SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

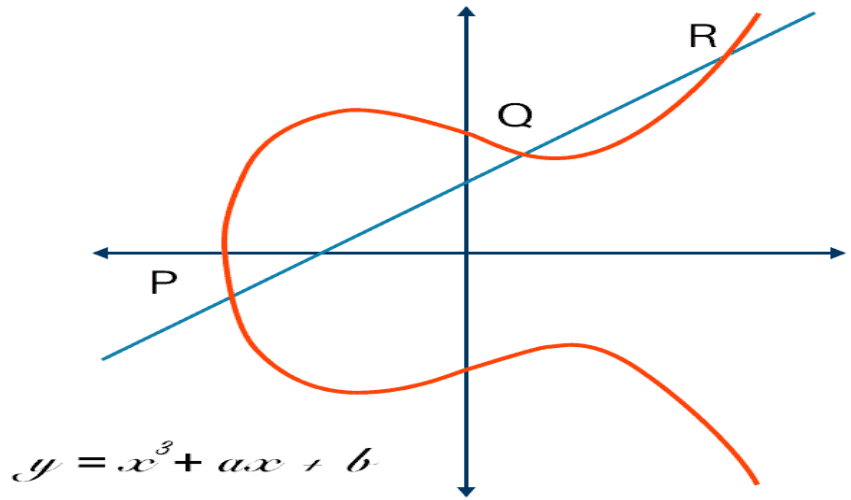
COURSE NAME : Fundamentals Of Cryptography

II YEAR / III SEMESTER

Unit III-

Topic : Elliptic Curve Cryptography

- Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
- ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.
- **Elliptic Curve Cryptography (ECC)** is a key-based technique for encrypting data.
- ECC focuses on pairs of public and private keys for decryption and encryption of web traffic.
- ECC is frequently discussed in the context of the Rivest–Shamir–Adleman (RSA) cryptographic algorithm.
- RSA achieves one-way encryption of things like emails, data, and software using prime factorization.



What is Elliptic Curve Cryptography?

- ECC, an alternative technique to RSA, is a powerful cryptography approach. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves.
- RSA does something similar with prime numbers instead of elliptic curves, but ECC has gradually been growing in popularity recently due to its smaller key size and ability to maintain security.
- This trend will probably continue as the demand on devices to remain secure increases due to the size of keys growing, drawing on scarce mobile resources.
- This is why it is so important to understand elliptic curve cryptography in context.
- ECC creates keys that are more difficult, mathematically, to crack. For this reason, ECC is considered to be the next generation implementation of public key cryptography and more secure than RSA.
- An elliptic curve for current ECC purposes is a plane curve over a finite field which is made up of the points satisfying the equation:
  $y^2=x^3 + ax + b$.
- In this elliptic curve cryptography example, any point on the curve can be mirrored over the x-axis and the curve will stay the same. Any non-vertical line will intersect the curve in three places or fewer

Elliptic Curve Cryptography vs RSA

The difference in size to security yield between RSA and ECC encryption keys is notable. The table below shows the sizes of keys needed to provide the same level of security. In other words, an elliptic curve cryptography key of 384 bit achieves the same level of security as an RSA of 7680 bit.

RSA Key Length (bit)	ECC Key Length (bit)
1024	160
2048	224
3072	256
7680	384
15360	521

There is no linear relationship between the sizes of ECC keys and RSA keys. That is, an RSA key size that is twice as big does not translate into an ECC key size that's doubled. This compelling difference shows that ECC key generation and signing are substantially quicker than for RSA, and also that ECC uses less memory than does RSA.

- Also, unlike in RSA, where both are integers, in ECC the private and public keys are not equally exchangeable. Instead, in ECC the public key is a point on the curve, while the private key is still an integer.
- A quick comparison of the advantages and disadvantages of ECC and RSA algorithms looks like this:
- ECC features smaller ciphertexts, keys, and signatures, and faster generation of keys and signatures.
- Its decryption and encryption speeds are moderately fast.
- ECC enables lower latency than inverse throughout by computing signatures in two stages.
- ECC features strong protocols for authenticated key exchange and support for the tech is strong.
- The main disadvantage of ECC is that it isn't easy to securely implement.
- Compared to RSA, which is much simpler on both the verification and encryption sides, ECC is a steeper learning curve and a bit slower for accumulating actionable results.
- However, the disadvantages of RSA catch up with you soon.
- Key generation is slow with RSA, and so is decryption and signing, which aren't always that easy to implement securely.

- **Advantages of Elliptic Curve Cryptography**

- Public-key cryptography works using algorithms that are easy to process in one direction and difficult to process in the reverse direction.
- For example, RSA relies on the fact that multiplying prime numbers to get a larger number is easy, while factoring huge numbers back to the original primes is much more difficult.
- However, to remain secure, RSA needs keys that are 2048 bits or longer.
- This makes the process slow, and it also means that key size is important.
- Size is a serious advantage of elliptic curve cryptography, because it translates into more power for smaller, mobile devices.
- It's far simpler and requires less energy to factor than it is to solve for an elliptic curve discrete logarithm, so for two keys of the same size, RSA's factoring encryption is more vulnerable.
- Using ECC, you can achieve the same security level using smaller keys.
- In a world where mobile devices must do more and more cryptography with less computational power, ECC offers high security with faster, shorter keys compared to RSA.