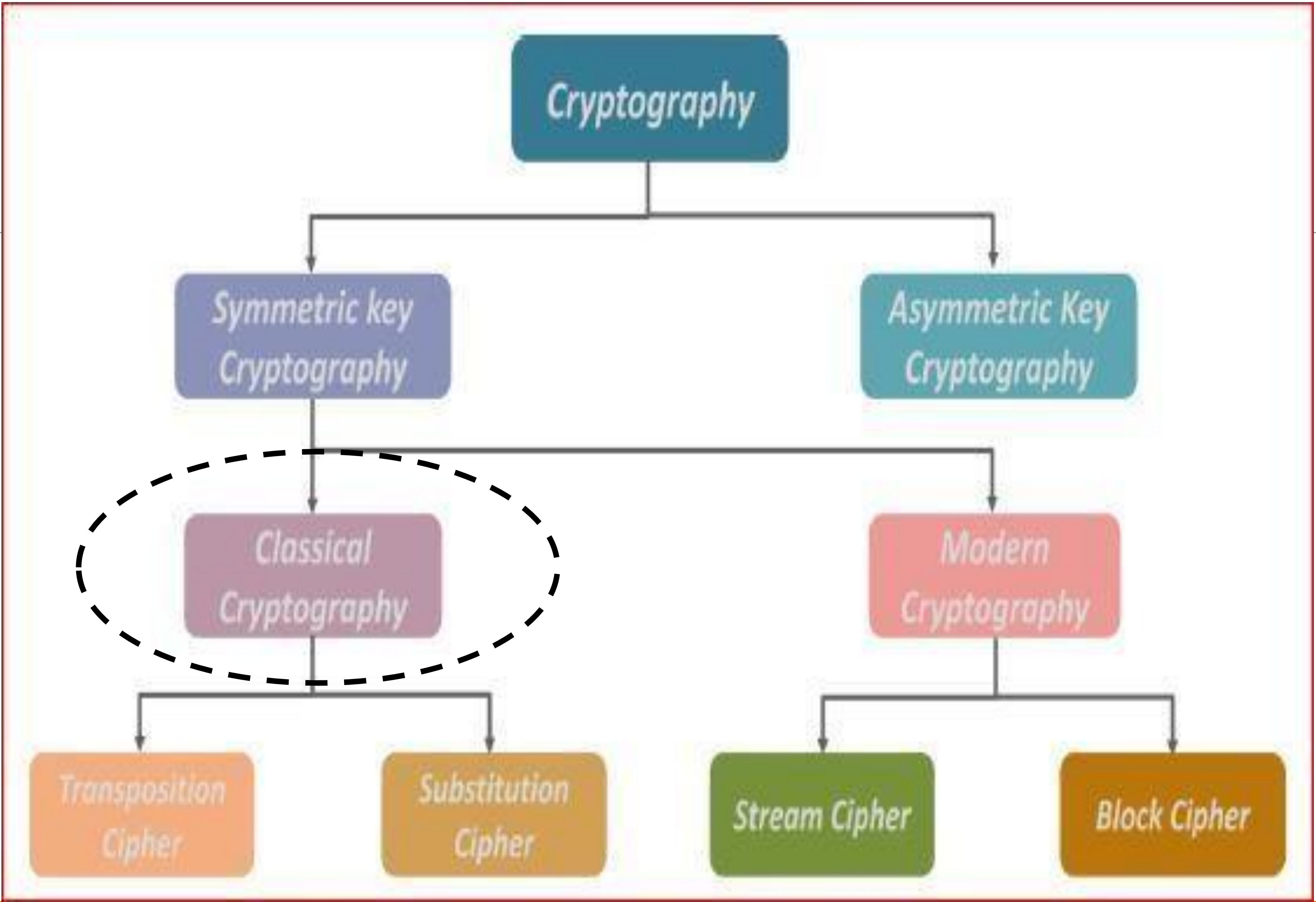
# CRYPTOGRAPHY

## LECTURE THREE

## Classical ( Traditional ) Encryption Techniques

*Assist prof. Dr. Saja J. Mohammed*


Cryptography
Symmetric key Cryptography
Asymmetric Key Cryptography
Classical Cryptography
Modern Cryptography
Transposition Cipher
Substitution Cipher
Stream Cipher
Block Cipher

# Classical (Traditional) Ciphers

- Plaintext is viewed as a sequence of elements (e.g., bits or characters)

- **Classical ciphers can be classified in to two types:**

**1. Transposition (or permutation) cipher Technique:** rearranges the position of the plain text's characters. In transposition cipher technique, the position of the character is changed but character's identity is not changed.

**2. Substitution cipher Technique:** Plain text characters are replaced with other characters, numbers and symbols as well as in substitution cipher technique, character's identity is changed while its position remains unchanged.

| | Transposition Cipher Technique | Substitution Cipher Technique |
|---|---|---|
| 1. | Plain text characters **are rearranged** with respect to the position. | Plain text characters **are replaced** with other characters, numbers and symbols. |
| 2. | The position of the character is changed but character's identity is not changed. | Character's identity is changed while its position remains unchanged. |
| 3. | Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher. | Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher. |
| 4. | Drawbacks: The Keys which are nearer to correct key can disclose plain text. | Drawbacks: The letter with low frequency can detect plain text, (**in mono alphabetic**) |
| 5. | Example : Rail Fence Cipher. | Example : Caesar Cipher. |

# Transposition Cipher

- **Transposition technique** is an encryption method which is achieved by performing permutation over the plain text.

**Definition :**

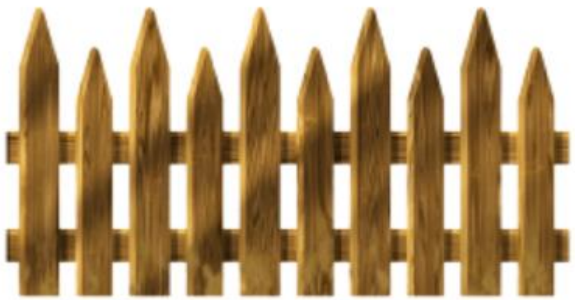
A **permutation** of a finite set of elements **S** is an ordered sequence of all the elements of S, with each element appearing exactly once. There are **n!** permutations of a set of **n** elements,

For example, if S = {a, b, c}, there are six permutations of S:

abc, acb, bac, bca, cab, cba

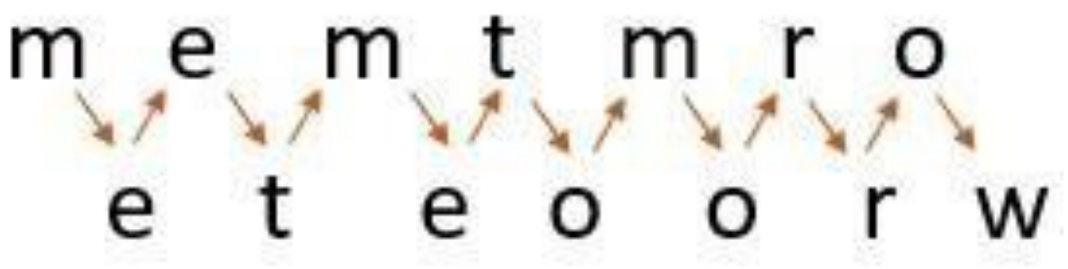
- In general it can be classified in to:
  1. Key-less transposition.
  2. Keyed transposition cipher.
- Such examples of an encryption algorithm working in this principle are:
  1. Rail Fence Transposition cipher.
  2. Columnar Transposition cipher.
  3. Route transposition cipher.

# 1. Rail Fence Cipher ( also called zigzag cipher)



- The rail fence cipher is the simplest transposition cipher., in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For example, to encipher the message “**meet me Tomorrow**” with a rail fence **of depth 2**, we write the following The steps to obtain cipher text using this technique are as follow:

- **Step 1:** The plain text is written as a sequence of diagonals.
- **Step 2:** Then, to obtain the cipher text the text is read as a sequence of rows.



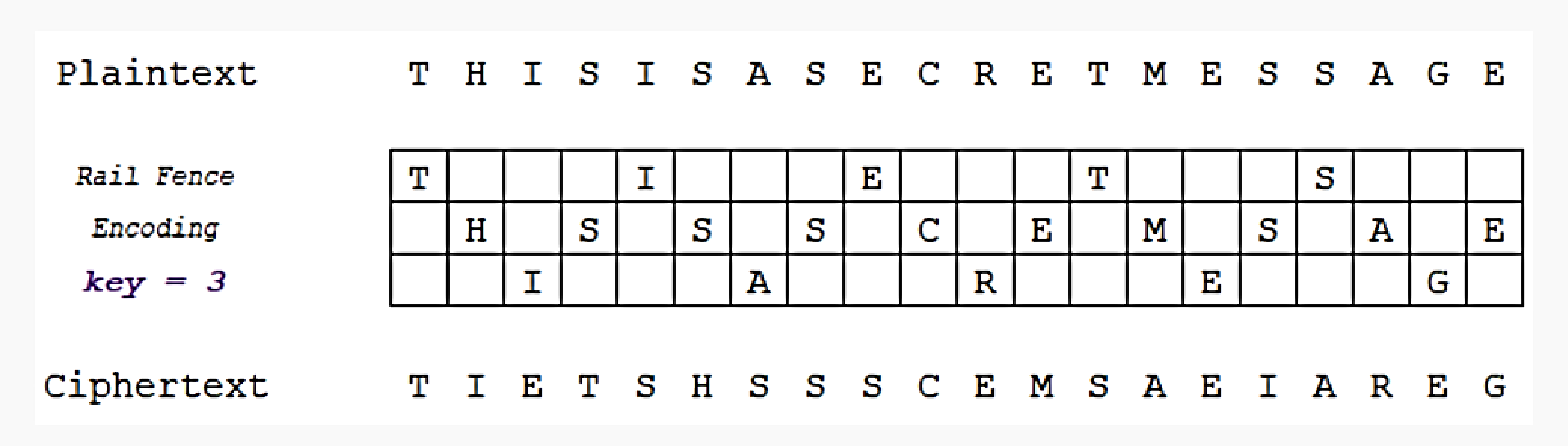
m e m t m r o

e t e o o r w

- Once you have written the message as a sequence of diagonals, to obtain the cipher text out of it you have to read it as a sequence of rows. So, reading the first row the first half of cipher text will be:
    - **m e m t m r o**
- Reading the second row of the rail fence, we will get the second half of the cipher text:
    - **e t e o o r w**
- Now, to obtain the complete cipher text combine both the halves of cipher text and the complete cipher text will be:
- **Cipher Text:** M E M T M R O E T E O O R W
- <u>**Rail fence cipher is easy to implement and even easy for a cryptanalyst to break this technique. So, there was a need for a more complex technique.**</u>

More complex Rail Fence Ciphers have more “rails”. For instance instead of writing the code over two lines (“rails”) you can write over three or four or more lines. The number of lines used in a Rail Fence Cipher is called the **key**.

**Key = 3**



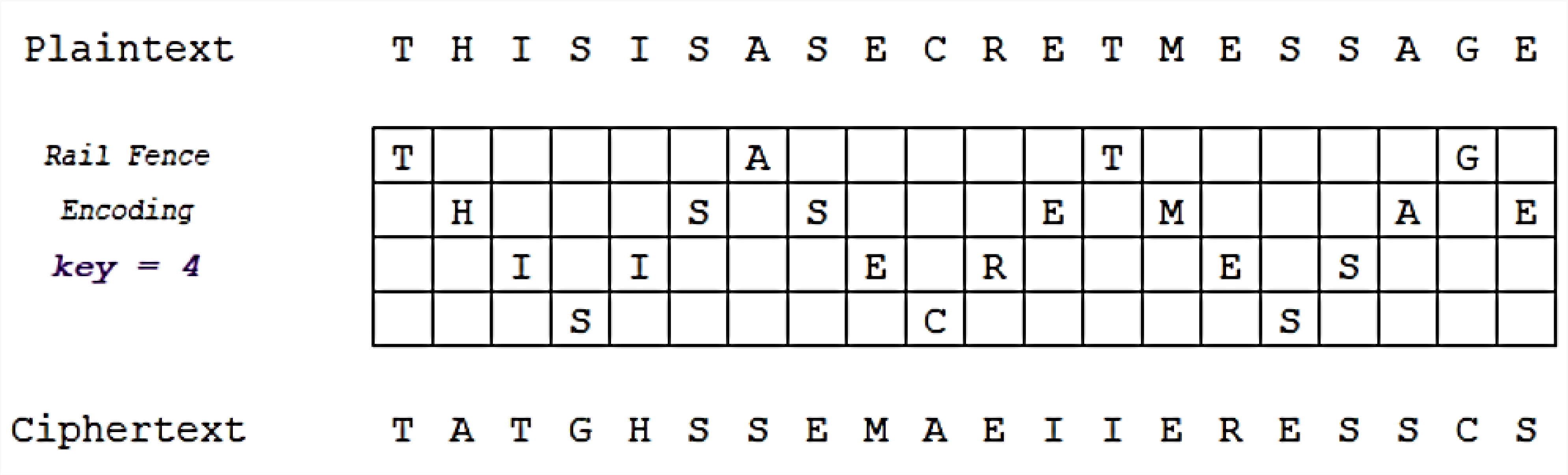
Plaintext T H I S I S A S E C R E T M E S S A G E

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Rail Fence* | T | | | | I | | | | E | | | | T | | | | S | | | |
| *Encoding* | | H | | S | | S | | S | | C | | E | | M | | S | | A | | E |
| *key = 3* | | | I | | | | A | | | | R | | | | E | | | | G | |

Ciphertext T I E T S H S S S C E M S A E I A R E G

A Rail Fence Cipher with 3 “rails” (Key = 3)

## Key = 4



Plaintext T H I S I S A S E C R E T M E S S A G E

Rail Fence Encoding *key = 4*

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T | | | | | | A | | | | | | T | | | | | | G | |
| | H | | | | S | | S | | | | E | | M | | | | A | | E |
| | | I | | I | | | | E | | R | | | | E | | S | | | |
| | | | S | | | | | | C | | | | | | S | | | | |

Ciphertext T A T G H S S E M A E I I E R E S S C S

A Rail Fence Cipher with 4 “rails” (Key = 4)