-1$$

Computes

$$A = \alpha G$$

Receives

$$B = (x_B, y_B)$$

Computes

The Cyclic Group

COMPUTE $2G = G + G$

$$s = \frac{3x_G^2 + a}{2y_G} \qquad s \equiv \frac{3(5^2)+2}{2(1)} \equiv 77 \cdot 2^{-1} \equiv 9 \cdot 9 \equiv 13 \pmod{17}$$

$$x_{2G} = s^2 - 2x_G \qquad x_{2G} \equiv 13^2 - 2(5) \equiv 16 - 10 \equiv 6 \pmod{17}$$

$$y_{2G} = s(x_G - x_{2G}) - y_G \qquad y_{2G} \equiv 13(5-6) - 1 \equiv -13 - 1 \equiv -14 \equiv 3 \pmod{17}$$

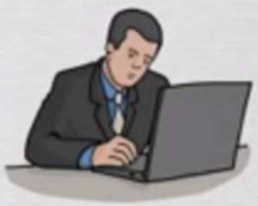
$$2G = (6, 3)$$

An Example

$$E: \quad y^2 \equiv x^3 + 2x + 2 \pmod{17}$$

$$G = (5, 1)$$
$$2G = (6, 3)$$
$$3G = (10, 6)$$
$$4G = (3, 1)$$
$$5G = (9, 16)$$
$$6G = (16, 13)$$
$$7G = (0, 6)$$
$$8G = (13, 7)$$
$$9G = (7, 6)$$
$$10G = (7, 11)$$
$$11G = (13, 10)$$
$$12G = (0, 11)$$
$$13G = (16, 4)$$
$$14G = (9, 1)$$
$$15G = (3, 16)$$
$$16G = (10, 11)$$
$$17G = (6, 14)$$
$$18G = (5, 16)$$
$$19G = \mathcal{O}$$

Bob



Bob picks

$\beta = 9$

Computes

$B = 9G = (7,6)$

Receives

$A = (10,6)$

Computes

$\beta A = 9A = 9(3G) = 27G = 8G = (13,7)$

Eve

$$y^2 \equiv x^3 + 2x + 2 \pmod{17}$$

$G = (5,1)$

$n = 19$

$A = (10,6)$

$B = (7,6)$

Alice

Alice picks

$\alpha = 3$

Computes

$A = 3G = (10,6)$

Receives

$B = (7,6)$

Computes

$\alpha B = 3B = 3(9G) = 27G = 8G = (13,7)$