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 :INTRODUCTION TO CRYPTOGRAPHY

INTRODUCTION TO CRYPTOGRAPHY

What is Cryptography

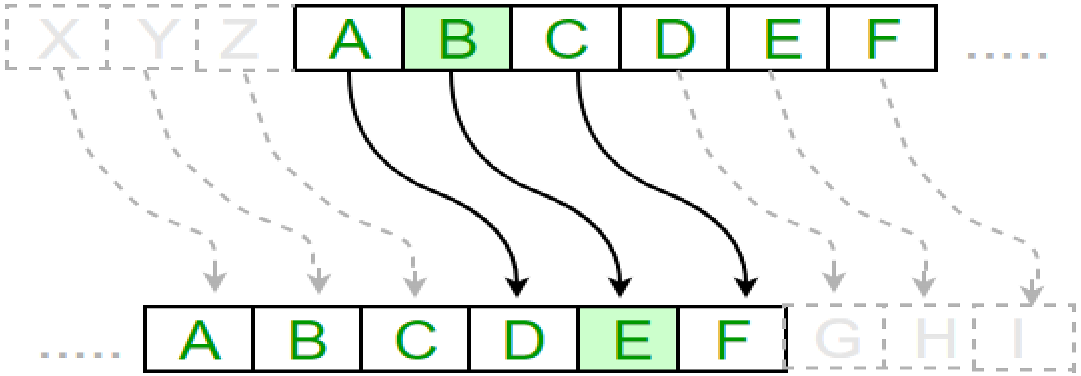
The word ‘cryptography’ originated from two greek words ‘Krypto’ means hidden and ‘graphene’ means writing.

Classical Cryptography

The roots are cryptography are found in Roman and Egyptian civilizations. Below are some of the ancient types of cryptography:

Caesar Cipher:

he ancient Greeks were well known for the use of Ciphers. The Caesar Cipher or Shift Cipher is one of the earliest and simplest well-known cryptographic techniques. It is a form of Substitution Cipher where each character in a word is replaced by a fixed number of positions. For example with a shift of 3, A is replaced by D, B by E, and so on.



Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

1.Confidentiality refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
2.Data integrity refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
3.Authentication is the process of making sure that the piece of data being claimed by the user belongs to it.
4.Non-repudiation refers to the ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

Types of Cryptography:
There are several types of cryptography, each with its own unique features and applications. Some of the most common types of cryptography include:
1. Symmetric-key cryptography: This type of cryptography involves the use of a single key to encrypt and decrypt data. Both the sender and receiver use the same key, which must be kept secret to maintain the security of the communication.
2. Asymmetric-key cryptography: Asymmetric-key cryptography, also known as public-key cryptography, uses a pair of keys – a public key and a private key – to encrypt and decrypt data. The public key is available to anyone, while the private key is kept secret by the owner.
Hash functions: A hash function is a mathematical algorithm that converts data of any size into a fixed-size output. Hash functions are often used to verify the integrity of data and ensure that it has not been tampered with.

Applications of Cryptography:

Cryptography has a wide range of applications in modern-day communication, including:

•**Secure online transactions:** Cryptography is used to secure online transactions, such as online banking and e-commerce, by encrypting sensitive data and protecting it from unauthorized access.

•**Digital signatures:** Digital signatures are used to verify the authenticity and integrity of digital documents and ensure that they have not been tampered with.

•**Password protection:** Passwords are often encrypted using cryptographic algorithms to protect them from being stolen or intercepted.

Military and intelligence applications: Cryptography is widely used in military and intelligence applications to protect classified information and communications

Types of Cryptographic Functions

- Secret key functions
- Public key functions
- Hash functions