Elliptic Curve

Part - II

By: Arun Mishra
DIAT, Pune

Elliptic Curve Cryptography

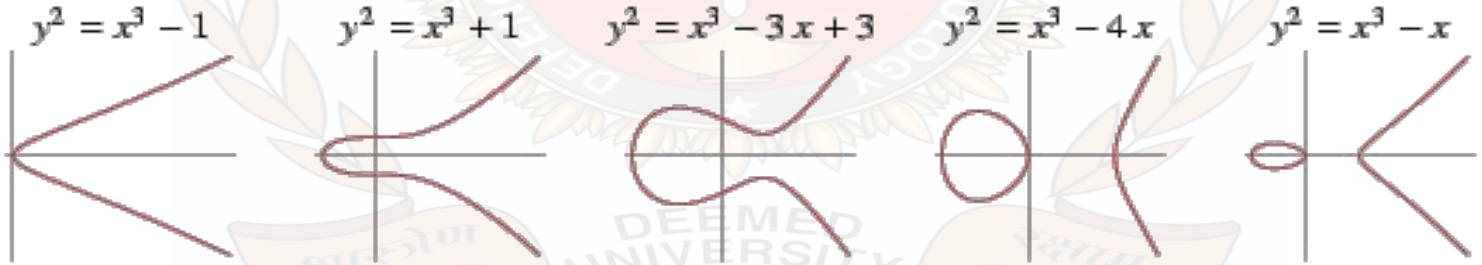
- majority of public-key crypto (RSA, D-H) uses integer arithmetic with very large numbers
- imposes a significant load in storing and processing keys and messages
- an alternative is to use elliptic curves
- **Offers same security with smaller bit sizes**

General form of a EC

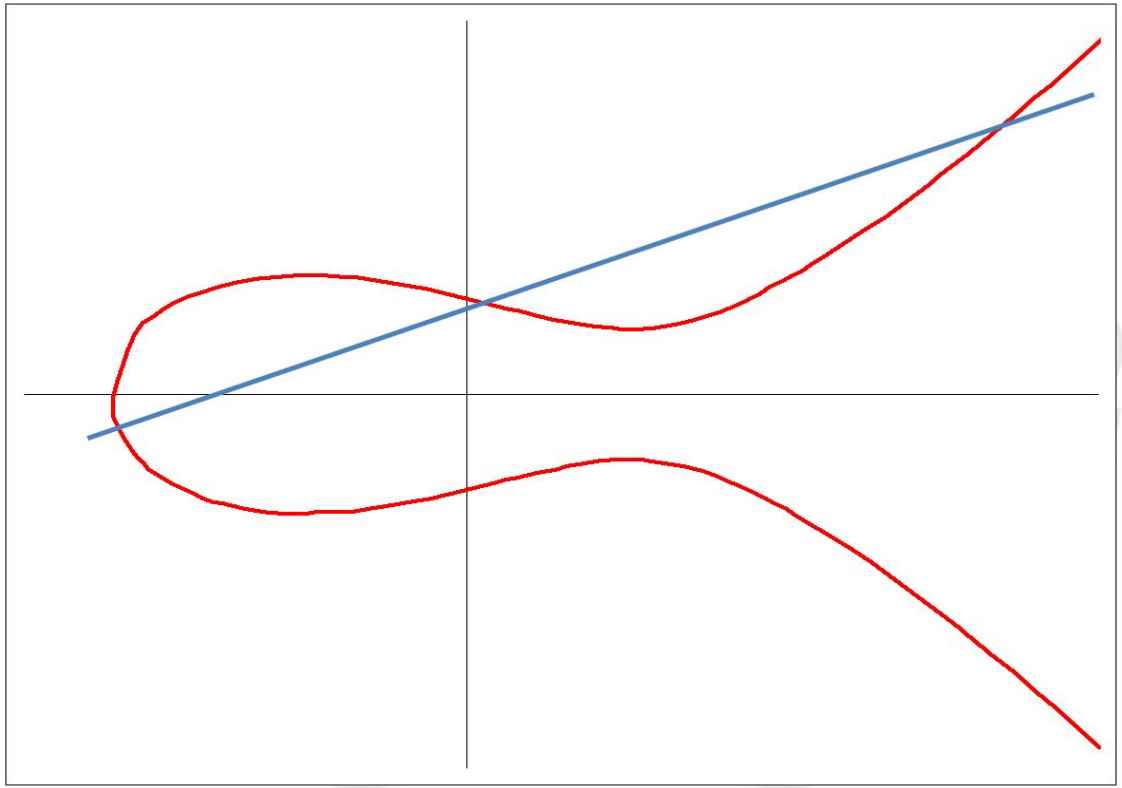
- An elliptic curve is a plane curve defined by an equation of the form

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

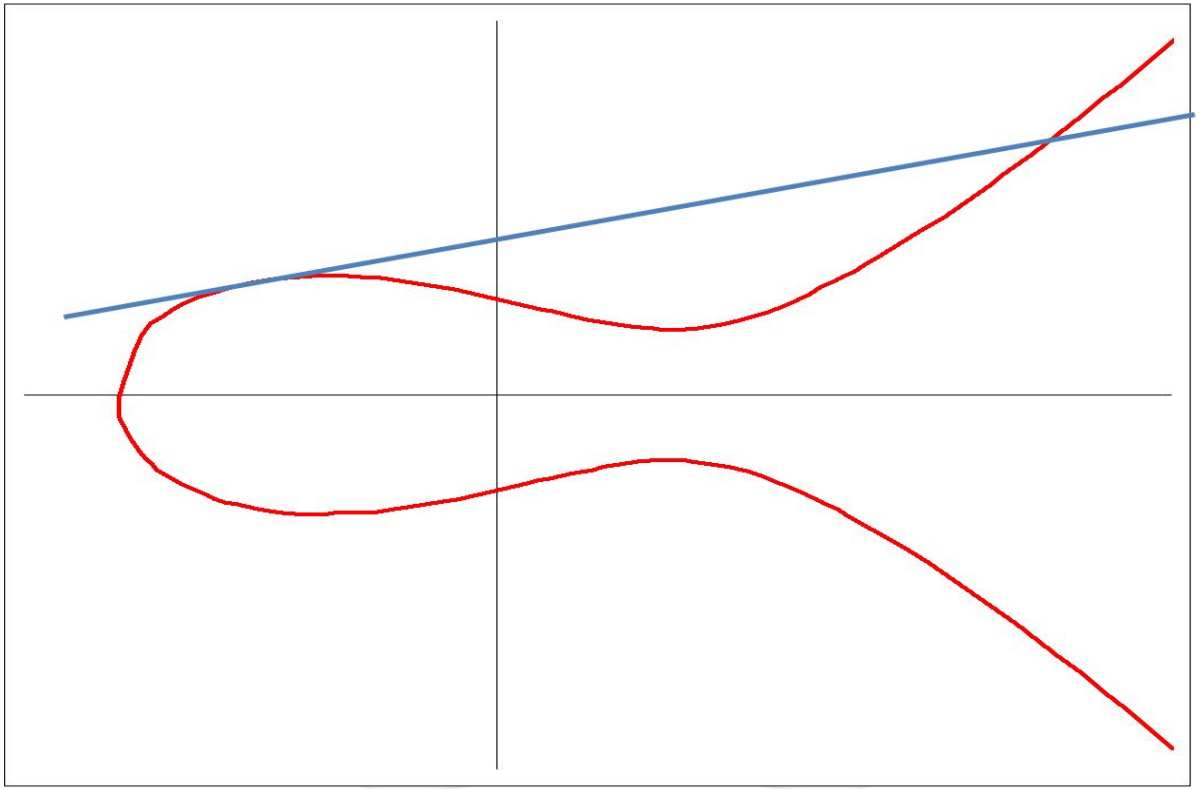
Examples



Elliptic Curve



Elliptic Curve



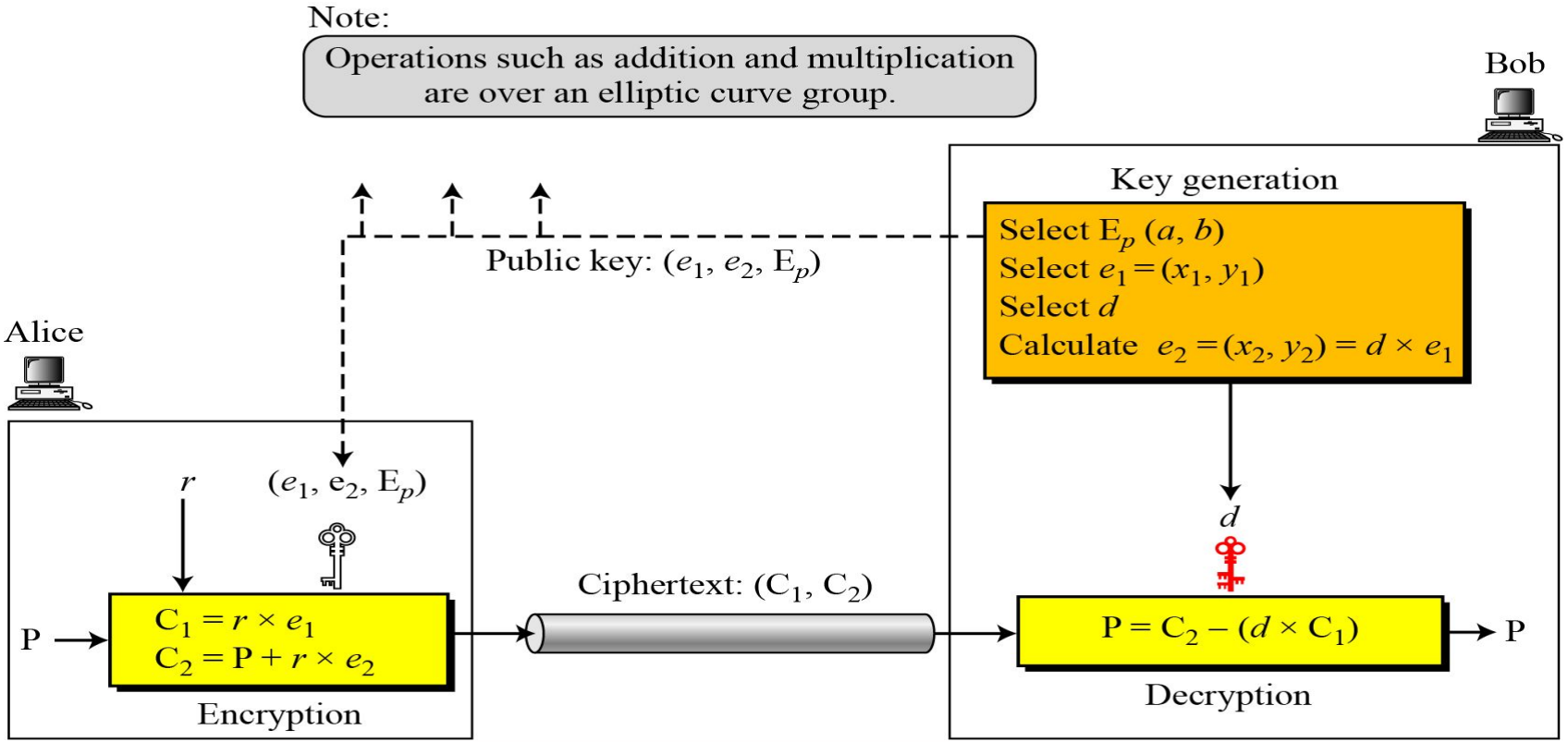
Finite Elliptic Curves

- Elliptic curve cryptography uses curves whose variables & coefficients are finite
- commonly used Method:
  - prime curves Ep(a,b) defined over Zp
    - use integers modulo a prime

Generic Procedures of ECC

- Both parties agree to some publicly-known data items
  - The elliptic curve equation
    - values of a and b
    - prime, p
  - A base point, B, taken from the elliptic curve
    - Similar to the generator used in current cryptosystems
- Each user generates their public/private key pair
  - Private Key = an integer, x, selected from the interval [1, p-1]
  - Public Key = product, Q, of private key and base point
    - (Q = x*B)

Generic Procedures of ECC to ElGamal



Generating Public and Private Keys

$E(a, b)$ $e_1(x_1, y_1)$ d $e_2(x_2, y_2) = d \times e_1(x_1, y_1)$

Encryption $C_1 = r \times e_1$ $C_2 = P + r \times e_2$

Decryption

$P = C_2 - (d \times C_1)$ The minus sign here means adding with the inverse.

How it Works

- P = C2 – (d * C1)

  = P + r* e2 – (d*r*e1)

  = P + (r*d*e1)- (r*d*e1) = P + 0 = P

Example – Elliptic Curve Cryptosystem

example of encipherment using an elliptic curve over GF(p).

1. *Bob selects $E_{67}(2, 3)$ as the elliptic curve over GF(p).*
2. *Bob selects $e_1 = (2, 22)$ and $d = 4$.*
3. *Bob calculates $e_2 = (13, 45)$, where $e_2 = d \times e_1$.*
4. *Bob publicly announces the tuple (E, e_1, e_2).*
5. *Alice wants to send the plaintext $P = (24, 26)$ to Bob. She selects $r = 2$.*

Finding an Inverse

- The reflection of point (x , y) is (x, -y)

  (-y is the additive inverse of y)

Example :

If p =13, the inverse of (4,2) is …….

Thank You!