A logo of a university

Description automatically generated

**قــســــــــــم الأمــــــــــــــــــــــــــن الــــــــــــــــــــــــــــــــــــسيبرانــــــــــــــــــــــــــــــــــــي**

**Department of Cyber Security**

**Subject:**

**Principles of Cyber Security**

**Class:**

**First**

**Lecturer:**

**Muntather AL-mussawee**

**Lecture: (8)**

**Components of Encryption System**

**Encryption Algorithms**

**1-Traditional encryption methods**

**Introduction**

* Encryption is the science of securing information and protecting it from unauthorized access. Before the advent of computers, ancient civilizations used various methods to encrypt messages, such as the Caesar cipher used by the Romans and the Scytale cipher used by the Greeks.
* Traditional encryption is primarily based on substitution (replacing letters with others) or transposition (rearranging letters), making the text unreadable without the correct key.
* Although these methods were effective in the past, the rise of computers made them vulnerable to frequency analysis and computational attacks. This led to the development of modern encryption techniques, such as symmetric-key encryption and public-key encryption, to secure digital data.

**المقدمه :**

* التشفير هو علم تأمين المعلومات وحمايتها من الوصول غير المصرح به، وهو أحد أقدم فروع علم التشفير. قبل ظهور الحواسيب، استخدمت الحضارات القديمة طرقًا مختلفة لتشفير الرسائل، مثل طريقة قيصر التي استخدمها الرومان، وطريقة سكيتالي التي استخدمها الإغريق.
* التشفير التقليدي يعتمد غالبًا على استبدال الحروف أو إعادة ترتيبها (التبديل)، مما يجعل النص غير مفهوم دون معرفة المفتاح المستخدم لفك التشفير.
* على الرغم من أن هذه الطرق كانت فعالة في الماضي، إلا أن ظهور الحواسيب جعل كسرها أمرًا سهلاً باستخدام تحليل الترددات والهجمات الحاسوبية، مما أدى إلى تطور تقنيات التشفير الحديثة مثل التشفير بالمفتاح المتماثل والتشفير بالمفتاح العام لحماية البيانات الرقمية.

**Some of the most well-known traditional encryption techniques include:**

1. Caesar Cipher – Shifts each letter in the plaintext by a fixed number of positions in the alphabet.
2. Simple Substitution Cipher – Replaces each letter with another letter according to a specific rule.
3. Playfair Cipher – Uses a 5×5 grid of letters to encrypt pairs of letters.
4. Vigenère Cipher – Uses a repeating key to apply multiple Caesar ciphers, making it harder to break than a simple shift cipher.
5. Hill Cipher – Uses matrix operations to encrypt text, providing more complex encryption.

# **Caesar Cipher Algorithm**

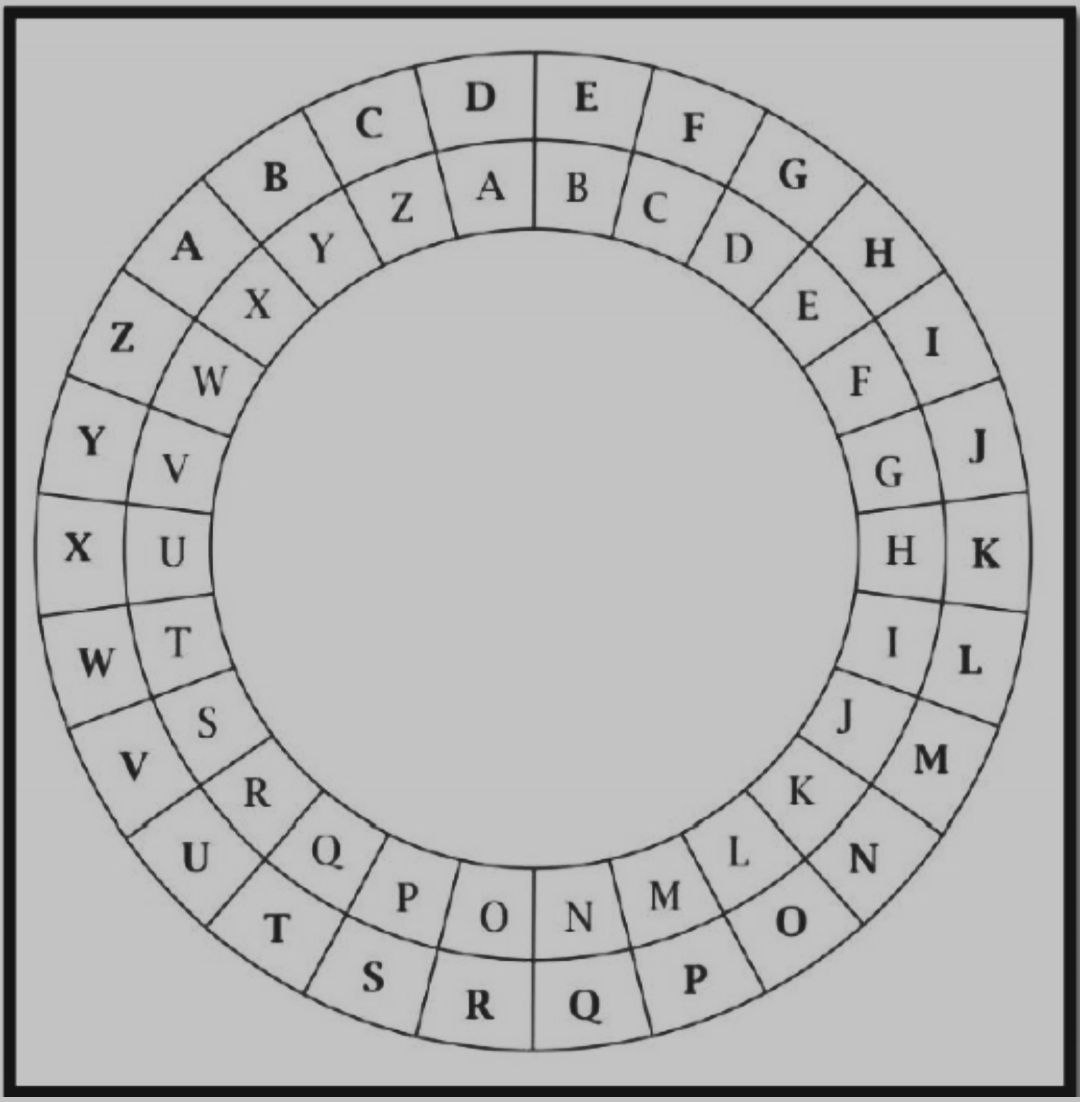
# Simplest and earliest known use of a substitution cipher

# Used by Julius Caesar

# First attested use in military affairs

# Involves replacing each letter of the alphabet with the letter

# standing three places (the key)



* Can define transformation as:



* Mathematically give each letter a number



* Algorithm can be expressed as:

C=E(3,p)=(p+3)mod(26)

* A shift may be of any amount, so that the general Caesar algorithm is:

C= E(k,p)=(p+k)mod26

* Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

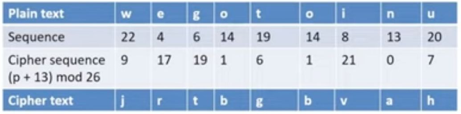
p= D(k,C)=(C-k)mod 26

Example:

suppose the key for a shift cipher is K= 13 and the plaintext is

*we go to INU*





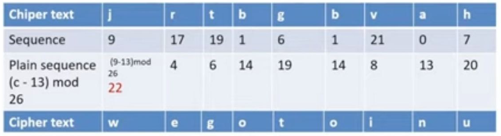
*Chiper text: jrtbgbvah*

Example:

suppose the key for a shift cipher is K= 13 and the chipper text is:

*Chiper text: jrtbgbvah*





*plain text: we go to inu*

Home Work on Caesar Cipher

suppose the key for a *shift cipher is K= 12* and the plaintext is *ILove INU*

*A. Find the cipher text?*

*B. Validate your answer! Hint decrypt you cipher text to get the same*

*plain text again*

**Rail Fence Cipher ( Zigzag Cipher)**

* The Rail Fence Cipher method is also known as the zigzag.
* This name comes from the way the characters are arranged in tracks resembling railroad fences, where the text is written in a zigzag fashion and then read row by row.
* We will implement the Zigzag Cipher algorithm using a certain number of rows, and then recover the original text from the ciphertext.
* هذا الاسم يأتي من الطريقة التي يتم بها ترتيب الأحرف على شكل مسارات تشبه أسوار السكك الحديدية، حيث يتم كتابة النص بطريقة متعرجة ثم قراءته صفًا بعد صف .
* سنقوم بتنفيذ خوارزمية التشفير بطريقة الزكزاك (Zigzag Cipher) باستخدام عدد معين من الصفوف، ثم نستعيد النص الأصلي من النص المشفر

**خطوات التشفير**

1. كتابة النص في نمط زكزاك عبر عدد محدد من الصفوف.

2. قراءة الحروف صفًا بعد صف للحصول على النص المشفر.

خطوات فك التشفير

1. إعادة توزيع الأحرف في نمط الزكزاك وفقًا لعدد الصفوف.

2. قراءة الحروف بالترتيب الأصلي لاستعادة النص.

**Example**: to encipher the message **"meet me after the toga party"** with

a **rail fence** of **depth 2**, we write the message **M** as follows:

**Solution:**

m e m a t r h t g p r y

e t e f e t e o a a t

The encrypted message **C** is **"MEMATRHTGPRYETEFETEOAAT"**

**Example**: Encrypt the message with **Key** or **Depth=3** and **Bottom-Up**,

M:"DISCONNECT THE PLUGS NOW"

**Solution:**

Rewritten the message first in the form:



Then the ciphertext is taken as:

**C**:” **SNTLNICNETHPUSODOCEGW “**

**Rail fence Technique: Zigzag**

* S/r agree about depth this represent the Key and then agree about

Strategy (Bottom Up or Top Down)

To decrypt as following:

1. Number of columns of Matrix =number of Cipher text characters.
2. Number of Rows = Depth value that agree between S/R.
3. Draw the Matrix depends on depth value and Direction(BU or TD)
4. Distribute the cipher text depends on idea.
5. Read Zigzag to find plain text.

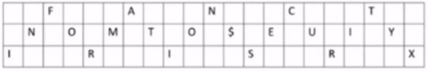
* In Rail Fence , may be use Double Ciphering that of course need

Double Deciphering:

**Example** : let the massage"**informationSsecurity**"use **RF** with **depth =3**

and **BU**,then encrypt result using **Depth =2** and **TD**?

(( Double Encryption



C1="FANCTNOMTOSEUIYIRISRX"



C2="FNTOTSUYRSXACNMOEIIIR"

meet me after ,**depth=2**, **TD**



C. "MEMATRETEFE"

P="MEETMEAFTER"