Elliptic Curve Cryptography(ECC)

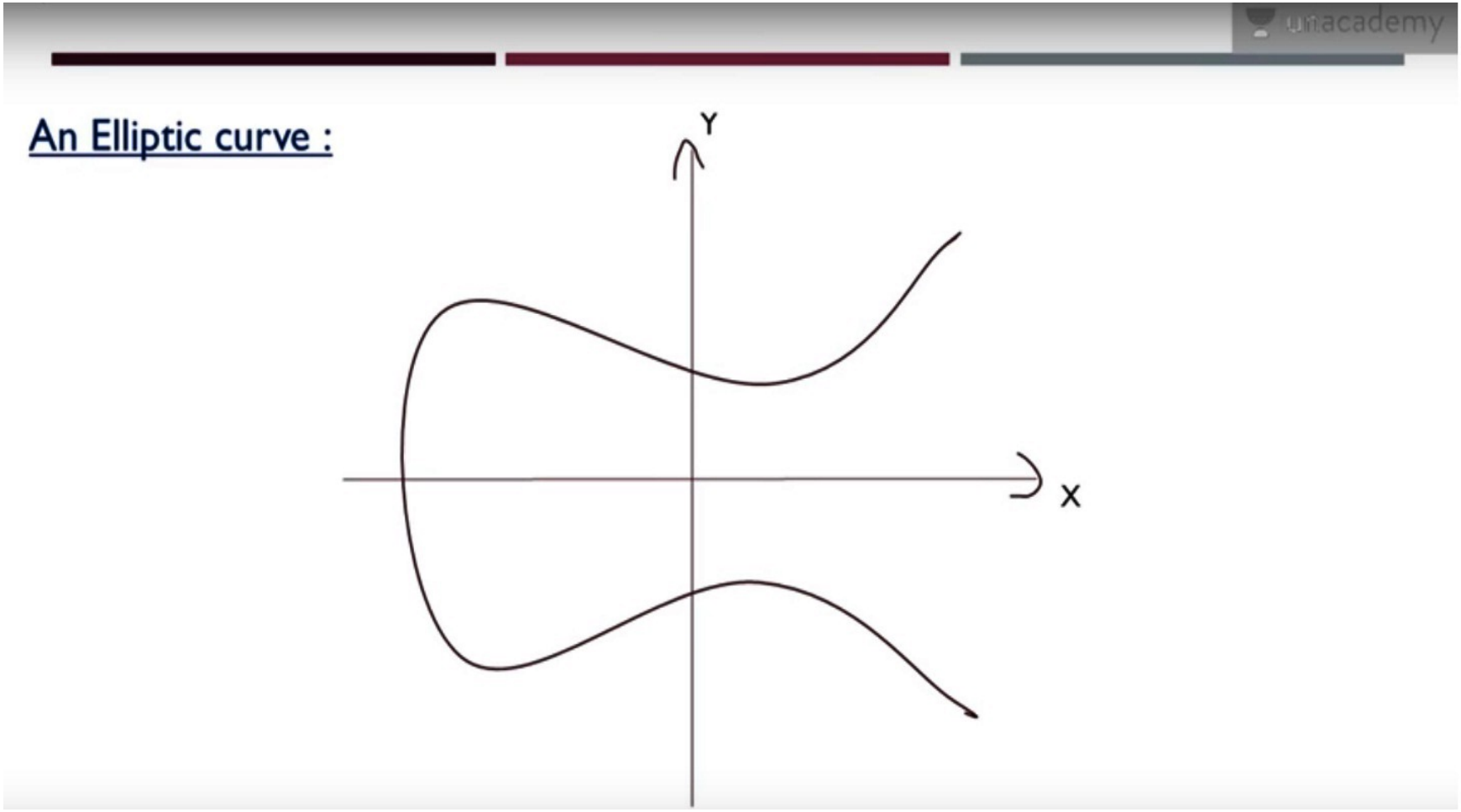
ECC

unacademy

ECC

- Asymmetric / Public key cryptosystem.
- ECC provides equal security with smaller key size.
- ECC makes use of Elliptic curves.
- Elliptic curves are defined by mathematical functions - Cubic functions.
- eg:- $y^2 = x^3 + ax + b$

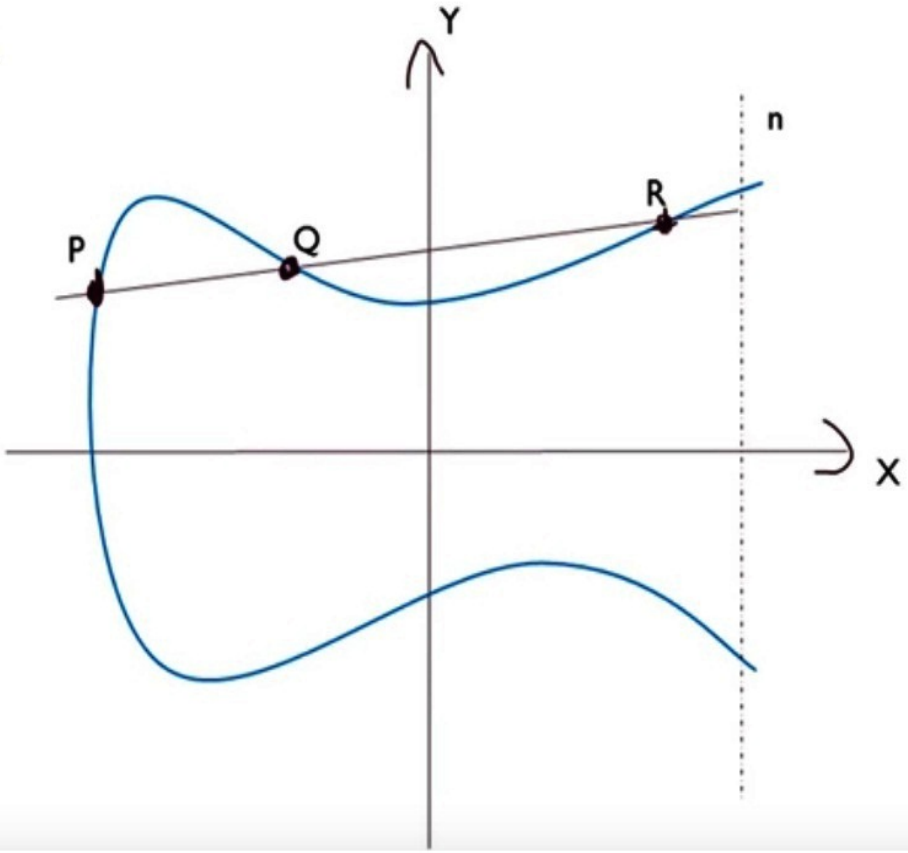
ECC



ECC

unacademy

An Elliptic curve :



ECC

ECC

- Let E_p (a,b) be the elliptic curve .
- Consider equation, Q = kP
  where Q, P $\in E_p$ (a,b) and k < n
- It should be easy to find Q given k and P.
- But should be extremely difficult to find k given Q and P.

- Is a one way function - trap door function.
- Called the discrete logarithm problem.

ECC

ECC - Key Exchange

Global Public elements.

$E_q(a,b)$: Elliptic curve with parameters a, b & q
q is a prime or integer of the form 2^m

G : Point on elliptic curve whose order is large value n.

Alice key Generation.

Select private key n_A ; $n_A < n$

Calculate public key P_A ; $P_A = n_A \times G$

Bob key Generation.

Select private key n_B ; $n_B < n$

Calculate public key P_B ; $P_B = n_B \times G$

Secret key calculation by Alice

$K = n_A \times P_B$

Secret key calculation by Bob

$K = n_B \times P_A$

ECC

ECC - Encryption & Decryption

- Let the message be M.
- First encode the message M into a point on the elliptic curve.
- Let this point be P_m.
- Now this point is encrypted.
- For encrypting choose a random positive integer k.
- Then $C_m = \{kG, P_m + kP_B\}$ where G is the base point.

- For decryption, multiply first point in the pair with receiver's secret key.
  i.e, $kG \times n_B$
- Then subtract it from second point in the pair.
  i.e, $P_m + kP_B - (kG \times n_B) = P_m + kP_B - (kP_B) = P_m$

References