**Elliptic Curve Cryptography**

1) An approach for implementation of public-key cryptography according to the algebraic structure of elliptic curves over finite fields.

Notice: In public-key cryptography, two types of key are used: Public and Private. The public key is used for encryption of the plain text as oppose to the private key that is used for decryption of the cipher text.

2) **Advantage**: It has the same level of security as the non-ECC-based techniques, but with having a smaller key size.

3) Its security strength depends on the ability to compute a Point Multiplication.

Notice: Point multiplication is achieved by point addition and point doubling operations.

4) An elliptic curve:

* It is a plane curve over a finite field rather than the real numbers.
* It consists of the points that satisfy the equation:
* It also has a distinguished point at infinity 🡪 Infinity Point Notation = O
* It should be non-singular 🡪

Notice 1: Non-singular curve means having no cusp, intersection, or isolated point.

Notice 2: If the delta parameter is positive, the graph has two components otherwise it has one component.

5) Finite Field: A field that contains finite number of elements.

6) Main parameters in ECC:

* = A Finite Field
* = Elliptic Curve
* = Order = The number of elements of a finite field
* = An element of the curve