Elliptic curve cryptography [ECC]

- Elliptic curve cryptography [ECC] is a **public-key** cryptosystem just like RSA, Rabin, and El Gamal.
- Every user has a **public** and a **private** key.
  - Public key is used for encryption/signature verification.
  - Private key is used for decryption/signature generation.
- Elliptic curves are used as an extension to other current cryptosystems.
  - Elliptic Curve Diffie-Hellman Key Exchange
  - Elliptic Curve Digital Signature Algorithm

ECC- Algorithm

- Both parties agree to some publicly-known data items
  - The **elliptic curve equation** $y^2 = x^3 + ax + b \bmod p$
    - values of ***a*** and ***b*** such that $4a^3 + 27b^2 \neq 0$
    - prime, ***p***
  - The **elliptic group** is computed from the elliptic curve equation
  - A **base point**, G, taken from the elliptic group
- Each user generates their public/private key pair
  - Private Key = an integer, x selected from the interval [1, p-1]
  - Public Key = product of private key and base point

    (Product = x*G)

Example :

- Suppose Alice wants to send to Bob an encrypted message.

– Both agree on a base point, G.

– Alice and Bob create public/private keys.

– Alice : Private Key = n_A

Public Key = $P_A = n_A * G$

– Bob : Private Key = n_B

Public Key = $P_B = n_B * G$

– Alice takes plaintext message, M, and encodes it onto a point, P_M, from the elliptic group.

Encryption : Alice choose another random k – value from { 1,2,… p-1 }

Cipher text : $C_m = \{ KG, P_m + KP_B \}$

Decryption : by Bob

Take the first point from Cm - KG

Multiply KG and private key of Bob : Product = n_B KG

Take the second point from Cm and subtract the product from it

$P_m + KP_B - n_B KG$

Substitute $P_B = n_B * G$ Then $P_m + K n_B * G - n_B KG = Pm$

ECC is particularly beneficial for application where:

- computational power is limited (wireless devices, PC cards)
- integrated circuit space is limited (wireless devices, PC cards)
- High speed is required.
- Intensive use of signing, verifying or authenticating is required.

- Signed messages are required to be stored or transmitted (especially for short messages).
- Bandwidth is limited (wireless communications and some computer networks). Advantages:
- Shorter key lengths
  - Encryption, Decryption and Signature Verification speed up
  - Storage and bandwidth savings