NETWORK PROTOCOLS & SECURITY
23EC2210 R/A/E

Topic:

A Security Model, Asymmetric & Symmetric key Ciphers

Session – 34

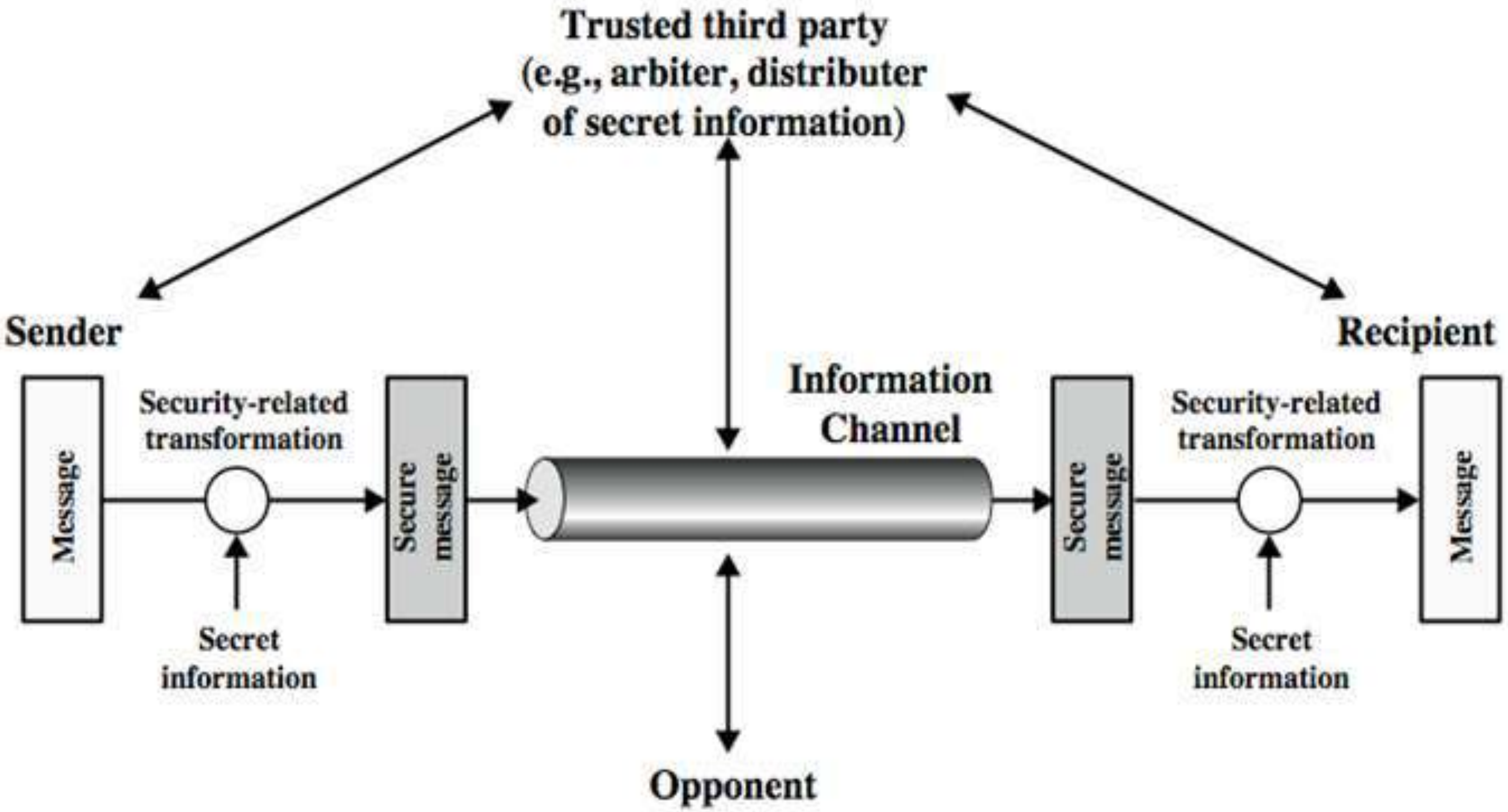
Classic Encryption Techniques

- **Plain Text**: Original Message
- **Encryption/Encipherment**: Process of Converting from Plain text to Cipher text
- **Decryption/Decipherment**: Restoring the plaintext from the cipher text.
- **Cryptography**: Many schemes used for encryption.
- **Cryptanalysis**: Techniques for deciphering a message without any knowledge of the enciphering details.
- **Cryptology**: areas of Cryptography and Cryptanalysis together are called Cryptology

Classic Encryption Techniques

- **Encryption Algorithm**: Performs various substitution and transpositions on the plain text.
- **Secret Key**: Value independent of plain text and the algorithm.
- **Cipher Text**: Scrambled Message produced as Output.
- **Decryption Algorithm**: Encryption Algorithm in reverse.

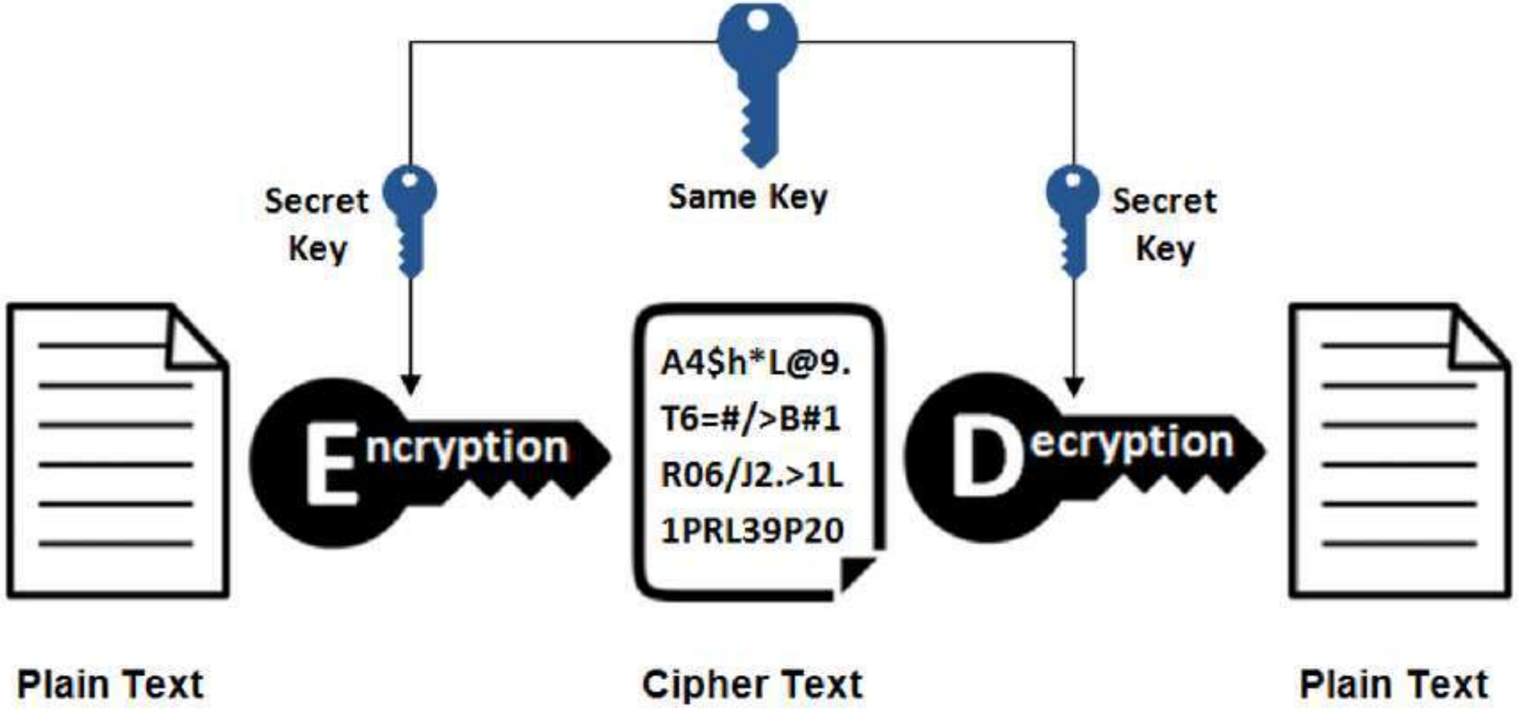
A Model for Network Security



Cryptography

- **Cryptography** is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information.

- The prefix “crypt” means “hidden” and suffix “graphy” means “writing”.



Cryptography

Cryptography is associated with the process of converting ordinary plain text into incomprehensible text and vice-versa.

It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

1. Symmetric key Cryptography

- Symmetric encryption is also called secret key encryption, and it uses just one key, called a shared secret, for both encrypting and decrypting.

- This method is the opposite of Asymmetric Encryption where one key is used to encrypt and another is used to decrypt.

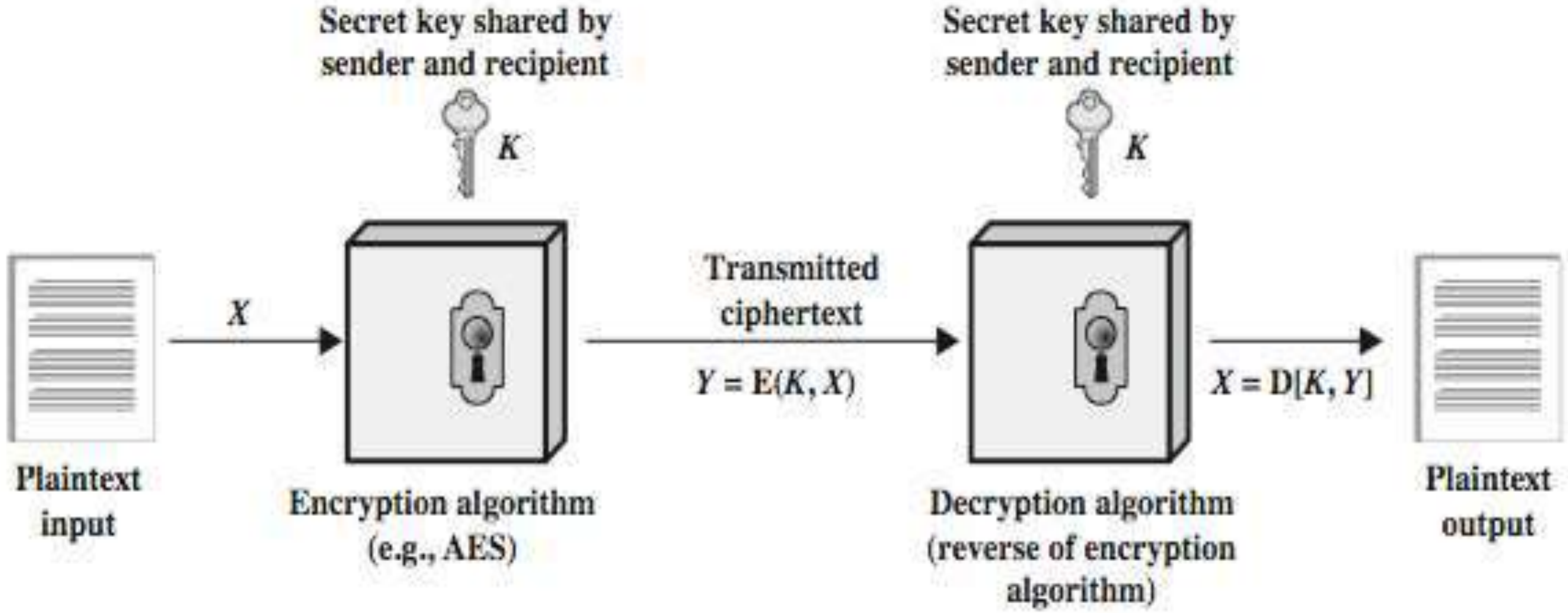
Cryptography

2. Public key cryptography

- uses a **pair of keys to encrypt and decrypt** data to protect it against **unauthorized access or use**.

NOTE: Symmetric cryptography was one-type prior to invention of public-key in 1970's and by far most widely used (still) is significantly faster than public-key cryptography.

Symmetric Cipher Model


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
$Y = E(K, X)$
$X = D[K, Y]$
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Symmetric Cipher Model

- Two requirements for secure use of symmetric encryption:

  - a strong encryption algorithm

  - a secret key known only to sender / receiver

- Mathematically

  $Y = E(K, X) = E_K(X)$

  $X = D(K, Y) = D_K(Y)$

- A secure channel is required to distribute the key, this is a big problem in symmetric cryptography

Symmetric Cipher Model

Cryptographic algorithms are characterized by the type of encryption operations used

substitution, transposition, product

Substitution: Elements of plain text is mapped with another element

Transposition: Elements of plaintext are rearranged

Product: Combination of Substitution and Transposition

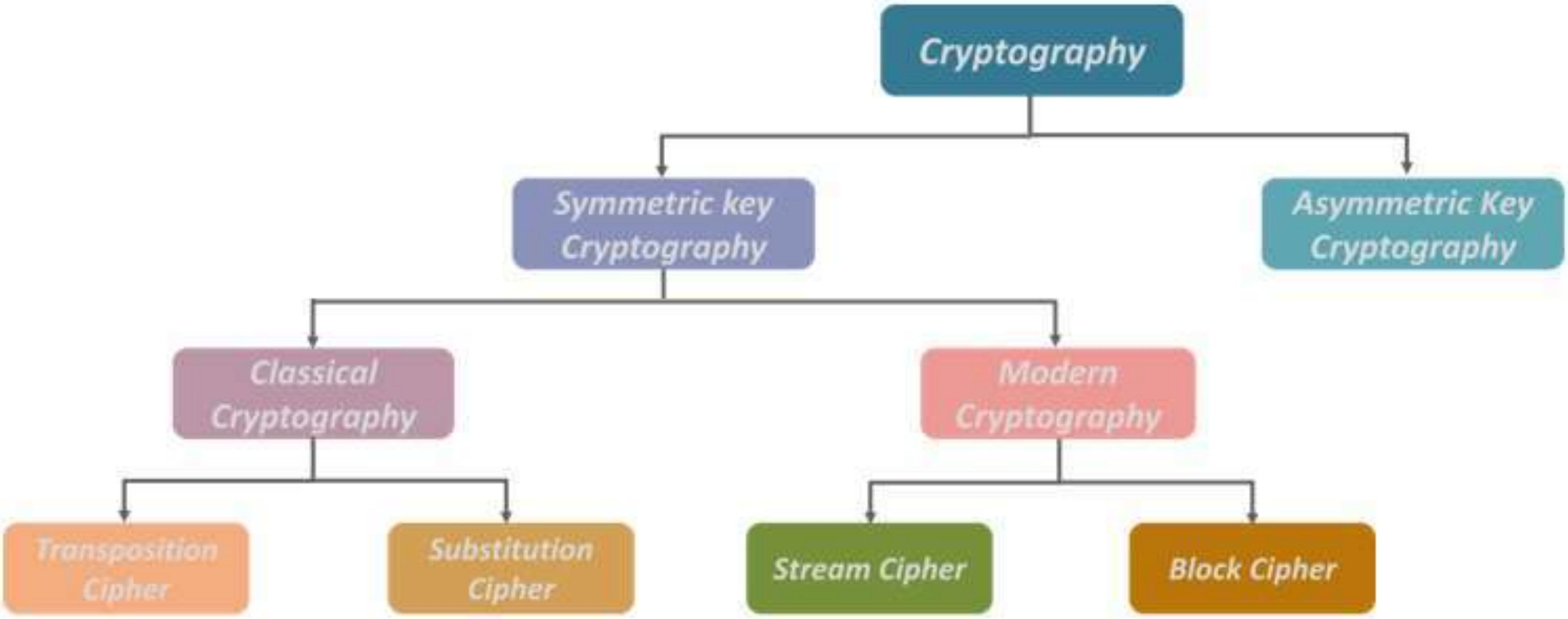
Symmetric Cipher Model

- **The way in which plaintext is processed**

  Block Cipher: Input is Processed one block at a time and outputs a block

  Stream Cipher: Process the input element one at a time and outputs one element at a time.

Cryptography Methods



Cryptography

Symmetric key Cryptography

Asymmetric Key Cryptography

Classical Cryptography

Modern Cryptography

Transposition Cipher

Substitution Cipher

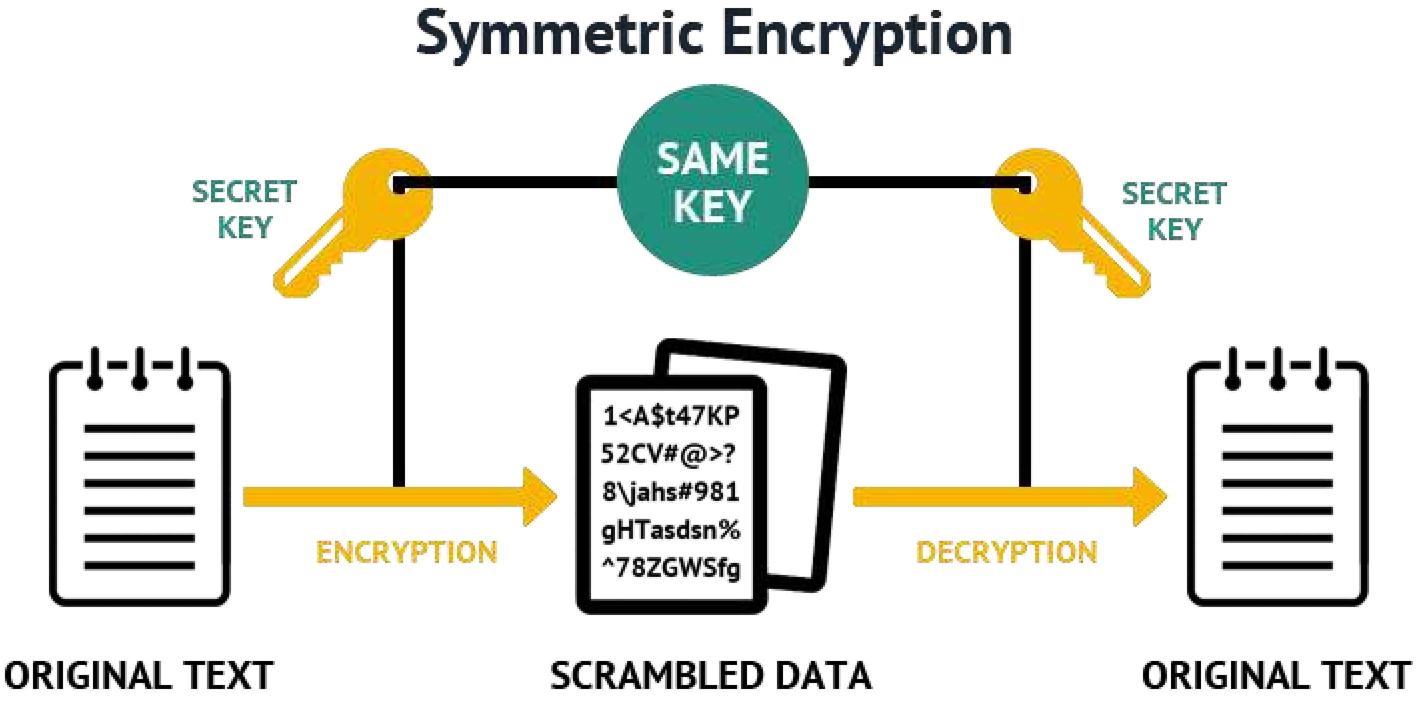
Stream Cipher

Block Cipher

Symmetric Cryptography

Symmetric Cryptography

Symmetric encryption is a data encryption method whereby the same key is used to encode and decode information.



Classical Symmetric Encryption Methods

Substitution Ciphers

- Is a technique in which plaintext letters are replaced with other letters, numbers, or symbols.
- **Substitution Cipher Methods:**
  - ➢ Caesar Cipher
  - ➢ Mono-alphabetic Cipher
  - ➢ Playfair Cipher

Transposition Ciphers

- Is a technique where the order of alphabets in the plaintext is rearranged to form a cipher text.
- **Transposition Cipher methods:**
  - ➢ Columnar Cipher
  - ➢ Rail fence Cipher