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 I

Topic : Prime Numbers

- A prime number is a whole number greater than 1 whose only factors are 1 and itself. A factor is a whole number that can be divided evenly into another number.
- The first few prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29. Numbers that have more than two factors are called composite numbers.
- The number 1 is neither prime nor composite.
- For every prime number, for example "*p,*" there exists a prime number that is greater than *p,* called *p*'.
- This mathematical proof, which was demonstrated in ancient times by the Greek mathematician Euclid, validates the concept that there is no "largest" prime number.
- As the set of natural numbers ***N*** = {1, 2, 3, ...} proceeds, prime numbers do generally become less frequent and are more difficult to find in a reasonable amount of time.

- prime is a number that must be reducible to the form $2^n - 1$, where n is a prime number. The first few known values of n that produce Mersenne primes are where $n = 2$, $n = 3$, $n = 5$, $n = 7$, $n = 13$, $n = 17$, $n = 19$, $n = 31$, $n = 61$, and $n = 89$.

- **Prime numbers and cryptography**

- Encryption always follows a fundamental rule: the algorithm -- or the actual procedure being used -- doesn't need to be kept secret, but the key does.
- Prime numbers can be very useful for creating keys.
- For example, the strength of public/private key encryption lies in the fact that it's easy to calculate the product of two randomly chosen prime numbers.
- However, it can be very difficult and time-consuming to determine which two prime numbers were used to create an extremely large product, when only the product is known.
- In RSA (Rivest-Shamir-Adleman), a well-known example of public key cryptography, prime numbers are always supposed to be unique. The primes used by the Diffie-Hellman key exchange and the Digital Signature Standard (DSS) cryptography schemes, however, are frequently standardized and used by a large number of applications.