

- ❖ **Computer Security :-** is the protection of computing systems and the data that they store or access. It refers to the technological safeguards and managerial procedures that can be applied to computer hardware, programs, and data.
- ❖ **Data Security :-** refers to the protection of data from accidental, or unauthorized modifications or destructions, or disclosure to unauthorized persons.
- ❖ **Privacy :-** it is the right of an individual to decide what information he wish to share with others and what information he will accept from others.
- ❖ **Integrity :-** it refers not only to the correctness of data (message or file) but its resources and validity.
- ❖ **Data Integrity :-** is the property that data has not been changed or destroyed in an unauthorized manner.
- ❖ **Authentication :-** is the granting a user of right access to a protected program, or a process.
- ❖ **System Integrity :-** is the ability of a system to operate according to some specifications even in the face of deliberate attempts to make the system behave differently.
- ❖ **Confidentiality :-** is the property that information is not made available or disclosed to unauthorized persons.
- ❖ **Identification :-** the identification of a user, file, program, or other object is the unique name or number assigned to that object.

Why is the Computer Security Important?

1. Provide support for the critical business processes.
2. Provide protection for the personal and sensitive information.

What will happen if your computer gets hacked?

1. It could be used to hide some programs.
2. It could generate a large amount of unwanted traffic.
3. Some one could send illegal software from your computer to others without you realize it.
4. Someone could access personal information.
5. Someone could record all your keys that are used like passwords.

Good Security Standards :-

If follows the rule of 90/10, it means that 10% of security are *technical* while 90% of security depends on *computer user* (you).

For example:- the lock of the door represent the 10% while the remembering to lock the door, checking if the door is closed, etc., this represents the 90%. So we need the both 90 and 10 to get the effective security.

The Effective Security :-

Means the following:-

1. Everyone who uses a computer needs to understand how to keep their computer and data secure.
2. Learn the good computing security procedures.
3. Report anything unusual and notify the appropriate persons.

The Consequences of Security Violation :-

1. Loss of employee trust.
2. It causes risks to security and integrity of personal information.
3. Loss of business information.

Internet Privacy and Security:-

1. **Privacy on Internet :-** It means the measures to protect data during their transmission over a collection of interconnected networks. Social networking sites like Facebook, personal web pages have also become public sources of personal information. So :-
 - ❖ Do not write personal details online. Assume that anything you post to those websites is public and could be used against you.
 - ❖ The good rule is to post only the information that you desire to be public in that websites.
 - ❖ Put in your mind that anything you will post in public website is more difficult to take it back even if you delete it, since copies of this information will still exist on other computer or websites.

Cautions when using Social Network:-

1. Remember that the internet is not private.
2. Do not give out personal or sensitive information to anyone you don't know.
3. Don't provide personal or sensitive information to internet site unless you are using trusted and secure web pages.
4. Some web pages display an internet address directly, so don't click on such address.
5. A little lock is putting at the end of "http" address; this means that website is secure.

2. **Internet Security Cautions :-**

1. Make sure you know where you are going before clicking on a link.
2. Use only known, trusted and secure websites when you enter sensitive or personal information.

3. To help avoid viruses don't use internet explorer and use instead more secure alternative way like *Firefox* or *Safari*.

Security Involving Programs :-

Programs may cause two types of problems:-

1. These programs may transform of data to serve the users who must have no access to such data.
2. Theses programs may possible to penetrate by other systems leading to prevent authorized person from accessing them and at the same time allow unauthorized access to it.

Information Access Problems :-

There are several types of software that can be used to gain access to unauthorized data or information:-

a) *Trapdoors*

A set of access points that are put in the system by programmer for the following possibility points:-

1. To identify future modification of the system.
2. To access to mistakes in the future.
3. Allowing the designer of accessing to the program after the completion of its design.

Causes of Trapdoors:-

Usually the programmer must remove these points during program development but it can be found in the programs for the following reasons:-

1. The programmer forgot to delete these points.
2. Programmer usually leaves these points in order to help the rest of the parts of the program test or to assist in the maintenance of that program.

So we note that the advantage of **Trapdoors** is that we can test the performance of the system, while the disadvantages are that it is used by the programmer for a break.

b) Trojan Horse

For the similarity of his work with the legend of Trojan Horse wooden which hid by a number of soldiers Greeks and they were the reason to open the city of Trojan.

It is a kind of software which is loaded with major program and doing some hidden functions that are often concentrated to penetrate the system.

Trojan horses may steal information or damage the host computer systems and may be used for the download by search engines or by installing online games or applications based on internet taking advantage of security gaps that allow unauthorized access to the system.

c) Salami Attack

Is a process similar to the process slicer where small deducted (يستقطع) money from each account an amount so that this part is not observed in the normal case.

This type of software is attacking the banks where the decimals deduct each amount daily and will be transferred to another account without being noticed and within days or months will get the beneficiary on the huge amounts of money.

Also the customer who will be deducted from his account decimals will not demanding to clarify the matter because it will be regarded as the amount deducted is worthwhile.

Programs that leak information

This type of software is leaking the information and delivery it to person not authorized to get it.

The generic name for this type of program is (Covert or Hidden Channels).

Are a hidden channels or programs used to penetrate the system and leaking of information from the system.

For example; a programmer when designing a specific program for the bank, is entitled to deal with the data and its size as required by the banking program, but access to that data after completion the designing of the program is unacceptable.

How to Create Covert Channels

1. The programmer can encode data through a formula to replace the output, for example replace the word (total) with (totals) by adding (s) to the end of the word as it is represents the bit itself Covert Channel through which is part of the information transfer.
2. In same case, the programmer can not access the data through the program, but it calls another program that converts the data to the first program and is not observable.
3. The smart programmer can develop Covert Channel, for example, assume that the program reached a confidential data (بيانات سرية) during execution and that the programmer will create of dual-coding and through which passes the information to that coding.

Service Problems

This kind of problem depends on designing programs to influence the work of the system and the services provided by the user, causing stops these services and the failure of this is called "*fail of service*".

Types of service problems:-**a) Greedy Programs**

Programs that are change the sequence of important for programs to implement, for example, in multi-processes systems, there is a time to run each program so when one program waiting for input data for input devices, the CPU will enter in the waiting state, leading to wait for the implementation od other programs.

b) Viruses

Are programs that impact on other programs by making adjustments.

These programs are considered an extension for Greedy Programs.

Its problems:-

1. Viruses interference to systems that have a number of users to access data, for example e-mail.
2. Viruses can multiply in the system a very short time and often can not determine the source and the small size of these programs help to hide in complex programs such as Data Base.

c) Worms

Is malicious software that repeats them in order to spread into the rest of the computers that are used in computer network depending on the failure in the security system that is used.

Worms differ from viruses that viruses make changes on programs that are dominated by, while worms causing harm in a simple computer networking through the destruction of **bandwidth**.

Worms don't make any change in files but only settle in the memory and repeat them and are often used parts of the operating system specially the invisible parts for the users.

Program Development Controls against Program Attacks

(a) Modularity (b) Encapsulation (c) information Hiding

a) Modularity:- is the process of dividing a program into subtasks called (Modules), each task do certain function. There are several advantages from writing program into partial tasks:-

1. Maintainability

The maintenance of the system be directed process where only the specific module maintenance.

2. Understandability

Program which consists of several parts is easy to understand and know his work compared to if large.

3. Correctability

Easy follow-up errors as they arise and this will lead to speed in correcting these errors.

b) Encapsulation

The concept of modularity lead to the independence of each module from the other, where each module is an independent object and this is known as the principle of encapsulation.

When making a program, each module will be surrounded by a shield preventing unwanted access from the outside, so that the process of encapsulation does not mean isolating modules from other parts of the program but sets handle modules with each other, and this will reduce the covert channel used to penetrate the system.

c) Information Hiding

Means hide the data and instructions of a module and this will lead to hide the function of module.

This process is desired in terms prevents the programmer from doing penetrate the module unless it is to know how the module works.

Independent Testing

The purpose of the test is to determine the validity of the program and during the test we can see the errors.

The purpose of the test:-

1. Test that shows errors is more accurate than the test you can not find something.
2. The testing process will assure us that the system works and is designed according to its purpose.
3. From a security stand point, the testing is very important because the programmer may hide another program within the system as a weakness to serve its own purposes.

Security Mechanism :- means the mechanism that is designed to detect, prevent, or recover from security attack. Remember that no single mechanism will support all functions required.

Chapter Two :-

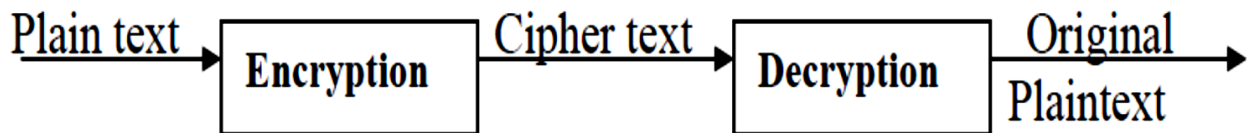
- ❖ **Cryptology** :- is the science of cryptography and cryptanalysis.
- ❖ **Cryptography** :- is the science of secret writing.
- ❖ **Plaintext (P)** :- is the original text which is understand by anyone.
- ❖ **Cipher text (C)** :- is an encrypted plaintext, sometimes called cryptogram.
- ❖ **Cipher** :- is a method of encipherment and decipherment.
- ❖ **Encipherment (Encryption) E** :- is the process of transformation Plaintext (P) to Ciphertext (C).
- ❖ **Decipherment (Decryption) D** :- is the process of transformation Ciphertext (C) to Plaintext (P).

- ❖ **A Key (K)** :- is a controller for Encipherment and Decipherment.
- ❖ **Cryptanalysis** :- is the science of methods of breaking ciphers.

Cryptography

Suppose a sender wants to send a message to a receiver. Moreover, this sender wants to send the message securely: she wants to make sure the unauthorized can not read the message.

A message is **plaintext** [sometime called **clear text**]. The process of disguising (تمويه) a message in such a way as to hide its contents is called **encryption**. An encrypted message is **cipher text**. The process of truing cipher text back into plaintext is **decryption**; this is all shown in figure below.



Plain text is denoted by **M**, for message or **P** for plaintext. It can be a stream of bits, a text file, a bitmap, a stream of digitized voice, a digital video image. Whatever. As far as a computer is concerned, **M** is simply binary data.

Cipher text is denoted by **C**. it is also binary data: some the same size as **M**. some time larger (by combining encryption with compression. **C** may be smaller than **M**).

The encryption functions **E** operate on **M** to produce **C**, or, in mathematical notation. $E(M) = C$

In the reverse process, the decryption functions **D** operate on **C** to produce **M**:

$$D(C) = M$$

Since the whole point of encryption and then decryption a message is to recover the original plain text, the following identity must hold true.

$$D(E(M)) = M$$

❖ The Components of Cryptographic System (Cryptosystem):-

1. A plaintext message (P).
2. A Ciphertext message (C).
3. A Key (K).
4. Enciphering transformations $C = E_{k1} (P)$
5. Deciphering transformations $P = D_{k2} (C)$

❖ The General Requirements of Cryptosystem:-

Cryptosystem must satisfy three general requirements:

- 1) The enciphering and deciphering transformations must be efficient for all keys.
- 2) The system must be easy to use.
- 3) The security of the system should depend only on the secrecy of the keys and not on the secrecy of the algorithms Encryption or Decryption.

❖ Cryptanalysis:-

Is the science and study of methods of breaking ciphers. A cipher is breakable if it is possible to determine the plaintext or key from the Ciphertext or to determine the key from both plaintext and Ciphertext.

❖ Types of Cryptanalysis attacks:-**1. Ciphertext-only attack:-**

The cryptanalyst has the cipher text of several messages, all of which have been encrypted using the same encryption algorithm, the cryptanalyst job is to recover the plain text of many message as possible, or better yet to deduce the key (or keys) used to encrypt the message. In order to decrypt other message encrypted with the same keys.

2. Known-plaintext attack:-

The cryptanalyst (attacker) has access not only to the cipher text of several message, but also to the plain text of those message. His job is to deduce the key (or keys) used to encrypt the message or an algorithm to decrypt any new message encrypted with the same key, (or keys).

3. Chosen-plaintext attack:-

The cryptanalyst (attacker) not only has access to the cipher text and associated plain text for several message. But he also chooses the plain text that gets encrypted, so his job is to divide the plaintext into several blocks by which he can deduce the key (or keys) used to encrypt the message or an algorithm to decrypt any new message encrypted with the same key (or keys).

4. Adaptive-chosen-plaintext attack:-

This is a special case of a chosen-plaintext attack. Not only can the cryptanalyst (attacker) choose the plaintext that is encrypted, but he can also modify his choice based on the result of previous encryption

5. Chosen-Ciphertext attack:-

The cryptanalyst (attacker) here can choose a set of encrypted messages and try to decrypt them to access the plaintext text with the key. This method is used to attack cryptographic systems using two keys K_1 , K_2 that is known as *Public-Key algorithm*, and sometimes attack cryptographic systems using one key which is known as *One-Key algorithm*.

6. Chosen-key attack:-

Here the cryptanalyst (attacker) has some information that has to do with different keys and tries to reach the desired key.

7. Rubber-hose cryptanalysis:-

Is the use of bribery, extortion and threat to access the key.

Note that, the methods from 1 to 4 assume that the cryptanalyst has complete knowledge of the encryption algorithm used.

❖ Threats types:-

1. **Passive:-** does not affect the system, just take the wanted data and information.
2. **Active:-** affect the system in addition to have the wanted data and information.

Types of Cryptosystem depending on keys:-

1. **Symmetric algorithms:-** this type also called Conventional System or Single-Key or One-Key in which (**key₁ = key₂**).
2. **Asymmetric algorithms:-** also called (Public-Key algorithm), use two different keys that is (**key₁ ≠ key₂**).

Note that:-

Encryption-key (k₁) is a **Public-Key** while Decryption-key (k₂) is **Private-Key**.

Mathematical Background

Number Theory:-

If we have a, b are integer numbers and $n > 0$

$a \bmod n = r$ where r is the remainder and $0 \leq r \leq n-1$

The rule will be:- $a \equiv b \pmod{n}$

If and only if one of these three conditions is satisfied:-

1. $a \bmod n = b \bmod n$
2. $n/(a-b)$ note that no remainder from this division.
3. $a \times k + b = n$ where k is an integer.

Example (1) :- $3 \equiv 2 \pmod{5}$ ____ $a=3$ $b=2$ $n=5$

1. $a \bmod n = b \bmod n$
 $3 \bmod 5 = 2 \bmod 5$
 $3 \neq 2$ (not satisfied)
2. $n/(a-b)$
 $5/(3-2)$
 $5/1 = 5$
3. $a \times k + b = n$
 $3 \times k + 2 = 5$
 $3k = 5-2$
 $3k = 3 \rightarrow k=1$ (must be integer)

Example (2) :- $17 \equiv 2 \pmod{5}$ ____ $a=17$ $b=2$ $n=5$

1. $a \bmod n = b \bmod n$
 $17 \bmod 5 = 2 \bmod 5$
 $2 = 2$ (this condition is satisfied)
2. $n/(a-b)$
 $5/(17-2)$
 $5/15$ (not satisfied because the result is not integer number)

$$3. a \times k + b = n$$

$$17 \times k + 2 = 5$$

$$17k = 5 - 2$$

$17k = 3 \rightarrow k = 3/17$ (k must be integer, not satisfied because the result is not integer number)

❖ Greatest Common Divisor GCD:-

Note that:- GCD (*Greatest Common Divisor*) of two or more integers, where at least one of them is non zero, is the largest positive integer that divides the numbers without a remainder, for example, the GCD of 8 and 12 is 4.

GCD is also known as *Greatest Common Factor* (GCF) or *Highest Common Factor* (HCF).

❖ Computing GCD using Subtraction method:-

وهي أن تقوم بطرح العدد الأصغر من الأكبر لتحصل على ناتج، ثم تطرحه من العدد الأصغر في البداية وتقوم بالأمر حتى تجد النتيجة صفر أي عندما يساوي $a = b$ وعندها ذلك هو القاسم المشترك وكما في المثال التالي:- لحساب القاسم المشترك الأكبر (198، 252)

$$\text{Abs}(252 - 198) = 54$$

$$\text{Abs}(198 - 54) = 144$$

$$\text{Abs}(144 - 54) = 90$$

$$\text{Abs}(90 - 54) = 36$$

$$\text{Abs}(54 - 36) = 18$$

$$\text{Abs}(36 - 18) = 18$$

$$\text{Abs}(18 - 18) = 0$$

$$\therefore \text{GCD}(252, 198) = 18$$

❖ **Computing GCD using Euclid's Algorithm method:-**

Use the theorem that:- $\text{GCD}(a, b) = \text{GCD}(b, a \bmod b)$

Euclid's Algorithm for computing GCD (a , b)

- A=a , B=b
- While B>0
 - R = A mod B
 - A = B
 - B = R
- Return A

Note that:-

- ✓ R = remainder and if R = 0 then GCD (a , b) = b
- ✓ Always (a > b)

Example (1):- Find GCD (1970 , 1066)

a=1970 b= 1066

A	B	R = A mod B
1970	1066	904
1066	904	162
904	162	94
162	94	68
94	68	26
68	26	16
26	16	10
16	10	6
10	6	4
6	4	2
4	2	0

Example (2):- GCD (27,18)

$$27 = 18 \cdot 1 + 9$$

$$18 = 9 \cdot 2 + 0$$

$$\text{GCD}(27,18) = 9$$

Example (3):- GCD (5,3)

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 1 + 1$$

$$1 = 1 \cdot 1 + 0$$

$$\text{GCD}(5,3) = 1$$

Example (4):- GCD (123,4567)

$$4567 = 123 \cdot 37 + 16$$

$$123 = 16 \cdot 7 + 11$$

$$16 = 11 \cdot 1 + 5$$

$$11 = 5 \cdot 2 + 1$$

$$5 = 1 \cdot 5 + 0$$

$$\text{GCD}(123,4567) = 1$$

Example (5):- GCD (34 , 17)

$$a=34 \quad b=17$$

$$34 = 2 \times 17 + 0 \quad (\text{here } R=0, \text{ so } \text{GCD}(34, 17) = 17 = b)$$

❖ Computing Inverse for two Dim matrix:-

حساب المعكوس للمصفوفة

يقصد به المعكوس الضربي للمصفوفة بحيث يكون حاصل ضرب [المصفوفة](#) في معكوسها يساوي [مصفوفة الوحدة](#).

إيجاد معكوس المصفوفة :

$$A^{-1} = \frac{\text{Adj}(A)}{|A|} \quad \text{يمكن إيجاد معكوس المصفوفة من القانون التالي :}$$

لحساب معكوس المصفوفة :

- حساب محدد المصفوفة والتأكد أنه لا يساوي صفر .
- حساب المصفوفة المرتبطة (المرافقة أو المصاحبة) .
- حساب المعكوس من القانون اعلاه .

قيمة المحدد :

- إذا كان المحدد من الدرجة الثانية 2×2 فإن قيمته تساوي مجموع حاصل ضرب عناصر القطر الرئيسي مطروحاً منه مجموع حاصل ضرب عناصر القطر الآخر .

$$\text{القطر الرئيسي} \rightarrow \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

يرمز للمحدد بالرمز Δ دلنا

مثال :

$$\Delta = \begin{vmatrix} -6 & -7 \\ 10 & 8 \end{vmatrix} = -6(8) - 10(-7) = -48 - (-70) = -48 + 70 = 22$$

إشارة المحدد

$$\begin{vmatrix} + & - & + \\ - & + & - \\ + & - & + \end{vmatrix}, \quad \begin{vmatrix} + & - \\ - & + \end{vmatrix}$$

- إذا كان المحدد من الدرجة الثالثة 3×3 فيمكن حساب قيمته باستعمال قاعدة الأقطار .
- خطوات إيجاد قيمة المحدد بقاعدة الأقطار :-
- 1 إعادة كتابة العمود الأول والثاني على يمين المحدد .
- 2 إيجاد مجموع حاصل ضرب عناصر القطر الرئيسي والقطرين الموازيين له على يمينه كما هو موضح بالصورة التالية :

a	b	c	b	c
d	e	f	e	f
g	h	i	h	i

- 3 إيجاد مجموع حاصل ضرب عناصر القطر الآخر والقطرين الموازيين له على يمينه كما هو موضح بالصورة التالية :

a	b	c	b	c
d	e	f	e	f
g	h	i	h	i

- 4 إيجاد قيمة المحدد بطرح ناتج الخطوة 3 من ناتج الخطوة 2

مثال :-

$$\begin{vmatrix} -8 & -4 & 1 \\ 0 & -5 & 6 \\ 3 & 4 & 2 \end{vmatrix} \text{ أوجد قيمة المحدد}$$

الحل :

1- إعادة كتابة المحدد بوضع العمودين الأول والثاني يمين المحدد

$$\begin{vmatrix} -8 & -4 & 1 \\ 0 & -5 & 6 \\ 3 & 4 & 2 \end{vmatrix} \begin{vmatrix} -8 & -4 \\ 0 & -5 \\ 3 & 4 \end{vmatrix}$$

2- إيجاد مجموع حاصل ضرب عناصر الأقطار :

$$\begin{vmatrix} -8 & -4 & 1 \\ 0 & -5 & 6 \\ 3 & 4 & 2 \end{vmatrix} \begin{vmatrix} -8 & -4 \\ 0 & -5 \\ 3 & 4 \end{vmatrix}$$

$$\begin{aligned} -8 (-5) 2 &= 80 \\ -4 (6) (3) &= -72 \\ 1 (0) (4) &= 0 \end{aligned}$$

$$80 + (-72) + 0 = 8$$

$$\begin{vmatrix} -8 & -4 & 1 \\ 0 & -5 & 6 \\ 3 & 4 & 2 \end{vmatrix} \begin{vmatrix} -8 & -4 \\ 0 & -5 \\ 3 & 4 \end{vmatrix}$$

$$\begin{aligned} 3 (-5) (1) &= -15 \\ 4 (6) (-8) &= -192 \\ 2 (0) (4) &= 0 \end{aligned}$$

$$-15 + (-192) + 0 = -207$$

3- طرح المجموع الثاني -207 من المجموع الأول 8

$$8 - (-207) = 8 + 207 = 215$$

4- إذن قيمة المحدد :-

$$\Delta = 215$$

مصفوفة المرافقات

إذا كانت $A = [a_{ij}]$ مصفوفة مربعة من درجة n فإننا نعرف العامل المرافق α_{ij} لعنصر a_{ij} ويحسب كالتالي :

$$Adj(A) = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix}, \quad \alpha_{ij} = (-1)^{i+j} M_{ij}$$

مثال : أوجد Adj المصفوفة التالية :

$$A = \begin{bmatrix} 1 & 1 & 3 \\ 0 & 1 & 0 \\ 2 & 0 & 4 \end{bmatrix}$$

الحل :

نقوم بحذف الصف والعمود الواقع فيهما العنصر ونضرب عناصر القطر الرئيسي مطروحاً منه ضرب عناصر القطر الآخر مع الأخذ بالاعتبار إشارة المحدد لكل عنصر :

$$\begin{vmatrix} + & - & + \\ - & + & - \\ + & - & + \end{vmatrix}$$

نأتي بالعنصر x_{11} والذي إشارته حسب المحدد + إذن نضرب المحدد ب +1

$$\alpha_{11} = +1 \begin{vmatrix} 1 & 0 \\ 0 & 4 \end{vmatrix} = +1(4 - 0) = 4$$

نأتي بالعنصر x_{12} والذي إشارته حسب المحدد - إذاً نضرب المحدد ب -1

$$\alpha_{12} = -1 \begin{vmatrix} 0 & 0 \\ 2 & 4 \end{vmatrix} = -1(0 - 0) = 0$$

نكمل الحل على نفس الطريقة :-

$$\alpha_{13} = +1 \begin{vmatrix} 0 & 1 \\ 2 & 0 \end{vmatrix} = +1(0 - 2) = -2$$

$$\alpha_{21} = -1 \begin{vmatrix} 1 & 3 \\ 0 & 4 \end{vmatrix} = -1(4 - 0) = -4$$

$$\alpha_{22} = +1 \begin{vmatrix} 1 & 3 \\ 2 & 4 \end{vmatrix} = +1(4 - 6) = -2$$

$$\alpha_{23} = -1 \begin{vmatrix} 1 & 1 \\ 2 & 0 \end{vmatrix} = -1(0 - 2) = 2$$

$$\alpha_{31} = +1 \begin{vmatrix} 1 & 3 \\ 1 & 1 \end{vmatrix} = +1(1 - 3) = -2$$

$$\alpha_{32} = -1 \begin{vmatrix} 1 & 3 \\ 0 & 1 \end{vmatrix} = -1(1 - 0) = -1$$

$$\alpha_{33} = +1 \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = +1(1 - 0) = 1$$

نقوم بصف العناصر الناتجة على شكل مصفوفة مرافقات .
إذن مصفوفة المرافقات تساوي :

$$Adj(A) = \begin{bmatrix} 4 & 0 & -2 \\ -4 & -2 & 2 \\ -2 & -1 & 1 \end{bmatrix}$$

حالة خاصة : حينما تكون المصفوفة 2×2 فلايجاد مصفوفة المرافقات لها نقوم بما يلي :

- 1- نبدل عناصر القطر الرئيسي .
- 2- نقلب إشارة عناصر القطر الآخر .

مثال :

$$A = \begin{bmatrix} 3 & 1 \\ 2 & 4 \end{bmatrix}$$

$$Adj(A) = \begin{bmatrix} 4 & -1 \\ -2 & 3 \end{bmatrix}$$

مثال 1 :-

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 2 \\ 3 & 3 & 4 \end{bmatrix}$$

الحل :

$$A^{-1} = \frac{Adj(A)}{|A|}$$

إذاً أولاً نأتي بـ $Adj(A)$:

$$\alpha_{11} = +1 \begin{vmatrix} 3 & 2 \\ 3 & 4 \end{vmatrix} = +1(12 - 6) = 6$$

$$\alpha_{12} = -1 \begin{vmatrix} 2 & 2 \\ 3 & 4 \end{vmatrix} = -1(8 - 6) = -2$$

$$\alpha_{13} = +1 \begin{vmatrix} 2 & 3 \\ 3 & 3 \end{vmatrix} = +1(6 - 9) = -3$$

$$\alpha_{21} = -1 \begin{vmatrix} 2 & 3 \\ 3 & 4 \end{vmatrix} = -1(8 - 9) = 1$$

$$\alpha_{22} = +1 \begin{vmatrix} 1 & 3 \\ 3 & 4 \end{vmatrix} = +1(4 - 9) = -5$$

$$\alpha_{23} = -1 \begin{vmatrix} 1 & 2 \\ 3 & 3 \end{vmatrix} = -1(3 - 6) = 3$$

$$\alpha_{31} = +1 \begin{vmatrix} 2 & 3 \\ 3 & 2 \end{vmatrix} = +1(4 - 9) = -5$$

$$\alpha_{32} = -1 \begin{vmatrix} 1 & 3 \\ 2 & 2 \end{vmatrix} = -1(2 - 6) = -4$$

$$\alpha_{33} = +1 \begin{vmatrix} 1 & 2 \\ 2 & 3 \end{vmatrix} = +1(3 - 4) = -1$$

$$Adj(A) = \begin{bmatrix} 6 & -2 & 3 \\ 1 & -5 & 3 \\ -5 & 4 & -1 \end{bmatrix}$$

ثانياً نأتي بـ $|A|$:

$$|A| = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 2 \\ 3 & 3 & 4 \end{vmatrix} \begin{vmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 3 \end{vmatrix}$$

$$= [1(3)(4) + 2(2)(3) + 3(2)(3)] - [3(3)(3) + 3(2)(1) + 4(2)(2)]$$

$$= (12 + 12 + 18) - (27 + 6 + 16)$$

$$= 42 - 49$$

$$= -7$$

So:-

$$A^{-1} = \frac{1}{-7} \begin{bmatrix} 6 & -2 & 3 \\ 1 & -5 & 3 \\ -5 & 4 & -1 \end{bmatrix}$$

Matrix Multiplication:- ضرب المصفوفات

إذا كانت هناك مصفوفتان A, B فإنهما تكونان قابلتين للضرب إذا كان عدد الأعمدة في المصفوفة اليسرى A مساوياً لعدد الصفوف في المصفوفة اليمنى B . فعلى سبيل المثال، المصفوفتين A , B رتبتهما (3 x 2) , (2 x 2) على الترتيب وتتكون من:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

حاصل الضرب $C = AB$ هو مصفوفة رتبتهـا (3 x 2) تعرف كالآتي:-

$$C = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \\ a_{31}b_{11} + a_{32}b_{21} & a_{31}b_{12} + a_{32}b_{22} \end{pmatrix}$$

أي أن المصفوفة الناتجة لها عدد من الصفوف يساوي عدد صفوف المصفوفة الأولى A وعدد من الأعمدة يساوي عدد أعمدة المصفوفة الثانية B ويكون كل عنصر من عناصر المصفوفة C وليكن C_{ik} (أي الواقع في الصف رقم I والعمود رقم k) مساوياً لمجموع حواصل ضرب عناصر الصف رقم I في المصفوفة اليسرى A في عناصر العمود رقم k من المصفوفة اليمنى B في نظيره.

مثال : إيجاد حاصل ضرب المصفوفتين:

$$A = \begin{pmatrix} 2 & 3 & -1 \\ 4 & 1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 1 \\ 4 & -2 \\ 5 & -3 \end{pmatrix}$$

الحل

$$C = A \times B$$

$$\begin{aligned} &= \begin{pmatrix} 2 \times 2 + 3 \times 4 + (-1 \times 5) & 2 \times 1 + 3 \times -2 + (-1 \times -3) \\ 4 \times 2 + 1 \times 4 + 2 \times 5 & 4 \times 1 + 1 \times -2 + 2 \times -3 \end{pmatrix} \\ &= \begin{pmatrix} 11 & -1 \\ 22 & -4 \end{pmatrix} \end{aligned}$$

مثال : إذا أخذنا:

$$\mathbf{A}_{(2 \times 3)} = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}, \quad \mathbf{B}_{(3 \times 2)} = \begin{pmatrix} 1 & 2 \\ 3 & 1 \\ 2 & 3 \end{pmatrix}$$

فإن المصفوفة A قابلة للضرب في المصفوفة B ويعطى حاصل الضرب C = AB من :-

$$\begin{aligned} \mathbf{C}_{(2 \times 2)} &= \begin{pmatrix} 3 \times 1 + 1 \times 3 + 2 \times 2 & 3 \times 2 + 1 \times 1 + 2 \times 3 \\ 2 \times 1 + 1 \times 3 + 3 \times 2 & 2 \times 2 + 1 \times 1 + 3 \times 3 \end{pmatrix} \\ &= \begin{pmatrix} 10 & 13 \\ 11 & 14 \end{pmatrix} \end{aligned}$$

ومن جهة أخرى فإن المصفوفة B قابلة للضرب في المصفوفة A ويعطى حاصل الضرب D = BA من :-

$$\begin{aligned} \mathbf{D}_{(3 \times 3)} &= \begin{pmatrix} 1 \times 3 + 2 \times 2 & 1 \times 1 + 2 \times 1 & 1 \times 2 + 2 \times 3 \\ 3 \times 3 + 1 \times 2 & 3 \times 1 + 1 \times 1 & 3 \times 2 + 1 \times 3 \\ 2 \times 3 + 3 \times 2 & 2 \times 1 + 3 \times 1 & 2 \times 2 + 3 \times 3 \end{pmatrix} \\ &= \begin{pmatrix} 7 & 3 & 8 \\ 11 & 4 & 9 \\ 12 & 5 & 13 \end{pmatrix} \end{aligned}$$

ومن هذا يتضح أن $AB \neq BA$ أي أن خاصية الإبدال لاتصلح للمصفوفات حتى لو كانت رتبة مصفوفة

حاصل ضرب $A \times B$ تساوي رتبة مصفوفة حاصل ضرب $B \times A$.

وضرب المصفوفات له الخصائص التالية :-

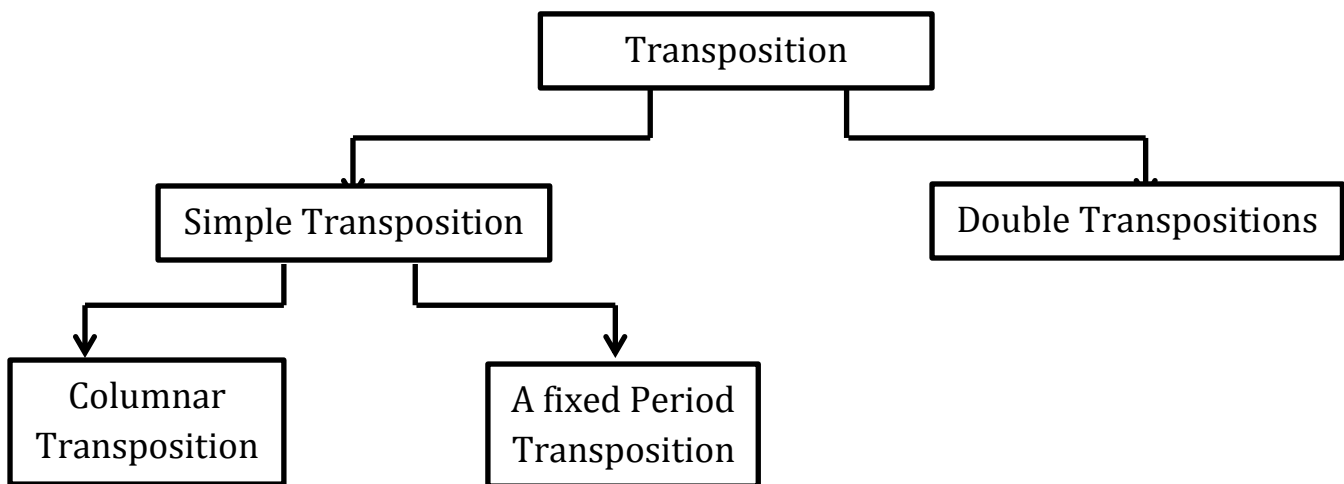
- 1) $A (B + X) = AB + AX$
- 2) $(A + B) C = AC + BC$
- 3) $A (BC) = AB (C)$

Chapter Three

Traditional related to all ciphers used before seventies, they are divided into:-

1. Transposition Ciphers
2. Substitution Ciphers

1. Transposition Ciphers



Simple Transposition Columnar Transposition:-

1. Compute the characters in plaintext.
2. Create two dimensional matrix (no. of row \times no. of columns equal the length of plaintext and be sure that the no. of columns must be the largest, for example, if the length of plaintext equal to 15 then the Dim of a matrix will be 3×5 (3-rows and 5-columns). If the length of plaintext equal to 17 then the Dim of a matrix will be 3×6 (3-rows and 6-columns).
3. The length of key equal to the no. of columns.
4. Fill matrix locations with characters of plaintext row by row and in case there is an empty location in matrix, fill it with (x).
5. Put the key as a label for columns.
6. To get the cipher text, scan the columns of matrix depending on key values and take the corresponding matrix values.

Example 1:-

If the plaintext = ibnalhaithem

The length of plaintext = 12

Dim of Matrix= 3×4

Now using key= 4213 so the length of key = 4

4 2 1 3

i b n a

l h a i

t h e m

Now to have the cipher text, use the key in sequential and take the corresponding matrix contents as shown below:-

C= nae bhh aim ilt

C= naebhhaimilt

No. of column 1 2 3 4

For Deciphering:- create the same DIM empty matrix then filling it with the cipher text depending on the key 4213, then scan matrix elements row by row as shown below:-

4 2 1 3

i b n a

l h a i

t h e m

P= ibnalhaithem

Example 2:-

Plaintext = this is transposition

Key = code

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
		1	2	3											4										
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

∴ Key = code = 1423

The length of plaintext = 19

Dim of Matrix= 4×5

	1	4	2	3
t	h	i	s	
i	s	t	r	
a	n	s	p	
o	s	i	t	
i	o	n	x	

∴ Cipher text = tiaoi itsin srptx hsnso

Example 3:-

Plaintext = WE ARE DISCOVERED FLEE AT ONCE

Key = ZEBRAS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2		3												4	5									6
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

∴ Key = ZEBRAS = 632415

The length of plaintext = 25

Dim of Matrix= 6×5

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	X	X	X	X	X

∴ Cipher text = EVLNX ACDTX ESEAX ROFOX DEECX WIREE

Simple Transposition (Fixed Period d):-

1. Divide plaintext into equal periods.
2. The length of key equal to the length of period, if d=4 then length of key =4 also.

Using the previous example If the plaintext = ibnalhaithem and d=4 then the length of key=4

i	b	n	a	l	h	a	i	t	h	e	m
1	2	3	4	1	2	3	4	1	2	3	4

If key = 4213

C=	a	b	i	n	i	h	l	a	m	h	t	e	C= abinih	l	a	m	h	t	e
	4	2	1	3	4	2	1	3	4	2	1	3							

For Deciphering, begin first with the (CC) text using $k_2 = 4123$ to get intermediate cipher text (C), then use $k_1 = 3142$ to get plaintext, as shown below:-

$$\begin{array}{cccc|cccc|cccc|cccc} \text{CC=} & \text{t} & \text{h} & \text{a} & \text{i} & \text{d} & \text{e} & \text{e} & \text{i} & \text{r} & \text{a} & \text{b} & \text{h} & \text{m} & \text{x} & \text{e} & \text{x} \\ & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 \end{array}$$

Now using $k_2 = 4123$ to get (C)

$$\begin{array}{cccc|cccc|cccc|cccc} \text{C=} & \text{h} & \text{a} & \text{i} & \text{t} & \text{e} & \text{e} & \text{i} & \text{d} & \text{a} & \text{b} & \text{h} & \text{r} & \text{x} & \text{e} & \text{x} & \text{m} \\ & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \end{array}$$

Now using $k_1 = 3142$ to get plaintext (P)

$$\begin{array}{cccc|cccc|cccc|cccc} \text{C=} & \text{h} & \text{a} & \text{i} & \text{t} & \text{e} & \text{e} & \text{i} & \text{d} & \text{a} & \text{b} & \text{h} & \text{r} & \text{x} & \text{e} & \text{x} & \text{m} \\ & 3 & 1 & 4 & 2 & 3 & 1 & 4 & 2 & 3 & 1 & 4 & 2 & 3 & 1 & 4 & 2 \end{array}$$

$$\begin{array}{cccc|cccc|cccc|cccc} \text{P=} & \text{a} & \text{t} & \text{h} & \text{i} & \text{e} & \text{d} & \text{e} & \text{i} & \text{b} & \text{r} & \text{a} & \text{h} & \text{e} & \text{m} & \text{x} & \text{x} \\ & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \end{array}$$

Example :- use the previous example but using two different simple transposition (Columnar and Fixed Period) with $k_1 = 31524$ for columnar and $k_2 = 3142$ with $d = 4$ for Fixed period.

$P = \text{athiedeibrahem}$ So, Plaintext length=14 \therefore Dim of matrix = 5×3

3	1	5	2	4
a	t	h	i	e
d	e	i	b	r
a	h	e	m	x

$C = \text{the ibm ada erx hie}$

$C = \text{tehibmadaerxhie}$

No. of column	1	2	3	4	5
---------------	---	---	---	---	---

Now using $k_2 = 3142$ with $d = 4$ for Fixed period

$C =$	t	e	h	i	b	m	a	d	a	e	r	x	h	i	e	x
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4

$CC =$	h	t	i	e	a	b	d	m	r	a	x	e	e	h	x	i	$CC = \text{htieabdmraxeehxi}$
	3	1	4	2	3	1	4	2	3	1	4	2	3	1	4	2	

Now for Deciphering, first use k_2 to decipher (CC) to get the intermediate cipher text (C), then use k_1 to get plaintext (P), as shown below:-

$CC =$	h	t	i	e	a	b	d	m	r	a	x	e	e	h	x	i
	3	1	4	2	3	1	4	2	3	1	4	2	3	1	4	2

C= t e h i | b m a d | a e r x | h i e x
 1 2 3 4 | 1 2 3 4 | 1 2 3 4 | 1 2 3 4

Now using $k_1 = 31524$ columnar method, create matrix with 5-columns because the length of key = 5, so divide the length of C on the length of key to get the number of rows.

Note that we dispose the remainder from division operation.

∴ Length of C=16 and Length of k=5

∴ $16/5=3$ remainder =1(dispose)

C= t e h | i | b m | a d | a | e r x | h i e | x
 1 2 3 | 1 | 2 3 | 1 2 3 | 1 | 2 3 | 1 2 3 |
 1 | | 2 | 3 | 4 | 5 |

3 1 5 2 4

a t h i e

d e i b r

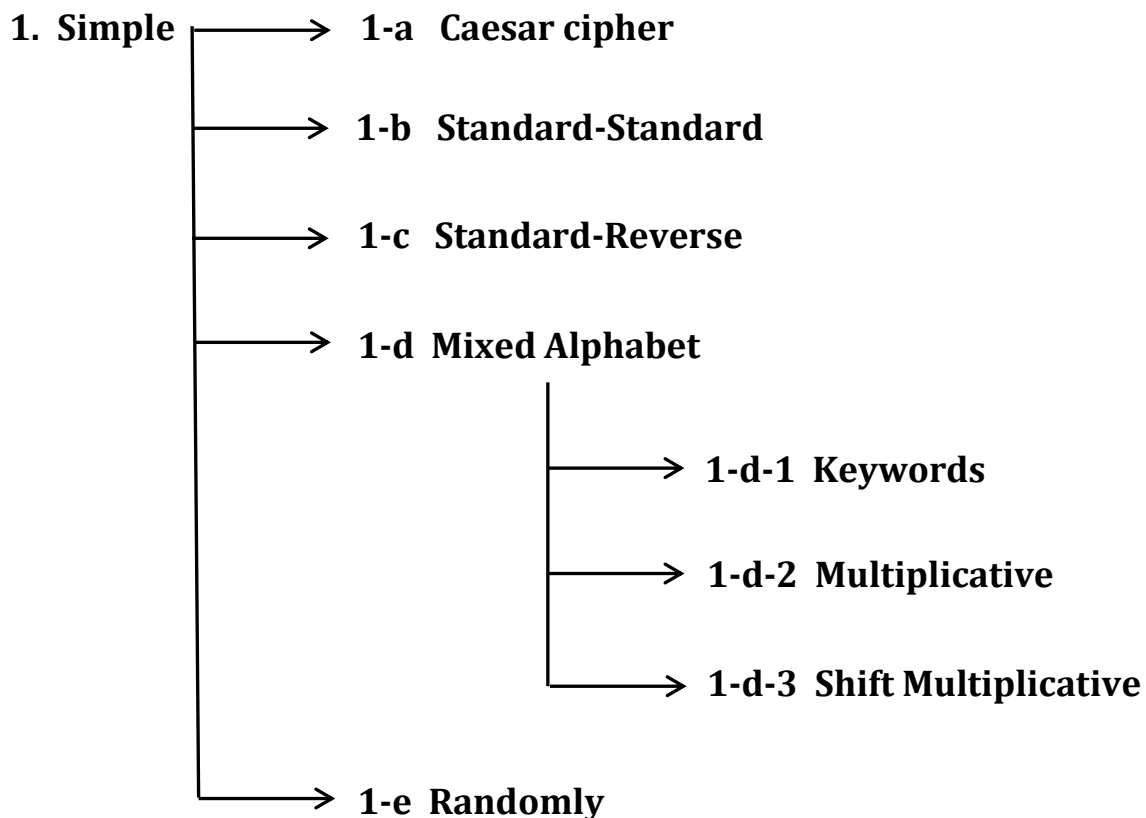
a h e m

∴ P= athiedeibrahem

2. Substitution Ciphers:-

Have four types:-

1. Simple
2. Homophonic
3. Polyalphabetic
4. Polygram (Polygraphic)



In this type of cipher method, we need the English alphabet from a to z.


1-a Caesar cipher:-

The Caesar cipher shifts all the letters in a piece of text by a certain number of places. The key for this cipher is a letter which represents the number of place for the shift. So, for example, a key D means “shift 3 places” and a key M means “shift 12 places”. Note that a key A means “do not shift” and a key Z can either mean “shift 25 places” or “shift one place backwards”. For example, the word “CAESAR” with a shift P becomes “RPTHGP”.

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

- First, write down all the letters of the alphabet.
- Now we will decide a number for encryption. For example, it can be 1, 2, 3... or -1, -2, -3, etc. We will be using "+2" for this example. Now write the all alphabet again under the first one but shift it to right 2 times and transfer surplus letters from the and to the head.
- If we were to encrypt the word "instructables" it would be "glqrpsaryzjcq".

Note that:- While we create the cipher we have used "+2" as key but while decrypting it will be "-2".

Plain line	A B C D E F G H I J K L M N O P Q R S T U V W X <u>Y</u> <u>Z</u>
	
Cipher line	<u>Y</u> <u>Z</u> A B C D E F G H I J K L M N O P Q R S T U V W X

Plain= INSTRUCTABLES	I N S T R U C T A B L E S
	G L Q R P S A R Y Z J C Q

∴ Cipher text will be= GLQRPSARYZJCQ

Note that:- Instead of using numbers we can use **words as keys**.

To do that; choose a word, remove the surplus letters from the word and write the rest of the alphabet next to it.

(Do not write the letters which are on your word as well.)

Note that:- cipher table will always be the same. Bottom line is the cipher line while the top line is decrypted line. It doesn't matter how you write it. For example if the letter is "L" with (-3) you will go back (3) steps and get the letter "I".

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A → 0, B → 1, ..., Z → 25.

Encryption of a letter x by a shift n can be described mathematically as,

$$E_n(x) = (x+n) \bmod 26$$

Decryption is performed similarly,

$$D_n(x) = (x-n) \bmod 26$$

Example:-

Plaintext= THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Key= 3 means deciphering is done in reverse, with a right shift of 3.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

$$D_n(x) = (x-n) \bmod 26$$

$$D(T) = (19-3) \bmod 26 = 16 \bmod 26 = 16 \rightarrow Q$$

$$D(H) = (7-3) \bmod 26 = 4 \bmod 26 = 4 \rightarrow E$$

$$D(E) = (4-3) \bmod 26 = 1 \bmod 26 = 1 \rightarrow B$$

And so on, also you can use the table above to get the cipher text, and the resultant cipher text is

Plaintext= THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Ciphertext= QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

1-b Standard to Standard:- Use the following form:-

For Ciphering $C = (P+K) \bmod 26$

For Deciphering $P = (C-K) \bmod 26$

In case of using Caesar cipher, usually use $k=3$

Example:-

$P = \text{omarabd}$

Key = 4

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$C() = (P+K) \bmod 26$$

$$C(o) = (14+4) \bmod 26 = 18 \rightarrow s$$

$$C(m) = (12+4) \bmod 26 = 16 \rightarrow q$$

$$C(a) = (0+4) \bmod 26 = 4 \rightarrow e$$

$$C(r) = (17+4) \bmod 26 = 21 \rightarrow v$$

$$C(a) = (0+4) \bmod 26 = 4 \rightarrow e$$

$$C(b) = (1+4) \bmod 26 = 5 \rightarrow f$$

$$C(d) = (3+4) \bmod 26 = 7 \rightarrow h$$

$$\therefore C = \text{sqvevfh}$$

$$P() = (C-K) \bmod 26$$

$$P(s) = (18-4) \bmod 26 = 14 \rightarrow o$$

$$P(q) = (16-4) \bmod 26 = 12 \rightarrow m$$

$$P(e) = (4-4) \bmod 26 = 0 \rightarrow a$$

$$P(v) = (21-4) \bmod 26 = 17 \rightarrow r$$

$$P(e) = (4-4) \bmod 26 = 0 \rightarrow a$$

$$P(f) = (5-4) \bmod 26 = 1 \rightarrow b$$

$$P(h) = (7-4) \bmod 26 = 3 \rightarrow d$$

$$\therefore P = \text{omarabd}$$

Note that:-

→ If the result of $(C-K)$ or $(P+K)$ greater than 26, then subtract 26 from it to get positive number that is less than 26.

$$\begin{aligned}\text{Ex:- } C(Z) &= (Z+4) \bmod 26 \\ &= (25+4) \bmod 26 \\ &= (29-26) \bmod 26 \\ &= 3 \bmod 26 \\ &= 3 \rightarrow D\end{aligned}$$

→ In case of the result of $(C-K)$ or $(P+K)$ is negative then use $(26 - (P+K))$ for ciphering or $(26-(C-K))$ for deciphering, this means subtract the negative number from 26, as shown below:-

$$\begin{aligned}\text{Example (1) :- } 29 \bmod 26 &= (29-26) \bmod 26 \\ &= 3 \bmod 26 = 3 \rightarrow D\end{aligned}$$

$$\begin{aligned}\text{Example (2) :- } -1 \bmod 26 &= (29-1) \bmod 26 \\ &= 25 \bmod 26 = 25 \rightarrow Z\end{aligned}$$

1-c Standard-Reverse :- In this method, the shifting is toward the left side, so use the following form:-

For Cipherring $C=(K-P) \bmod 26$

For Decipherring $P=(K-C) \bmod 26$

Example:-

$P=nesrin$ and $k=6$

Use this table of alphabet from a to z with its corresponding numbers from 0 to 25.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$C() = (K-P) \bmod 26$$

$$C(n) = (6-13) \bmod 26 = -7 \bmod 26$$

$$= (26 - 7) \bmod 26$$

$$= 19 \bmod 26 = 19 \rightarrow t$$

$$C(e) = (6-4) \bmod 26 = 2 \rightarrow c$$

$$C(s) = (6-18) \bmod 26 = -12 \bmod 26$$

$$= (26 - 12) \bmod 26$$

$$= 14 \bmod 26 = 14 \rightarrow o$$

$$C(r) = (6-17) \bmod 26 = -11 \bmod 26$$

$$= (26 - 11) \bmod 26$$

$$= 15 \bmod 26 = 15 \rightarrow p$$

$$C(i) = (6-8) \bmod 26 = -2 \bmod 26$$

$$= (26 - 2) \bmod 26$$

$$= 24 \bmod 26 = 24 \rightarrow v$$

$$P() = (K-C) \bmod 26$$

$$P(t) = (6-19) \bmod 26 = -13 \bmod 26$$

$$= (26 - 13) \bmod 26 = 13 \rightarrow n$$

$$P(c) = (6-2) \bmod 26 = 4 \rightarrow e$$

$$P(o) = (6-14) \bmod 26 = -8 \bmod 26$$

$$= (26 - 8) \bmod 26$$

$$= 18 \bmod 26 = 18 \rightarrow s$$

$$P(p) = (6-15) \bmod 26 = -9 \bmod 26$$

$$= (26 - 9) \bmod 26$$

$$= 17 \bmod 26 = 17 \rightarrow r$$

$$C(y) = (6-24) \bmod 26 = -18 \bmod 26$$

$$= (26 - 18) \bmod 26$$

$$= 8 \bmod 26 = 8 \rightarrow i$$

$$C(t) = n$$

1-d Mixed Alphabet :-

1-d-1 Keyword:- in this method we must have a keyword with plaintext, the steps of this method are explained below:-

1. Write the alphabet letters from a to z.
2. Take the keyword with no repeated letters (no repeated letters must be found).
3. Put the new keyword under the corresponding alphabet and the alphabet letters that is not found in the keyword must be added to the end of the keyword.

Example (1):- if the keyword = Baghdad university , Plaintext = mohammed
 Now the new keyword = baghduniversty

For ciphering, use this table (from top line down to the third line)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
*	*		*	*		*	*	*				*				*	*	*	*	*				*	
b	a	g	h	d	u	n	i	v	e	r	s	t	y	c	f	j	k	l	m	o	p	q	w	x	z

Plaintext	m	o	h	a	m	m	e	d	
									C= tcibttdh
ciphertext	t	c	i	b	t	t	d	h	

Now return to algorithm with the following two examples:-

Example (1):- P= aliabd key= 3

Now use the table of alphabet

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$C = (P * K) \bmod 26$$

$$C(a) = (0 * 3) \bmod 26 = 0 \rightarrow a$$

$$C(l) = (11 * 3) \bmod 26 = 33 \bmod 26 = 7 \rightarrow h$$

$$C(i) = (8 * 3) \bmod 26 = 24 \bmod 26 = 24 \rightarrow y$$

$$C(a) = a$$

$$C(b) = (1 * 3) \bmod 26 = 3 \rightarrow d$$

$$C(d) = (3 * 3) \bmod 26 = 9 \rightarrow j \quad \therefore C = ahyadj$$

Example (2):- P= "hello" and key= 7

$$C = (P * K) \bmod 26$$

$$C(h) = (7 * 7) \bmod 26 = 49 \bmod 26 = 23 \rightarrow x$$

$$C(e) = (4 * 7) \bmod 26 = 28 \bmod 26 = 2 \rightarrow c$$

$$C(l) = (11 * 7) \bmod 26 = 77 \bmod 26 = 25 \rightarrow z$$

$$C(l) = z$$

$$C(o) = (14 * 7) \bmod 26 = 20 \rightarrow u \quad \therefore C = xczzu$$

1-d-3 Shift + Multiplicative (Affine Cipher):-

For ciphering:-

$$C = (P * K_1 + k_2) \bmod 26 \text{ with } K_1 \text{ is a prime number}$$

$$T = (P * K_1) \bmod 26$$

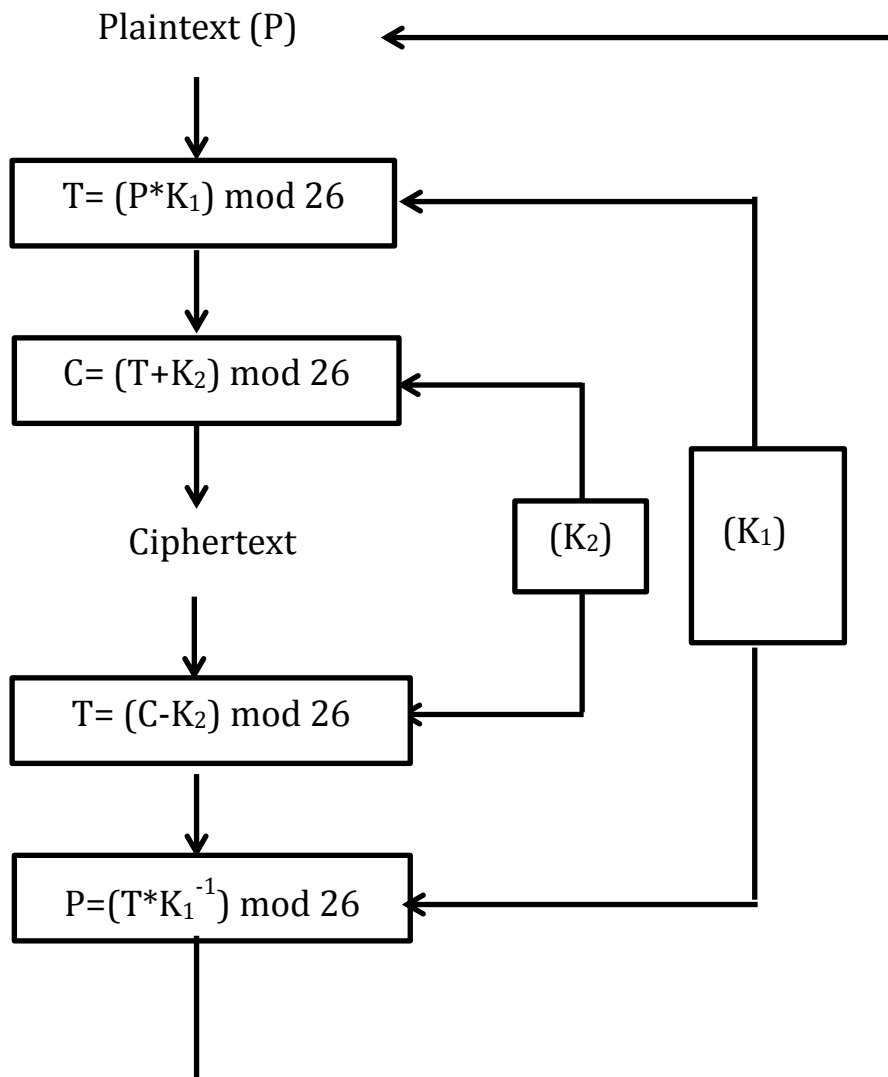
$$C = (T + K_2) \bmod 26$$

For deciphering:-

$$P = ((C - K_2) * K_1^{-1}) \pmod{26}$$

$$T = (C - K_2) \pmod{26}$$

$$P = (T * K_1^{-1}) \pmod{26}$$



Example (1):- Plaintext= omar and K₁=3 and K₂=2

Using the same table of alphabet

a b c d e f g h i j k l m n o p q r s t u v w x y z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

$$C(o) = (14*3+2) \bmod 26$$

$$= 44 \bmod 26 = 18 \rightarrow S$$

$$C(m) = (12*3+2) \bmod 26 = 38 \bmod 26 = 12 \rightarrow m$$

$$C(a) = (0*3+2) \bmod 26 = 2 \rightarrow c$$

$$C(r) = (17*3+2) \bmod 26$$

$$= 53 \bmod 26 = 1 \rightarrow b \quad \therefore C = smcb$$

Example (2):- Plaintext= hello and key (7, 2)

This means $K_1 = 7$ and $K_2 = 2$

$$C(h) = (07*7+2) \bmod 26$$

$$= 25 \bmod 26 = 25 \rightarrow z$$

$$C(e) = (04*7+2) \bmod 26$$

$$= 28 \bmod 26 = 4 \rightarrow e$$

$$C(l) = (11*7+2) \bmod 26 = 1 \rightarrow b$$

$$C(l) = b$$

$$C(o) = (14*7+2) \bmod 26$$

$$= 22 \rightarrow w \quad \therefore C = zebbw$$

Now for deciphering "zebbw" with key pair (7, 2):-

$$P(z) = ((25-2)* 7^{-1}) \bmod 26 = 07 \rightarrow h$$

$$P(e) = ((4-2)* 7^{-1}) \bmod 26 = 07 \rightarrow h$$

$$P(b) = ((1-2)* 7^{-1}) \bmod 26 = 11 \rightarrow l$$

$$P(b) = 11 \rightarrow l$$

$$P(w) = ((22-2)* 7^{-1}) \bmod 26 = 14 \rightarrow o \quad \therefore P = hello$$

1-e Randomly:-

يتم الاتفاق بين شخصين على ان احرف معينة يقابلها احرف معينة اخرى

Example:-

$$P(o) = C(s) \quad P(m) = C(t) \quad P(a) = C(f) \quad P(r) = C(k)$$

If P= omarabd

Then C= stfkckfbd

2. Homophonic Substitution Cipher:-

2.1 Beal Cipher:- Each letter in the secret message is replaced with a number which represents the position of a word in an assistant text which start with this letter.

في هذه الطريقة لا يوجد مفتاح للحل ولكن يوجد نص مساعد حيث ان اول حرف من كل كلمة في النص ياخذ رقم وبدون تكرار وهذا الرقم يمثل رقم الكلمة او تسلسل الكلمة ضمن هذا النص المساعد.

Example (1):- If the assistant text = zainab muhammed and P= zahzuh

The assistant text will be as follows after dispose the repeated letters from it.

Assistant text = zainbmuhed

z	a	i	n	b	m	u	h	e	d
01	02	03	04	05	06	07	08	09	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
...

P= z a h z u h C= 010208110718
 C= 01 02 08 11 07 18

Now for Deciphering:-

C= 01 02 08 11 07 18 P= zahzuh

P= z a h z u h

Example (2):- If the assistant text = Republic of Iraq university of Baghdad College of Education for Pure Science

P= PURECUPES

Assistant text = Republic Of Iraq University Of Baghdad College Of Education For Pure Science

The first letter from each word in assistant text will be = ROIUOBCEFPS

The assistant text will be after dispose repeated letters will be = ROIUBCEFPS

R	O	I	U	B	C	E	F	P	S
01	02	03	04	05	06	07	08	09	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
...

Plaintext= P U R E C U P E S C= 090401070614191710
 Ciphertext= 09 04 01 07 06 14 19 17 10

ملاحظة:- كل رمز يستخدم مرة واحدة فقط مثلا في المثال السابق احتجنا الى الحرف (e) مرتين في النص الصريح لكن في النص المشفر فكل مرة اخذ قيمة رقمية مختلفة مرة اخذ الرقم 07 ومرة اخرى اخذ الرقم 17.

2.2 Multiequivalent Substitution:-

For each letter of alphabet letters there are two sets of symbols and then you get two different messages, one real and the other fake. Since each text is encrypted, there are two explicit texts. When analyze the code, the

cryptanalyst will get two meaningful texts, so he or she should decide which one is real and the other is fake. This will increase the confidentiality of the system.

لكل حرف من الحروف الابجدية يوجد مجموعتين من الرموز فيتم عند ذلك الحصول على رسالتين مختلفتين احدهما حقيقية والاخرى مزيفة.

وبما انه لكل نص مشفر هنالك نصين صريحين لذلك عند تحليل الشفرة سوف يحصل المحلل على نصين ذات معنى وبالتالي عليه ان يقرر احدى هاتين الرسالتين حقيقية والاخرى مزيفة وهذا سوف يزيد من درجة السرية للنظام.

3. Polyalphabetic Substitution Cipher:-

The difference between this method and Simple Substitution is that the Polyalphabetic use multiple substitutions while Simple substitution Ciphers are considered as monoalphabetic simple substitution cipher.

ميزة هذه الطرق هو تكرار المفتاح اسفل النص الصريح.

This method has three type of ciphering:-

3.1 Vigenere Cipher:- is the simplest Polyalphabetic substitution cipher in which key is multiple letters long.

المفتاح عبارة عن كلمة وتكرر تحت النص الصريح ويكون الحل هنا باستخدام طريقتين اما باستخدام الجدول او باستخدام المعادلات وكما في الصيغة التالية:- (مشابهة لصيغة *standard-standard*) لكن في هذه الطريقة يتم تكرار المفتاح اسفل النص الصريح لاكثر من مرة وبشكل دوري بينما في صيغة (*standard-standard*) فيتم استخدام المفتاح كقيمة رقمية مثلا $K=4$

For ciphering $C = (P+K) \bmod 26$

For deciphering $P = (C-K) \bmod 26$

اما باستخدام الجدول فيتم استخدام طريقة *Shifting* للحروف الى جهة اليسار مع ملاحظة ان الاعمدة في الجدول تمثل *plaintext* بينما الاسطر تمثل *key*. حيث نضع النص الصريح *plaintext* ونضع تحته الكلمة المفتاحية (*key*) ونبحث عن حالات تقاطع الحرف في النص الصريح *plaintext* مع الحرف في (*key*) ضمن الجدول. ملاحظة ان هذا الجدول يستخدم فقط للتشفير.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Example (1):- Plaintext = cryptography

Key = ali

By using table:-

plaintext values = c r y p t o g r a p h y
 Key word =

a	l	i
---	---	---

a	l	i
---	---	---

a	l	i
---	---	---

a	l	i
---	---	---

 cipher values = c c g p e w g c i p s g

Example (2):- Plaintext = the forth class

Key = car

(1):- By using table:-

plaintext values = t h e f o r t h c l a s s
 Key word = c a r | c a r | c a r | c a r | c
 cipher values = v h v h o i v h t n a j u

(2):- By using equations of ciphering and deciphering:-

plaintext=	t	h	e	f	o	r	t	h	c	l	a	s	s
	19	7	4	5	14	17	19	7	2	11	0	18	18

Key word=	c	a	r	c	a	r	c	a	r	c	a	r	c
	2	0	17	2	0	17	2	0	17	2	0	17	2

For ciphering:-

$$C=(P+K) \bmod 26$$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$C(t) = (19+2) \bmod 26 = 21 \rightarrow v$$

$$C(h) = (7+0) \bmod 26 = 7 \rightarrow h$$

$$C(e) = (4+17) \bmod 26 = 21 \rightarrow v$$

$$C(f) = (5+2) \bmod 26 = 7 \rightarrow h$$

$$C(o) = (14+0) \bmod 26 = 14 \rightarrow o$$

$$C(r) = (17+17) \bmod 26 = 8 \rightarrow i$$

$$C(t) = (19+2) \bmod 26 = 21 \rightarrow v$$

$$C(h) = (7+0) \bmod 26 = 7 \rightarrow h$$

$$C(c) = (2+17) \bmod 26 = 19 \rightarrow t$$

$$C(l) = (11+2) \bmod 26 = 13 \rightarrow n$$

$$C(a) = (0+0) \bmod 26 = 0 \rightarrow a$$

$$C(s) = (18+17) \bmod 26 = 9 \rightarrow j$$

$$C(s) = (18+2) \bmod 26 = 20 \rightarrow u$$

$\therefore C = v h v h o i v h t n a j u$

Now for deciphering:-

plaintext values = v h v h o i v h t n a j u

Key word = c a r c a r c a r c a r c

$$P=(C-K) \bmod 26$$

$$P(v) = (21-2) \bmod 26 = 19 \rightarrow t$$

$$P(h) = (7-0) \bmod 26 = 7 \rightarrow h$$

$$P(v) = (21-17) \bmod 26 = 4 \rightarrow e$$

$$P(h) = (7-2) \bmod 26 = 5 \rightarrow f$$

- $P(o) = (14-0) \bmod 26 = 14 \rightarrow o$
- $P(i) = (8-17) \bmod 26 = (26-9) \bmod 26 = 17 \rightarrow r$
- $P(v) = (21-2) \bmod 26 = 19 \rightarrow t$
- $P(h) = (7-0) \bmod 26 = 7 \rightarrow h$
- $P(t) = (19-17) \bmod 26 = 2 \rightarrow c$
- $P(n) = (13-2) \bmod 26 = 11 \rightarrow l$
- $P(a) = (0-0) \bmod 26 = 0 \rightarrow a$
- $P(j) = (9-17) \bmod 26 = (26-8) \bmod 26 = 18 \rightarrow s$
- $P(u) = (20-2) \bmod 26 = 18 \rightarrow s$ $\therefore P = \text{theforthclass}$

Example (3):- Plaintext = she is listening

Key = pascal

Plaintext	=	s	h	e	i	s	l	i	s	t	e	n	i	n	g
Keyword	=	p	a	s	c	a	l	p	a	s	c	a	l	p	a

		s	h	e	i	s	l	i	s	t	e	n	i	n	g
Plaintext values	=	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Key stream	=	15	0	18	2	0	11	15	0	18	2	0	11	15	0
Cipher values	=	7	7	22	10	18	22	23	18	11	6	13	19	2	6

$$C = (P+K) \bmod 26$$

Ciphertext	=	h	h	w	k	s	w	x	s	i	g	n	t	c	g
------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Now: - 1) You asked to decipher the resultant cipher text.

2) Resolve the previous example using table.

3.2 Beaufort Cipher:- Is similar to the previous method but using the *Standard to Reverse* ciphering and deciphering format.

For Ciphering $C = (K-P) \bmod 26$

For Deciphering $P = (K-C) \bmod 26$

في هذه الطريقة ايضا يكون المفتاح عبارة عن كلمة مفتاحية يتم تكرارها بشكل دوري تحت النص الصريح حيث يتم الحل بهذه الطريقة اما باستخدام الجدول المذكور سابقا او باستخدام المعادلات اعلاه. بالنسبة للجدول يتم استحداث جدول بعدد الاسطر يساوي 26 (a-z) وعدد الاعمدة يساوي 26 (a-z) مع ملاحظة ان الاسطر تمثل Key والاعمدة تمثل Plaintext ونبحث في حالة تقاطع key مع plaintext ونتيجة التقاطع (الموقع) يتم حساب المسافة اي بعد هذا التقاطع عن اول عمود من جهة اليسار ثم اخذ هذه المسافة واعادة احتسابها م جهة اليمين ولنفس السطر عند ذلك سوف نحصل على cipher.

If we have the key = F O R T I F I C A T I O N

And the plaintext = D E F E N D T H E E A S T W A L L

plaintext= D E F E N D T H E E A S T W A L L

key= | F O R T I F I C A T I O N | F O R T |

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	J	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

$$C(d) = (3-3) \bmod 26 = 0 \rightarrow a$$

$$C(e) = (0-4) \bmod 26 = (26-4) \bmod 26 = 22 \rightarrow w$$

$$C(p) = (1-15) \bmod 26 = (26-14) \bmod 26 = 12 \rightarrow m$$

$$C(a) = (3-0) \bmod 26 = 3 \rightarrow d$$

$$C(r) = (0-17) \bmod 26 = (26-17) \bmod 26 = 9 \rightarrow j$$

$$C(t) = (1-19) \bmod 26 = (26-18) \bmod 26 = 8 \rightarrow i$$

$$C(m) = (3-12) \bmod 26 = (26-9) \bmod 26 = 17 \rightarrow r$$

$$C(e) = (0-4) \bmod 26 = (26-4) \bmod 26 = 22 \rightarrow w$$

$$C(n) = (1-13) \bmod 26 = (26-12) \bmod 26 = 14 \rightarrow o$$

$$C(t) = (3-19) \bmod 26 = (26-16) \bmod 26 = 10 \rightarrow k$$

$$C(s) = (0-18) \bmod 26 = (26-18) \bmod 26 = 8 \rightarrow i$$

$$C = \text{ynrlhkwkwmdjirwoki}$$

For Deciphering $P = (K-C) \bmod 26$

Ciphertext = y n r l h k w k a w m d j i r w o k i

Keyword =

a	b	d	a	b	d	a	b	d	a	b	d	a	b	d	a	b	d	a
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

$$P(y) = (0-24) \bmod 26 = 26 - 24 = 2 \rightarrow c$$

$$P(n) = (1-13) \bmod 26 = 26-12 = 14 \rightarrow o$$

$$P(r) = (3-17) \bmod 26 = 26-14 = 12 \rightarrow m$$

And so on, finally we get the plaintext = computerdepartments.

Now, you asked to solve the same example but using table:-

ملاحظة:- طرق Vigenere و Beaufort تستخدمان نفس معادلات Standard to standard و Standard to Reverse لكن الفرق في نوع المفتاح المستخدم لانه في طرق Vigenere و Beaufort تكون عناصر المفتاح عبارة عن alphabet بينما في طرق Standard to standard و Standard to Reverse تكون عناصر المفتاح عبارة عن ارقام.

3.3 Running Key Cipher :-

The Running Key cipher has the same internal workings as the [Vigenere cipher](#). The difference lies in how the key is chosen; the Vigenere cipher uses a short key that repeats, whereas the running key cipher uses a long key this means the key does not repeat, making cryptanalysis more difficult.

In this method the length of key must be equal to the length of plaintext and the encryption process is performed using Vigenere cipher and decipher format. If the length of key is greater than the length of plaintext, then all the remaining letters in key must be deleted.

Example :- P= computer Key= omarabda

Plaintext = c o m p u t e r

Keyword = o m a r a b d a

Applying this format for ciphering $C = (P+K) \bmod 26$

So the Ciphertext will be = qamguuhr

Now for deciphering apply this format $P = (C-K) \bmod 26$ to get the plaintext = computer.

ملاحظات:-

⇐ يمكن ان يقال عن Vigenere و Beaufort عبارة عن انظمة دورية تعويضية لانها تستخدم مفتاح بطول معين ويتم تكراره تحت النص الصريح.

⇐ طريق Standard to Standard و Standard to Reverse يكون المفتاح فيها عبارة عن قيمة رقمية واحدة تستخدم لتشفير كل حروف النص الصريح اما في حالة Vigenere و Beaufort و Running Key فان المفتاح هو نص معين ففي كل مرة يتم استخدام حرف معين لتشفير حرف معين من النص الصريح.

⇐ ما هو الاختلاف بين طرق Polyalphabetic Substitution وطريقة Beale Cipher ؟
الجواب:- في Beale Cipher تعطي النص المشفر على شكل قيم رقمية بينما طريقة Polyalphabetic Substitution يكون النص المشفر الناتج عبارة عن حروف.

3.4 One Time Pad (OTP) :-

- Also known as Verman, Use a random key with long as the message.
- In this type of ciphering, the encrypted message can not be broken because the key is a random number and because the key is used only once.
- The message is represented as a binary string (a sequence of 0's and 1's) using coding machine such as ASCII coding.
- The encryption is done by applying Exclusive OR (XOR) operation between message and key with the symbol \oplus is used.

a	b	c= a \oplus b
0	0	0
1	0	1
0	1	1
1	1	0

Example (1):-

Message ='IF'

Then its ASCII code =(1001001 1000110)

Key = (1010110 0110001)

Encryption:

1001001 1000110	plaintext
1010110 0110001	key
0011111 1110110	ciphertext

Decryption:

0011111 1110110	ciphertext
1010110 0110001	key
1001001 1000110	plaintext

Example (2):-

Message = 10010011000110 , Key = 10101100110001

For Cipherring:-

P = 1 0 0 1 0 0 1 1 0 0 0 1 1 0

K = 1 0 1 0 1 1 0 0 1 1 0 0 0 1

C = 0 0 1 1 1 1 1 1 1 1 0 1 1 1

C = 00111111110111

For Decipherring:-

C = 0 0 1 1 1 1 1 1 1 1 0 1 1 1

K = 1 0 1 0 1 1 0 0 1 1 0 0 0 1

P = 1 0 0 1 0 0 1 1 0 0 0 1 1 0

P = 10010011000110

Example (3):-

If you have a cipher text (ZHJ) which is ciphered two times, first by using Affine method with $k_1=9$ and $k_2=3$, and the second method by using One Time Pad (OTP) with key=(ALI); apply all steps required to get the initial plaintext.

Answer:-

Ciphertext= ZHJ	Z =25	H=7	J=9
	11001	00111	01001
KEY= ALI	A=0	L=11	I=8
	00000	01011	01000
Intermediate Ciphertext= Ciphertext \oplus Key	11001	01100	00001
	Z	M	B

Now using Affine Decipher method to get the initial Plaintext

$$P = ((C - K_2) * K_1^{-1}) \bmod 26$$

$$\because K_1 = 9 \quad \therefore K_1^{-1} = 3$$

$$K_2 = 3$$

$$P(Z) = ((25 - 3) * 3) \bmod 26 = 14 \text{ ----- (O)}$$

$$P(M) = ((12 - 3) * 3) \bmod 26 = 1 \text{ ----- (B)}$$

$$P(O) = ((1 - 3) * 3) \bmod 26 = 20 \text{ ----- (U)}$$

\therefore The initial Plaintext= OBU

4. Polygram Cipher:- A Polygram Substitution is a cipher in which a uniform substitution is performed on blocks of letters. Three types of cipher are included in this method and these are:-

4.1 Playfair Cipher

4.2 Hill Cipher

4.1 Playfair Cipher :- Also known as playfair square is a symmetric encryption technique and was the first diagram substitution cipher. This technique encrypts pairs of letters (digraphs) instead of single letter as in the simple substitution cipher and rather more complex Vigenere cipher.

- ❖ Plaintext is divided into 2-letters diagram.
- ❖ Use X to pad the last single letter.
- ❖ Create a 5×5 matrix of letters based on keyword.
- ❖ Fill the matrix with the letters of keyword (without duplicated).
- ❖ Fill rest of matrix with other letters.

Plaintext is encrypted two letters at a time,

1. If a pair is a repeated letter, insert filler like 'X'.
2. If both letters (of plaintext) locate in the same row, replace each with the nearby letters to the right side (wrapping back to start from end).
3. If both letters (of plaintext) locate in the same column, replace each with the letters below it (again wrapping to top from bottom).
4. Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair.

في هذا النوع نحتاج الى كلمة مفتاحية نعتمد عليها في بناء المصفوفة 5×5 تحتوي على 25 حرف ماعدا حرف (z) فانه نادر الظهور في الجمل او الكلمات فاذا ظهر فسوف ياخذ نفس موقع الحرف (i). في البداية ندخل الاحرف من الكلمة المفتاحية الى المصفوفة وبدون تكرار وبعد انهاء الكلمة المفتاحية نقوم بادخال الاحرف غير الموجودة في المصفوفة من الحروف الابجدية الى المصفوفة.

مثلا:-

Keyword :- Iraq is My Country

Alphabet:- a b c d e f g h I j k l m n p q r s t u v w x y z

i/j r a q s

m y c o u

n t b d e

f g h k l

p v w x z

- قبل عملية التشفير يجب ان نتأكد من ان عدد الحروف للنص الصريح يكون زوجي اما اذا كان فردي فيتم اضافة حرف مثلا X في نهاية النص الصريح ليكون عدد حروف النص الصريح زوجي.
- اذا كان هنالك حروف مكررة ضمن نفس المقطع فيتم الفصل بينهما بحرف ليكن مثلا X
- اذا كان حرفين صريحين في نفس الصف (Row) فان التشفير كل حرف سيكون الحرف الذي على يمينه واذا كان في اخر عمود من نفس الصف فالتشفير سيكون اول موقع من نفس السطر لكن من جهة اليسار، اي تحصل حالة التفاف لكن من جهة اليسار. اما في حالة فك الشفرة نأخذ الحرف على يساره بمرتبة واذا كان الاخير نأخذ اول موقع من جهة اليمين للمصفوفة.
- اذ كان الحرفين الصريحين في نفس العمود فان تشفير كل حرف يمثل الحرف الذي يكون الاسفل منه مع مراعاة اذا كان الاخير فانه سوف يأخذ الاعلى موقع من نفس العمود اي تحصل عملية التفاف لكن من نحو الاعلى. اما في حالة فك الشفرة فكل حرف سوف يأخذ الحرف الاعلى منه واذا كان الاول موقع فان عملية التفاف ستكون عكسية اي نحو الاسفل.
- اذا كان الحرفين في اعمدة واسطر مختلفة في هذه الحالة سوف نشكل شكل مربع والحروف الصريحة ستكون في الزوايا وناخذ الاحرف التي تقابلها في نفس الصف وكذلك في نفس الحالة في فك التشفير.

An example of a secret key in the playfair cipher:-

	l	g	d	b	a
	q	m	h	e	c
Secret Key =	u	r	n	i/j	f
	x	v	s	o	k
	z	y	w	t	p

If the plaintext= hello

plaintext=	he	lx	lo	
				∴ Ciphertext= erqzbx
Ciphertext=	ec	qz	bx	

Another example:-

	C	H	A	R	L
	E	S	B	D	F
Secret Key =	G	I/J	K	M	N
	O	P	Q	T	U
	V	W	X	Y	Z

Plaintext= THE SCHEME REALLY WORKS

For Cipherring:-

plaintext=	TH	ES	CH	EM	ER	EA	LX	LY	WO	RK	SX
Ciphertext =	PR	SB	HA	DG	DC	BC	AZ	RZ	VP	AM	BW

∴ Ciphertext = PRSBHADGDCBCAZRZVPAMBW

For Deciphering:-

Ciphertext = PR SB HA DG DC BC AZ RZ VP AM BW

plaintext= TH ES CH EM ER EA LX LY WO RK SX

Example :- keyword = Iraq is my country

Plaintext (1) = SHAHED MOHAMMED

Plaintext (2) = COLLEGE OF EDUCATION

4.2 Hill Cipher :- use matrix multiplication to encrypt a message.

هذه الطريقة تستخدم مبدأ تقطيع النص إلى عدد من المقاطع يمكن أن يكون حرفين أو أكثر حيث تستخدم طريقة ضرب المصفوفات وتقوم هذه الطريقة بتشفير أكثر من حرف في نفس الوقت من خلال تقطيع النص إلى مقاطع حيث يكون الأبعاد كل مقطع يعتمد على أبعاد مصفوفة Keyword فإذا كان حجم Keyword هو (2×2) فإن عملية تقطيع النص الصريح سيكون كل حرفين معاً أي أن عدد الحروف في كل مقطع يساوي اثنين، وفي حالة عدد الحروف في النص الصريح فردي فيجب إضافة X إلى نهاية النص الصريح.

$$\text{keyword} = \begin{bmatrix} K_{11} & K_{12} & K_{13} & \dots & K_{1m} \\ K_{21} & K_{22} & K_{23} & \dots & K_{2m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ K_{m1} & K_{m2} & K_{m3} & \dots & K_{mm} \end{bmatrix}$$

This key matrix must have a multiplicative inverse k^{-1} which is used for Deciphering.

For Ciphering:-

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} \times \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \pmod{26}$$

$$C_1 = (K_{11} \times P_1 + K_{12} \times P_2) \text{ mod } 26$$

$$C_2 = (K_{21} \times P_1 + K_{22} \times P_2) \text{ mod } 26$$

For Deciphering:-

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \underbrace{\begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}}_{k^{-1}} \times \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \text{ mod } 26$$

$$p_1 = (K_{11} \times C_1 + K_{12} \times C_2) \text{ mod } 26$$

$$p_2 = (K_{21} \times C_1 + K_{22} \times C_2) \text{ mod } 26$$

حيث ان مصفوفة k في اعلاه تمثل معكوس المصفوفة الاولى اي k^{-1} ويتم التعامل مع الارقام التسلسلية للحروف الابجدية ويتم تطبيق تلك المعادلات مع كل مقطع من النص الصريح او المشفر.

Example (1) :- if plaintext = COMPUTER

$$\text{and } K = \begin{bmatrix} 5 & 2 \\ 3 & 3 \end{bmatrix}$$

The plaintext should be divided into block of size two depending on key.

C	O	M	P	U	T	E	R
2	14	12	15	20	19	4	17

1- CO

$$C_1 = (K_{11} \times P_1 + K_{12} \times P_2) \text{ mod } 26$$

$$= (5 \times 2 + 2 \times 14) \text{ mod } 26$$

$$= 12 \rightarrow M$$

$$C_2 = (K_{21} \times P_1 + K_{22} \times P_2) \text{ mod } 26$$

$$= (3 \times 2 + 3 \times 14) \bmod 26$$

$$= 22 \rightarrow W$$

2- MP

$$C_1 = (5 \times 12 + 2 \times 15) \bmod 26$$

$$= 12 \rightarrow M$$

$$C_2 = (3 \times 12 + 3 \times 15) \bmod 26$$

$$= 3 \rightarrow D$$

3- UT

$$C_1 = (5 \times 20 + 2 \times 19) \bmod 26$$

$$= 8 \rightarrow I$$

$$C_2 = (3 \times 20 + 3 \times 19) \bmod 26$$

$$= 13 \rightarrow N$$

4- ER

$$C_1 = (5 \times 4 + 2 \times 17) \bmod 26$$

$$= 2 \rightarrow C$$

$$C_2 = (3 \times 4 + 3 \times 17) \bmod 26$$

$$= 11 \rightarrow L$$

$\therefore C = MWMDINCL$

For Deciphering:-

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \underbrace{\begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}}_{k^{-1}} \times \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \bmod 26$$

$$p_1 = (K_{11} \times C_1 + K_{12} \times C_2) \bmod 26$$

$$p_2 = (K_{21} \times C_1 + K_{22} \times C_2) \bmod 26$$

Now we need to compute the inverse of K as shown below:-

- Find d

$$d = (K_{11} \times K_{22} - K_{12} \times K_{21})$$

$$d = (5 \times 3 - 2 \times 3) \quad \therefore \underline{d=9}$$

- Find d^{-1}

هذا الجدول لحساب قيم المعكوس للاعداد الاولية بين (26-1)

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

$$\therefore d = 9 \quad \therefore d^{-1} = 3$$

- Take key matrix and replace the main diagonal with each other while the secondary diagonal only put (-) in front of them (multiplying by -1), as shown below, known as Adj(K):-

$$\text{Adj}(\mathbf{k}) = \begin{bmatrix} 3 & -2 \\ -3 & 5 \end{bmatrix}$$

- $K^{-1} = (d^{-1} \times \text{Adj}(K)) \text{ mod } 26$

$$K^{-1} = d^{-1} \times \begin{bmatrix} 3 & -2 \\ -3 & 5 \end{bmatrix} \text{ mod } 26$$

$$K^{-1} = 3 \times \begin{bmatrix} 3 & -2 \\ -3 & 5 \end{bmatrix} \text{ mod } 26$$

$$K^{-1} = \begin{bmatrix} 9 & -6 \\ -9 & 15 \end{bmatrix} \text{ mod } 26$$

$$K^{-1} = \begin{bmatrix} 9 \text{ mod } 26 & -6 \text{ mod } 26 \\ -9 \text{ mod } 26 & 15 \text{ mod } 26 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 9 & 26 - 6 \\ 26 - 9 & 15 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 9 & 20 \\ 17 & 15 \end{bmatrix}$$

The ciphered should be divided into block of size two depending on key.

M	W	M	D	I	N	C	L
12	22	12	3	8	13	2	11

$$K^{-1}_{11}=9 \quad K^{-1}_{12}=20 \quad K^{-1}_{21}=17 \quad K^{-1}_{22}=15$$

$$P_1 = (K_{11} \times C_1 + K_{12} \times C_2) \text{ mod } 26$$

$$P_2 = (K_{21} \times C_1 + K_{22} \times C_2) \text{ mod } 26$$

1- MW

$$P_1 = (9 \times 12 + 20 \times 22) \text{ mod } 26$$

$$= 2 \rightarrow C$$

$$P_2 = (17 \times 12 + 15 \times 22) \text{ mod } 26$$

$$= 14 \rightarrow O$$

2- MD

$$P_1 = (9 \times 12 + 20 \times 3) \text{ mod } 26$$

$$= 12 \rightarrow M$$

$$P_2 = (17 \times 12 + 15 \times 3) \text{ mod } 26$$

$$= 15 \rightarrow p$$

3- IN

$$P_1 = (9 \times 8 + 20 \times 13) \bmod 26$$

$$= 20 \rightarrow U$$

$$P_2 = (17 \times 8 + 15 \times 13) \bmod 26$$

$$= 19 \rightarrow p$$

4- CL

$$P_1 = (9 \times 2 + 20 \times 11) \bmod 26$$

$$= 4 \rightarrow E$$

$$P_2 = (17 \times 2 + 15 \times 11) \bmod 26$$

$$= 17 \rightarrow R$$

$\therefore P = \text{COMPUTER}$

Note that :- If we have for example

$$-36 \bmod 26$$

$$\rightarrow 26 - 36 = -10$$

$$\rightarrow 26 - 10 = 16$$

Example (2) :- Decipher the word NSUO by using HILL Cipher if key matrix as shown

$$K = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

Now we must find K^{-1}

- Step (1) :- Find d

$$d = (5 \times 3 - 6 \times 2)$$

$$d = (15 - 12)$$

$$d = 3$$

$$\therefore d^{-1} = 3$$

- Step (2) :- Rewrite key matrix in this form with replacing main diagonal with each other and multiply secondary diagonal by (-1)

$$K = \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix}$$

- $K^{-1} = (d^{-1} \times \text{Step}(2)) \text{ mod } 26$

$$K^{-1} = d^{-1} \times \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} \text{ mod } 26$$

$$K^{-1} = 9 \times \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} \text{ mod } 26$$

Chapter Four

❖ Types of Systems :-

1. Depending on Encryption / Decryption Key:-

- **Symmetric Algorithm:-** use one key (which must be secret) for ciphering and deciphering, known as **One Key Algorithm**.

$C = E_k (P)$ for Encryption

$P = D_k (C)$ for Decryption

- **A Symmetric Algorithm:-** use one key for ciphering and another key for deciphering, known as **Public Key Algorithm**.

$C = E_{k1} (P)$ for Encryption

$P = D_{k2} (C)$ for Decryption

K_1 is Public while K_2 is secret.

2. Depending on Cryptographic Techniques:-

The second type of systems that depend on encryption method.

- **Block Ciphers:-**
- **Stream Ciphers:-**

Block Ciphers:-

- Is a type of symmetric encryption which operates on blocks of data (means the same key is used for encryption and decryption).
- Operate on blocks (groups of bits) with fixed-length.
- A block cipher breaks message into fixed sized blocks.
- Takes one block (plaintext) at a time and transform it into another block of the same length using secret key.
- Decryption is performed by applying the reverse transformation to the Ciphertext block using the same key.

- Because the same key is used, each repeated sequence in the Plaintext becomes the same repeated sequence in the Ciphertext, and this could cause security concerns.
 - Popular block ciphers are (**Hill Cipher, Playfair Cipher, DES-Data Encryption Standard-, ECB**) with using the same key.
- ❖ **Hill Cipher:-** In which the size of each block is 2-character, or more, depending on the size of *key matrix*. In these ciphers, the values of each character in the Ciphertext depends on all the values of all characters in the plaintext, and the key is made of $m \times m$ matrix values, which is considered as a single key.
- ❖ **Playfair Cipher:-** In which the size of each block equal to 2-characters only that are encrypted together.
- ❖ **DES (Data Encryption Standard):-** In which each block must be of 64 bits only. This method combines between Substitution and Transposition Cipher, where the type of encryption is called Product Cipher.
- ❖ **ECB:-** This method has been used by German Submarines (العواصات الألمانية) in World War II through the use of dictionary contains many words and for every word there is a certain code that this dictionary will be located on both sides sender and receiver.

Advantages of Block Cipher:-

1. The possibility of parallel processing for more than one block at the same time.
2. Encryption is quick because all the time implemented n of encryption.
3. Error that occurs in a given block does not affect the other.
4. Each block in the Plaintext is encrypted independently.

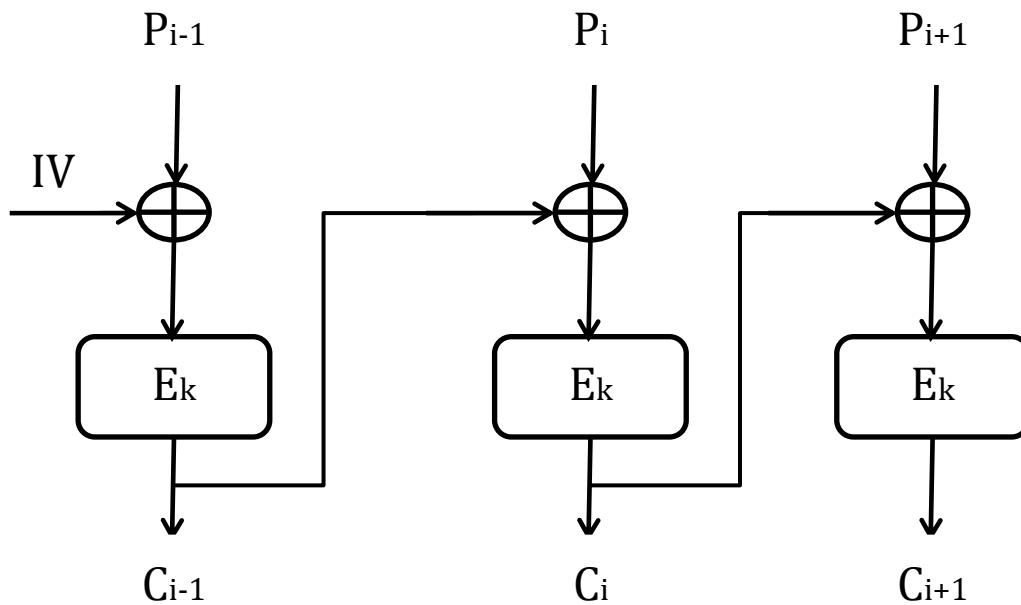
Disadvantages of Block Cipher:-

1. The similar blocks in the plaintext also generate similar blocks in the Ciphertext because all blocks using the same key.
2. Easy addition or deletion can be implemented on blocks.

To solve the problem of block cipher is the development of a new way known as **Cipher Block Chaining Mode (CBC)** in which each block depends on the other by connecting them by (Exclusive OR).

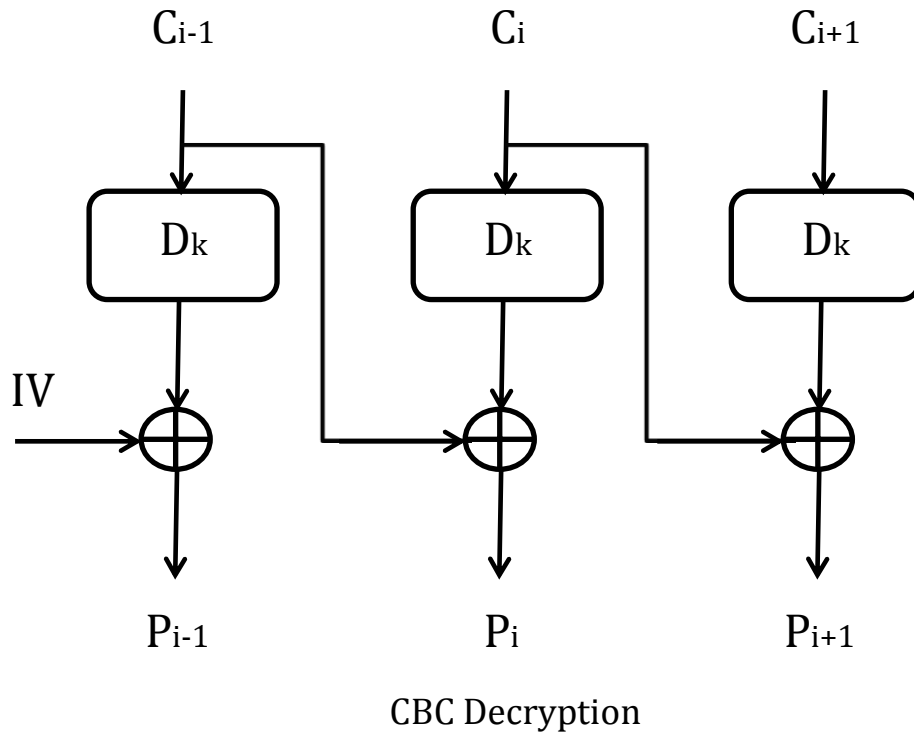
For Cipherring :- $C_i = E_k (P_i \oplus C_{i-1})$ For Deciphering :- $P_i = C_{i-1} \oplus D_k (C_i)$

Where :- C_{i-1} is the previous ciphered block.



CBC Encryption

IV initialization value which is used before first block because no block is found.



Advantages of CBC Ciphers:-

1. There is no possibility of addition or deletion.
2. Ending the state of similar blocks that were give us similar Ciphertext.

Disadvantages of CBC Ciphers:-

An error in a particular block for the rest of the blocks will be affected by that error.

Stream Ciphers:-

- Is the second type of system that depends on cryptographic techniques.
- Stream ciphers belong to the family of symmetric key ciphers.
- Stream ciphers combine Plaintext bits with a cipher bits stream by the use of **XOR** (Exclusive-OR) operation.

For ciphering:- $C_i = E_{k_i}(P_i) = (P_i \oplus K_i)$

For deciphering:- $D_k(C_i) = (C_i \oplus K_i)$
 $= ((P_i \oplus K_i) \oplus K_i) = P_i$

- In this type of ciphering the plaintext is divided into a set of bits that are corresponded with a set of bits for the Ciphertext, and for each bit there is a specific key related to it.

$$P = P_1 \quad P_2 \quad \dots \quad P_n$$

$$K = K_1 \quad K_2 \quad \dots \quad K_n$$

- It is possible to be periodic if reuse the key again after fixed periods, like Vigenere and Beaufort.

Stream Cipher اما ان تكون دورية periodic فيما لو اعيد استخدام المفتاح مرة اخرى بعد فترات ثابتة مثلا بعد 5 characters. مثال ذلك طريقة Vigenere و Beaufort.

- It is possible to be not periodic if the key is used once like Running Key and OTP.

Stream Cipher ممكن ان تكون غير دورية non periodic والتي تستخدم المفتاح مرة واحدة فقط. مثال ذلك Running Key و OTP.

Block Cipher & Stream Cipher Comparison:-

	Block Cipher	Stream Cipher
1	Processing or encoding plaintext is done as a fixed length block one by one. A block for example could be 64 or 128 bits in size.	Processing or encoding plaintext is done bit by bit. The block size here is simply one bit.
2	The same key is used to encrypt each of the blocks.	A different key is used to encrypt each of the bits.
3	Usually more complex and slower in operation.	Usually very simple and much faster.
4	More secure in most cases.	Equally secure if properly designed.
5	The key to the cipher text relationship could be very complicated.	Key is often combined with an initialization vector.
6	An error will affect the transformation of all characters in the same block.	An error in the encryption process affects only that character, because each symbol is separately encoded.
7	Slowness of encryption, the person using a block cipher must wait until entire block of plaintext symbols has been received before starting the encryption process.	Speed of transformation, because each symbol is encrypted without regard for any other plaintext symbols, each symbol is encrypted as soon as it is read, so the time required to encrypt a symbol depends only on the encryption algorithm itself, not on the time it takes to receive more plaintext.

Block Cipher algorithms

Feistel Cipher Structure:-

The inputs to the encryption algorithm are a plain text block of length $2w$ bits and a key k . The plain text block is divided into two halves, L_0 and R_0 . The two halves of the data pass through n rounds of processing and then combine to produce the cipher text block. Each round I has as inputs (L_{i-1}) and (R_{i-1}) , derived from the previous round, as well as a sub-key (k_i) derived from the overall k . In general the sub-keys (k_i) are different from k and from each other and are generated from the key by a sub-key generation algorithms.

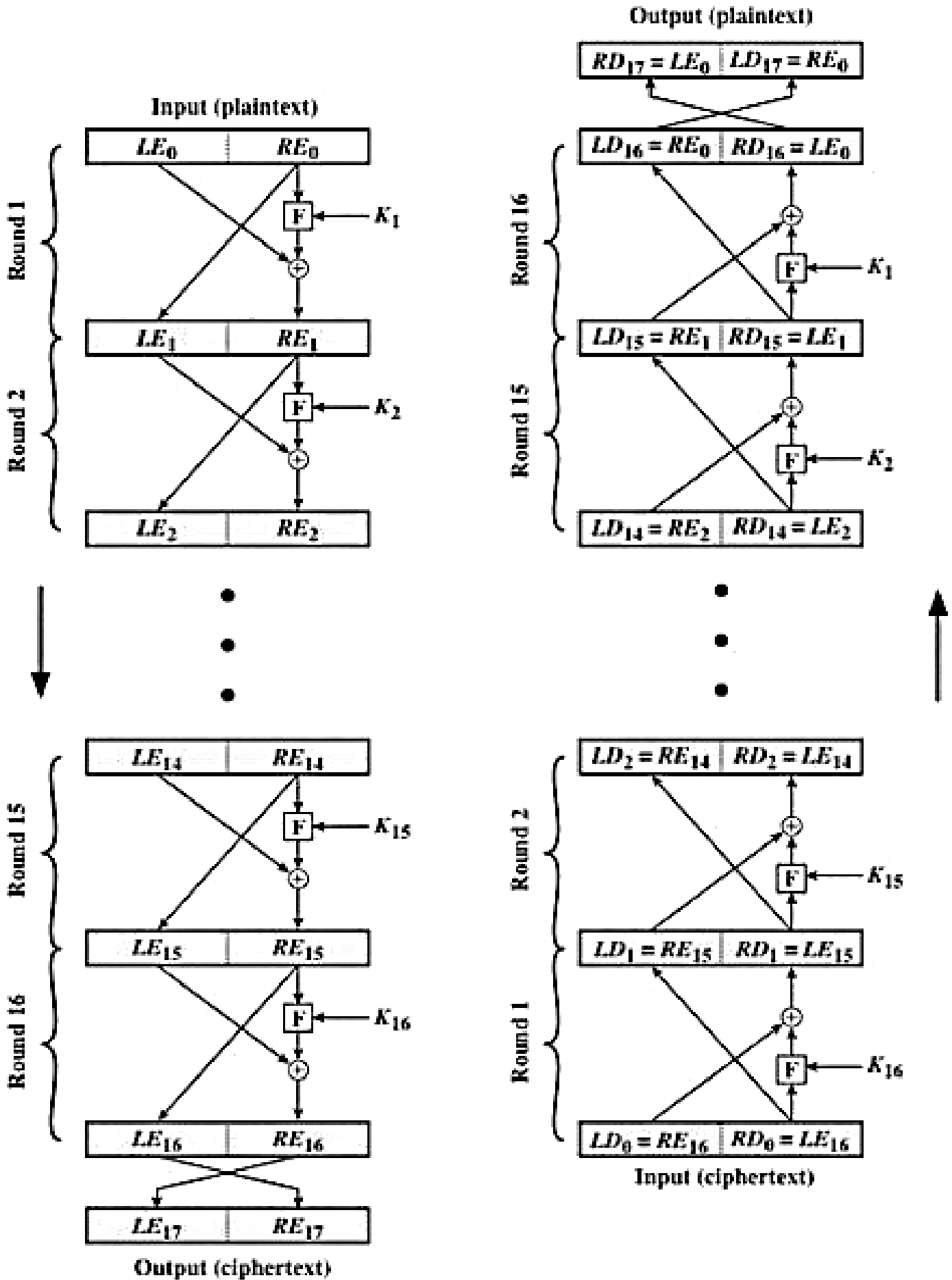
يكون Input لخوارزمية التشفير عبارة عن نص صريح Plaintext بطول $(2W)$ وايضا $key(k)$.
 يتم تجزأة Plaintext الى جزأين (L_0 , R_0) حيث يمر خلال معالجات دورية تسمى Rounds وبالاخير
 تدمج الجزأين مع بعضها للحصول على Ciphertext
 كل Round يكون لها Input هي (L_{i-1} , R_{i-1}) من المرحلة السابقة وايضا يكون هنالك Sub-key يتم
 اشتقاقه من key الاصلي
 بشكل عام تكون قيم Sub-key مختلفة عن key الاصلي وايضا مختلفة عن بعضها حيث يتم توليدها من
 المفتاح الاصلي باستخدام خوارزمية Sub-Key Generation Algorithm .

Feistel Cipher Design Elements:-

- **Block Size:-** Larger block sizes mean greater security but reduced encryption/decryption speed.
- **Key Size:-** Larger key size means greater security but may decrease encryption/decryption speed. The most common key length in modern algorithms is 128 bits.
- **Number of Rounds:-** The summary of the *Feistel* cipher is that a single round shows unsuitable security but that multiple rounds offer increasing security. A typical size is 16 rounds.
- **Sub-Keys Generation Algorithm**
- **Round Function (F)**

There are two other considerations in the design of a *Feistel* Cipher:

1. **Fast software encryption/decryption**
2. **Ease of Analysis.**



- In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two inputs – the key K and R. The function produces the output $f_{R, K}$. Then we XOR the output of the mathematical function with L.

في كل round فإن الجزء الايمن لا تحصل عليه تغييرات ولكن الجزء الايسر يمر خلال عملية تعتمد فيها على قيم الجزء الايمن والمفتاح
 بالبداية يتم تطبيق (round function f) التي تتعامل مع القيمة Sub-key و الجزء الايمن من النص كمدخلات inputs
 المخرجات من هذه الدالة يتم عمل XOR مع الجزء الايسر من النص.

- In real implementation of the **Feistel** Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key *a Sub-key* is derived from the encryption key. This means that each round uses a different key, although all these **Subkeys** are related to the original key.

بهذه الخوارزمية لا يتم التعامل مع key ولكن يتم استخدام خوارزمية Sub-key generation algorithm والتي تقوم بتوليد **Sub-key** من المفتاح الاصلي، لذلك كل round يكون **Sub-key** الخاص بها مختلف عن round الاخرى.

- The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round is the output L of the current round.

خطوة permutation تكون عند نهاية كل round يتم فيها اجراء عملية تبديل جزء L مع جزء R لذلك فان L للدورة التالية تمثل قيمة R للدورة الحالية وكذلك R للدورة التالية تمثل قيمة المخرج L للدورة الحالية.

- Above substitution and permutation steps form a 'round'. The number of rounds is specified by the algorithm design.

عدد ال rounds يعتمد على طريقة تصميم الخوارزمية.

- Once the last round is completed then the two sub blocks, 'R' and 'L' are concatenated in this order to form the cipher-text block.

بعد انتهاء اخر round فإن (L,R) sub blocks سوف يتم دمجها مع بعضها للحصول على Ciphertext.

The difficult part of designing a **Feistel** Cipher is selection of round function 'f'. In order to be unbreakable scheme, this function needs to have several important properties.

Decryption Process

The process of decryption in **Feistel** cipher is almost similar. Instead of starting with a block of plaintext, the cipher-text block is fed into the start of the **Feistel** structure and then the process thereafter is exactly the same as described in the given illustration. The process is said to be almost similar and not exactly same. In the case of decryption, the only difference is that the sub-keys used in encryption are used in the reverse order.

The final swapping of 'L' and 'R' in last step of the **Feistel** Cipher is essential (primary). If these are not swapped then the resulting cipher-text could not be decrypted using the same algorithm.

فك التشفير في هذه الخوارزمية تكون غالبا مشابهة لعملية التشفير ولكن بدلا من البدا بالنص الصريح يتم البدا ب Ciphertext block، الفرق الوحيد هو في استخدام Sub-key حيث يتم استخدامها بشكل معكوس في حالة فك التشفير.

ملاحظة:- خطوة التبدل تعتبر شيء اساسي ومهم وفي حالة عدم تنفيذها فان الناتج المشفر (Resultant Ciphertext) لا يمكن ان يعمل له Decipher باستخدام نفس الخوارزمية.

Number of Rounds

The number of rounds used in a **Feistel** Cipher depends on desired security from the system. More number of rounds provides more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes.

Encryption	Decryption
<ul style="list-style-type: none"> Split plaintext block into left and right halves:- Plaintext = (L₀, R₀) 	<ul style="list-style-type: none"> Ciphertext = (L_n, R_n)
<ul style="list-style-type: none"> For each round $i=1,2,\dots,n$ compute:- $L_i=R_{i-1}$ $R_i=L_{i-1} \oplus f(R_{i-1}, K_i)$ where f is round function and K_i is a subkey 	<ul style="list-style-type: none"> For each round $i=n,n-1,\dots,1$ compute:- $R_{i-1} = L_i$ $L_{i-1} = R_i \oplus f(R_{i-1}, K_i)$ where f is round function and K_i is a subkey
<ul style="list-style-type: none"> Ciphertext = (L_n, R_n) 	<ul style="list-style-type: none"> Plaintext = (L₀, R₀)

Data Encryption Standard (DES):-

The most widely used encryption scheme is defined in the data encryption standard (DES) adopted in 1977 by US Federal Standards, which encrypts 64-bit data using 56-bit key.

The algorithm involves carrying out combinations, substitutions and permutations between the text to be encrypted and the key, while making sure the operations can be performed in both directions (for decryption). The combination of substitutions and permutations is called a **product cipher**.

Overview:-

1. Symmetric Algorithm
2. Block Cipher
3. Uses a combination of Substitution and Transpositions (Permutations).
4. Goes through 16 Cycles (iterations).
5. The overall processing at each cycle can be summarized in the following formulas:-
$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$
6. Plaintext is organized into 64-bit blocks.
7. Uses a 56-bit Key.
8. The complex function involves both permutation and substitution operations. The substitution operation represented as table called "S-Boxes", simply maps each combination of 48 inputs bits into a particular 32-bit pattern.

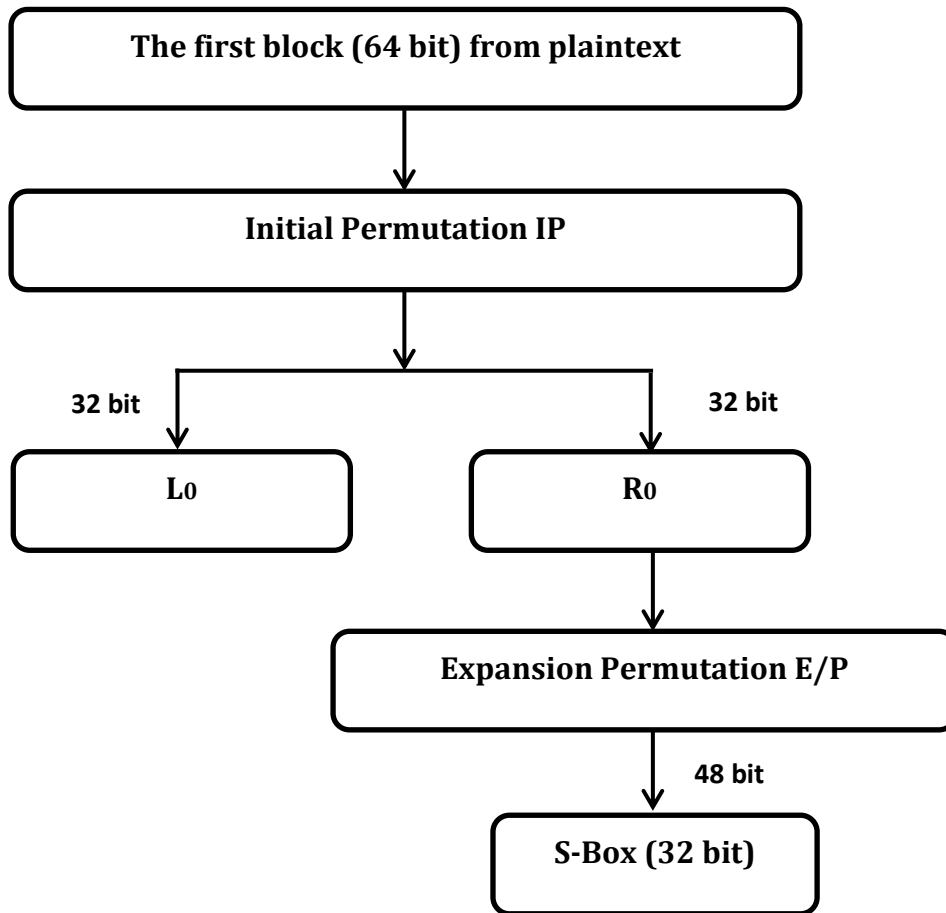
DES Steps:-

1. Initial permutation (IP) on input text (64-bit).
2. Split into right and left halves (32-bit).
3. Take right half and permute it (Expansion Permutation E/P).
4. Work on key (shift) 56-bit, then permute key (48-bits).
5. XOR resulting key with right half... result in 32-bit (S-BOX).
6. Permute result
7. XOR result with left half
8. End of cycle.

Key Transformation:-

1. Starts with 64-bit.
2. Drop every eighth bit = 56 bits (actually 64 bits, 8 bits parity check).
3. Split into two 28-bits halves.
4. Shift each key to the left (a number of bits).
5. Paste both halves.
6. 48-bit key is then permuted.

Plaintext:-



Initial Permutation IP:- is the first step of the data computation.

First the following matrix shows the plaintext represented as blocks of 8-bits, and these numbers from 1-64 represent the number of bit in the plaintext.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Firstly, each bit of a block is subject to initial permutation, which can be represented by the following initial permutation (IP) table:-

IP	<u>58</u>	<u>50</u>	<u>42</u>	<u>34</u>	<u>26</u>	<u>18</u>	<u>10</u>	<u>2</u>
	<u>60</u>	<u>52</u>	<u>44</u>	<u>36</u>	<u>28</u>	<u>20</u>	<u>12</u>	<u>4</u>
	<u>62</u>	<u>54</u>	<u>46</u>	<u>38</u>	<u>30</u>	<u>22</u>	<u>14</u>	<u>6</u>
	<u>64</u>	<u>56</u>	<u>48</u>	<u>40</u>	<u>32</u>	<u>24</u>	<u>16</u>	<u>8</u>
	<u>57</u>	<u>49</u>	<u>41</u>	<u>33</u>	<u>25</u>	<u>17</u>	<u>9</u>	<u>1</u>
	<u>59</u>	<u>51</u>	<u>43</u>	<u>35</u>	<u>27</u>	<u>19</u>	<u>11</u>	<u>3</u>
	<u>61</u>	<u>53</u>	<u>45</u>	<u>37</u>	<u>29</u>	<u>21</u>	<u>13</u>	<u>5</u>
	<u>63</u>	<u>55</u>	<u>47</u>	<u>39</u>	<u>31</u>	<u>23</u>	<u>15</u>	<u>7</u>

This permutation table shows, when reading the table from left to right then from top to bottom, that the 58th bit of the 64-bit block is in first position, the 50th in second position and so on.

Division into 32-bit blocks :- Once the initial permutation is completed, the 64-bit block is divided into two 32-bit blocks, respectively denoted **L** and **R** (for left and right). The initial status of these two blocks is denoted **L₀** and **R₀**:

L₀	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8

R₀	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

It is interesting to note that **L₀** contains all bits having an **even position** in the initial message, whereas **R₀** contains bits with an **odd position**.

Rounds:-

The **L_n** and **R_n** blocks are subject to a set of repeated transformations called **rounds**, shown in this diagram, and the details of which are given below:

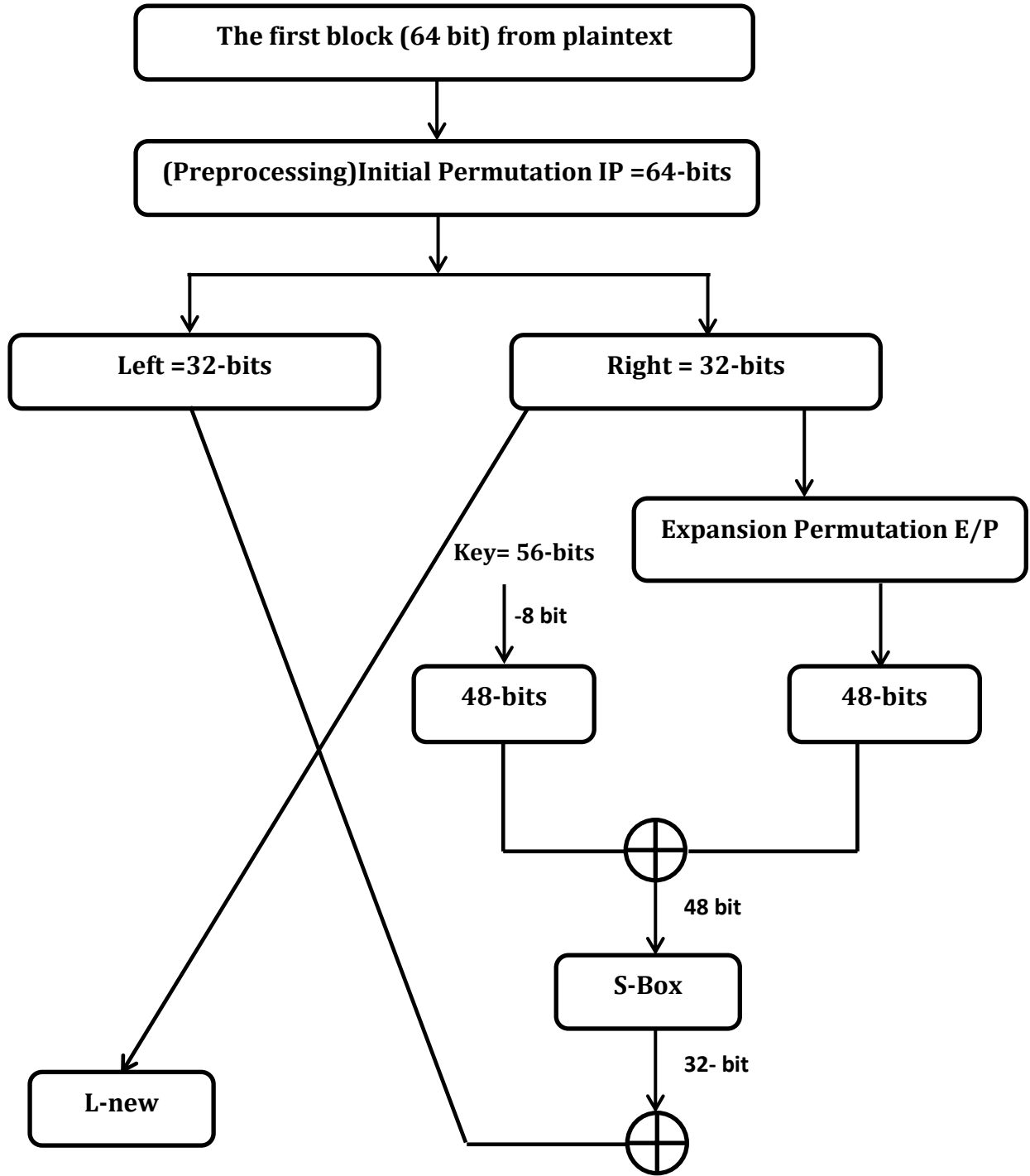
DES Round Structure:-

1. Uses two 32-bit L and R halves.
2. As for any **Feistel** Cipher can describe as:-

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

3. F takes 32-bit R half and 48-bit Subkey:-
 - Expand R to 48-bits using Expansion Permutation E/P.
 - Adds to Subkey using XOR.
 - Passes through 8 S-boxes to get 32-bit result.
 - Finally permutes using 32-bit permutation.



Expansion function

The 32 bits of the R_0 block are expanded to 48 bits thanks to a table called an *expansion table* (denoted E), in which the 48 bits are mixed together and 16 of them are duplicated:-

(Note that the numbers from 1 to 32 represent the number of blocks in R_0 half).

R_0	1	2	3	4
	5	6	7	8
	9	10	11	12
	13	14	15	16
	17	18	19	20
	21	22	23	24
	25	26	27	28
	29	30	31	32

Expansion is done by adding the last column (of the above matrix) and put it before the first column with a note that is the last value in the column is placed at the beginning of the column, while the rest of the column values are shifted down one position.

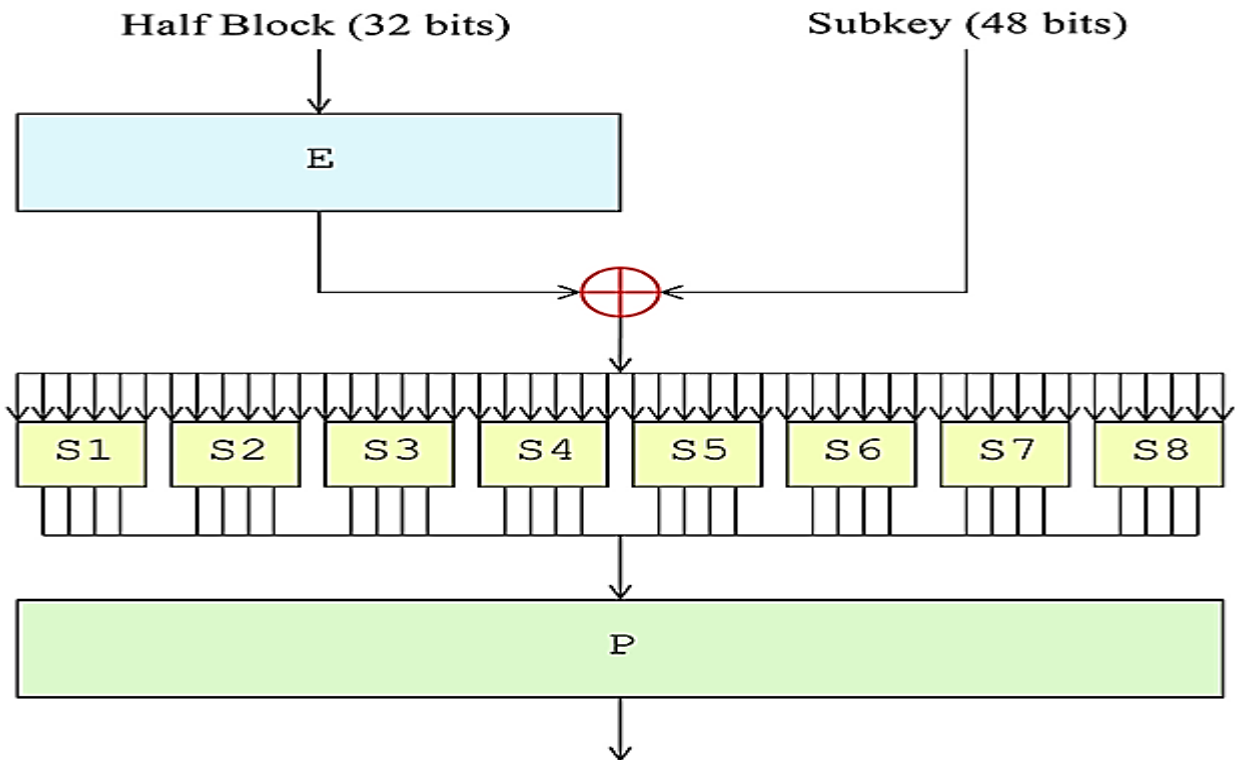
E	32	1	2	3	4	5
	4	5	6	7	8	9
	8	9	10	11	12	13
	12	13	14	15	16	17
	16	17	18	19	20	21
	20	21	22	23	24	25
	24	25	26	27	28	29
	28	29	30	31	32	1

As such, the last bit of R_0 (that is, the 7th bit of the original block) becomes the first, the first becomes the second, etc.

In addition, the bits 1, 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, 24, 25, 28 and 29 of R_0 (respectively 57, 33, 25, 1, 59, 35, 27, 3, 61, 37, 29, 5, 63, 39, 31 and 7 of the original block) are duplicated and scattered in the table.

Exclusive OR with the key:-

The resulting 48-bit table is called R'_0 or $E[R_0]$. The DES algorithm then *exclusive ORs* the first key K_1 with $E[R_0]$. The result of this *exclusive OR* is a 48-bit table we will call R_0 out of convenience (it is not the starting R_0 !).



Substitution function:-

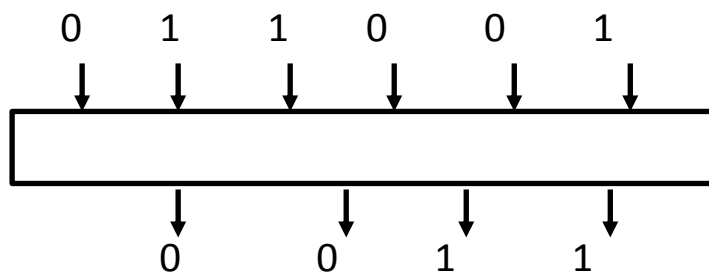
R_0 is then divided into 8 6-bit blocks, denoted R_{0i} . Each of these blocks is processed by **selection functions** (sometimes called **Substitution Boxes** or **Compression Functions S-Boxes**), generally denoted S_i . The s-boxes are substitution based on table of 4 rows and 16 columns. Suppose the block B_j is the six bits $(b_1, b_2, b_3, b_4, b_5, b_6)$. Bits b_1 and b_6 taken together, from a two-bit binary number $b_1 b_6$, having a decimal value from 0 to 3, call this value r .

Bits b_2, b_3, b_4 and b_5 taken together from a four-bit binary number $b_2 b_3 b_4 b_5$ having a decimal value from 0 to 15 call the value c . The substitution from the S-Boxes transform each 6-bit block B_j into the 4-bit result shown in row r , column c of section S_j of table.

Example:- Assume S_7 in a binary is 010011

Then $r = 01 = 1$ $c = 1001 = 9$

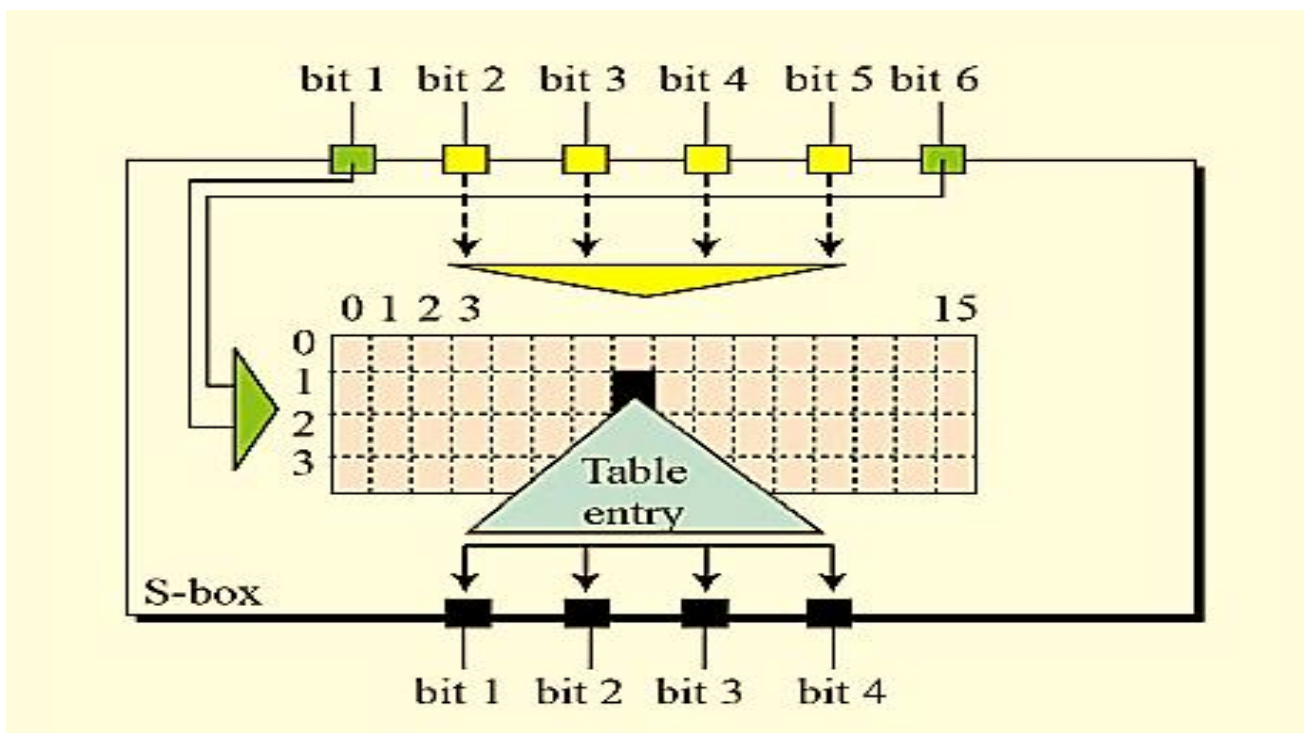
The transformation of block B_7 is found in row 1 and column $= (1,9) = 3 = 0011$



The first and last bits of each R_{0i} determine (in binary value) the line of the selection function; the other bits (respectively 2, 3, 4 and 5) determine the columns. As the selection of the line is based on two bits, there are 4 possibilities (0, 1, 2, 3). As the selection of the column is based on 4 bits, there are 16 possibilities (0 to 15). Thanks to this information, the selection function "selects" a ciphered value of 4 bits.

Here is the first substitution function, represented by a 4-by-16 table:-

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13



Let R_{01} equal 101110 . The first and last bits give 10 , that is, 2 in binary value. The bits 2, 3, 4 and 5 give 0111 , or 7 in binary value. The result of the selection function is therefore the value located on line no. 2, in column no. 7. It is the value 11 , or 111 binary.

Each of the 8 6-bit blocks is passed through the corresponding selection function, which gives an output of 8 values with 4 bits each.

Here are the other selection functions:-

S_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
1	03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
2	00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
3	13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09

S_3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

S_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	07	13	14	03	00	06	09	10	01	02	08	05	11	12	04	15
1	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
2	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
3	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
1	14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
2	04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
3	11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03

S_6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	01	10	15	09	02	06	08	00	13	03	04	14	07	05	11
1	10	15	04	02	07	12	09	05	06	01	13	14	00	11	03	08
2	09	14	15	05	02	08	12	03	07	00	04	10	01	13	11	06
3	04	03	02	12	09	05	15	10	11	14	01	07	06	00	08	13

S_7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	04	11	02	14	15	00	08	13	03	12	09	07	05	10	06	01
1	13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
2	01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
3	06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12

S_8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	02	08	04	06	15	11	01	10	09	03	14	05	00	12	07
1	01	15	13	08	10	03	07	04	12	05	06	11	00	14	09	02
2	07	11	04	01	09	12	14	02	00	06	10	13	15	03	05	08
3	02	01	14	07	04	10	08	13	15	12	09	00	03	05	06	11

Each 6-bit block is therefore substituted in a 4-bit block. These bits are combined to form a 32-bit block.

Permutation:-

The obtained 32-bit block is then subject to a permutation **P** here is the table:-

P	16	7	20	21	29	12	28	17
	1	15	23	26	5	18	31	10
	2	8	24	14	32	27	3	9
	19	13	30	6	22	11	4	25

Exclusive OR:-

All of these results output from **P** are subject to an *Exclusive OR* with the starting L_0 (as shown on the first diagram) to give R_1 , whereas the initial R_0 gives L_1 .

Iteration:- All of the previous steps (*rounds*) are repeated 16 times.

Inverse initial permutation:-

At the end of the iterations, the two blocks L_{16} and R_{16} are re-joined, then subject to inverse initial permutation:

IP-1	40	8	48	16	56	24	64	32
	39	7	47	15	55	23	63	31
	38	6	46	14	54	22	62	30
	37	5	45	13	53	21	61	29
	36	4	44	12	52	20	60	28
	35	3	43	11	51	19	59	27
	34	2	42	10	50	18	58	26
	33	1	41	9	49	17	57	25

The output result is a 64-bit Ciphertext

Example:- If the plaintext = mohammed

To find the initial permutation:-

a b c d e f g h i j k l m n o p q r s t u v w x y z
 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Using this to convert to binary form :- 128, 64, 32, 16, 8, 4, 2, 1

m = 12 = 00001100
o = 14 = 00001110
h = 7 = 00000111
a = 0 = 00000000
m = 12 = 00001100
m = 12 = 00001100
e = 4 = 00000100
d = 3 = 00000011

1/0	2/0	3/0	4/0	5/1	6/1	7/0	8/0
9/0	10/0	11/0	12/0	13/1	14/1	15/1	16/0
17/0	18/0	19/0	20/0	21/0	22/1	23/1	24/1
25/0	26/0	27/0	28/0	29/0	30/0	31/0	32/0
33/0	34/0	35/0	36/0	37/1	38/1	39/0	40/0
41/0	42/0	43/0	44/0	45/1	46/1	47/0	48/0
49/0	50/0	51/0	52/0	53/0	54/1	55/0	56/0
57/0	58/0	59/0	60/0	61/0	62/0	63/1	64/1

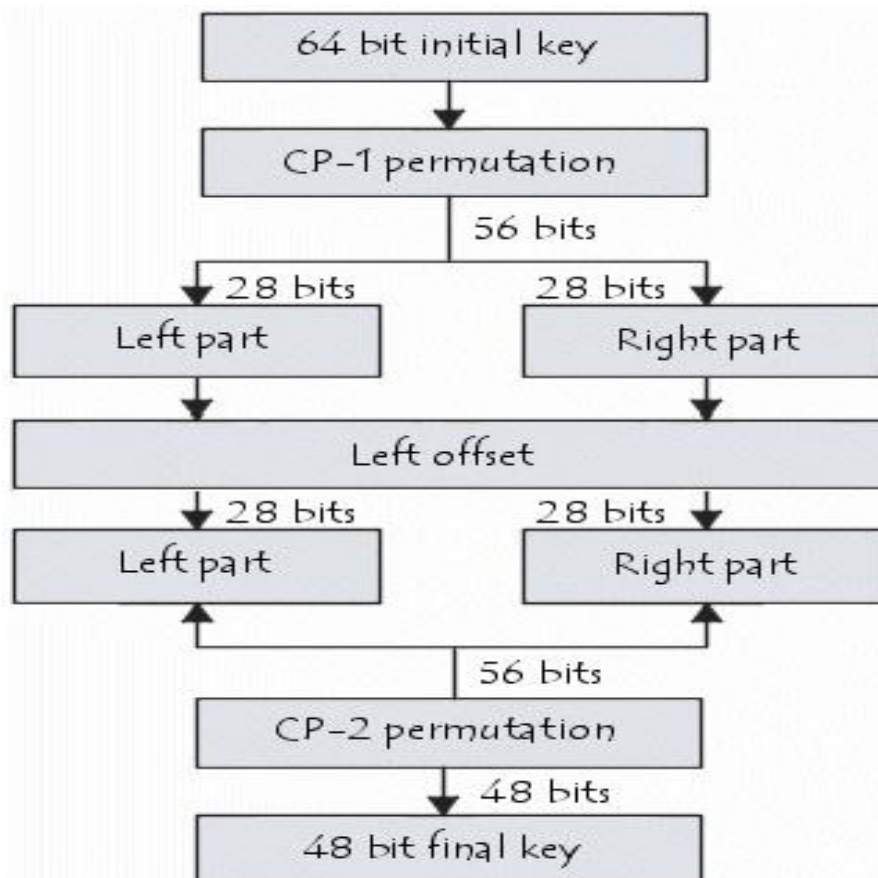
IP	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8
	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

IP	0	0	0	0	0	0	0	00000000
	0	0	0	0	0	0	0	00000000
	0	1	1	1	0	1	1	01110111
	1	0	0	0	0	1	0	10000100
	0	0	0	0	0	0	0	00000000
	0	0	0	0	0	0	0	00000000
	0	0	1	1	0	0	1	00110011
	1	0	0	0	0	1	1	10000110

Generation of keys:-

Given that the DES algorithm presented above is public, security is based on the complexity of encryption keys.

The algorithm below shows how to obtain, from a 64-bit key (made of any 64 alphanumeric characters), 8 different 48-bit keys each used in the DES algorithm:



Firstly, the key's parity bits are eliminated so as to obtain a key with a useful length of 56 bits.

The first step is a permutation denoted **PC-1** (permutation choice-1) whose table is presented below:-

PC-1	57	49	41	33	25	17	9	1	58	50	42	34	26	18
	10	2	59	51	43	35	27	19	11	3	60	52	44	36
	63	55	47	39	31	23	15	7	62	54	46	38	30	22
	14	6	61	53	45	37	29	21	13	5	28	20	12	4

This table may be written in the form of two tables **L_i** and **R_i** (for left and right) each made of 28 bits:-

L_i /C₀	57	49	41	33	25	17	9
	1	58	50	42	34	26	18
	10	2	59	51	43	35	27
	19	11	3	60	52	44	36

R_i /D₀	63	55	47	39	31	23	15
	7	62	54	46	38	30	22
	14	6	61	53	45	37	29
	21	13	5	28	20	12	4

The result of this first permutation is denoted **L₀** and **R₀**.

These two blocks are then rotated to the left; such that the bits in second position take the first position, those in third position take the second, etc. the bits in first position move to last position.

The two 28-bit blocks are then grouped into one 56-bit block. This passes through a permutation, denoted **PC-2 (permutation choice-2)**, giving a 48-bit block as output, representing the key K_i .

Left Shift (LS):-

Number of rounds	Shifting amount (Offset)
1, 2, 9, 16	1
3, 4, 5, 6, 7, 8, 10	2
15, 14, 13, 12, 11	2

PC-2	14	17	11	24	1	5
	3	28	15	6	21	10
	23	19	12	4	26	8
	16	7	27	20	13	2
	41	52	31	37	47	55
	30	40	51	45	33	48
	44	49	39	56	34	53
	46	42	50	36	29	32

Repeating the algorithm makes it possible to give the 16 keys K_1 to K_{16} used in the DES algorithm.

Example:- Generate the first and second DES sub keys given that the output of the permuted choice1

01111111 10101010 01010101 10001111 00011111 01000000 00000001
00001011

1/0	2/1	3/1	4/1	5/1	6/1	7/1	8/1
9/1	10/0	11/1	12/0	13/1	14/0	15/1	16/0
17/0	18/1	19/0	20/1	21/0	22/1	23/0	24/1
25/1	26/0	27/0	28/0	29/1	30/1	31/1	32/1
33/0	34/0	35/0	36/1	37/1	38/1	39/1	40/1
41/0	42/1	43/0	44/0	45/0	46/0	47/0	48/0
49/0	50/0	51/0	52/0	53/0	54/0	55/0	56/1
57/0	58/0	59/0	60/0	61/1	62/0	63/1	64/1

C ₀	57/0	49/0	41/0	33/0	25/1	17/0	9/1
	1/0	58/0	50/0	42/1	34/1	26/0	18/1
	10/0	2/1	59/0	51/0	43/0	35/0	27/0
	19/0	11/1	3/1	60/0	52/0	44/0	36/1
D ₀	63/1	55/0	47/0	39/1	31/1	23/0	15/1
	7/1	62/0	54/0	46/0	38/1	30/1	22/1
	14/0	6/1	61/1	53/0	45/0	37/1	29/1
	21/0	13/1	5/1	28/0	1/20	12/0	4/1

$C_0 = 0000101 \ 0001101 \ 0100000 \ 0110001$

$D_0 = 1001101 \ 1000111 \ 0110011 \ 0110101$

Shift left one position

$C_1 = 000101 \ 0001101 \ 0100000 \ 01100010$

$D_1 = 001101 \ 1000111 \ 0110011 \ 01101011$

DES Example

Example:- If the plaintext = mohammed

With key = 01111111 10101010 01010101 10001111 00011111 01000000
00000001 00001011

a b c d e f g h i j k l m n o p q r s t u v w x y z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

m = 12 = 00001100
o = 14 = 00001110
h = 7 = 00000111
a = 0 = 00000000
m = 12 = 00001100
m = 12 = 00001100
e = 4 = 00000100
d = 3 = 00000011

1/0	2/0	3/0	4/0	5/1	6/1	7/0	8/0
9/0	10/0	11/0	12/0	13/1	14/1	15/1	16/0
17/0	18/0	19/0	20/0	21/0	22/1	23/1	24/1
25/0	26/0	27/0	28/0	29/0	30/0	31/0	32/0
33/0	34/0	35/0	36/0	37/1	38/1	39/0	40/0
41/0	42/0	43/0	44/0	45/1	46/1	47/0	48/0
49/0	50/0	51/0	52/0	53/0	54/1	55/0	56/0
57/0	58/0	59/0	60/0	61/0	62/0	63/1	64/1

Initial permutation:-

IP	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8
	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

IP	0	0	0	0	0	0	0	L ₀
	0	0	0	0	0	0	0	
	0	1	1	1	0	1	1	
	1	0	0	0	0	1	0	
	0	0	0	0	0	0	0	R ₀
	0	0	0	0	0	0	0	
	0	0	1	1	0	0	1	
	1	0	0	0	0	1	1	

Division into 32-bit blocks :-

L ₀ =	0	0	1	0	R ₀ =	1/0	2/0	3/1	4/0
	0	0	1	0		5/0	6/0	7/1	8/1
	0	0	1	1		9/0	10/0	11/0	12/1
	0	0	0	0		13/0	14/0	15/0	16/0
	0	0	1	0		17/0	18/0	19/1	20/0
	0	0	1	0		21/0	22/0	23/1	24/0
	0	0	1	0		25/0	26/0	27/0	28/0
	0	0	0	1		29/0	30/0	31/0	32/1

Expansion to the right half	32/1	1/0	2/0	3/1	4/0	5/0
	4/0	5/0	6/0	7/1	8/1	9/0
	8/1	9/0	10/0	11/0	12/1	13/0
	12/1	13/0	14/0	15/0	16/0	17/0
	16/0	17/0	18/0	19/1	20/0	21/0
	20/0	21/0	22/0	23/1	24/0	25/0
	24/0	25/0	26/0	27/0	28/0	29/0
	28/0	29/0	30/0	31/0	32/1	1/0

Exclusive OR with the key:-

First we must do some processing on key before XOR with the previous result:-

Starts with key =64-bit.....,

1/0	2/1	3/1	4/1	5/1	6/1	7/1	8/1
9/1	10/0	11/1	12/0	13/1	14/0	15/1	16/0
17/0	18/1	19/0	20/1	21/0	22/1	23/0	24/1
25/1	26/0	27/0	28/0	29/1	30/1	31/1	32/1
33/0	34/0	35/0	36/1	37/1	38/1	39/1	40/1
41/0	42/1	43/0	44/0	45/0	46/0	47/0	48/0
49/0	50/0	51/0	52/0	53/0	54/0	55/0	56/1
57/0	58/0	59/0	60/0	61/1	62/0	63/1	64/1

Paste both halves.....48-bit key is then permuted.

The first step is a permutation denoted PC-1 (permutation choice-1) whose table is presented below:-

Drop every eighth bit = 56 bits (actually 64 bits, 8 bits parity check).....

PC-1	57/0	49/0	41/0	33/0	25/1	17/0	9/1	1/0	58/0	50/0	42/1	34/0	26/0	18/1
	10/0	2/1	59/0	51/0	43/0	35/0	27/0	19/0	11/1	3/1	60/0	52/0	44/0	36/1
	63/1	55/0	47/0	39/1	31/1	23/0	15/1	7/1	62/0	54/0	46/0	38/1	30/1	22/1
	14/0	6/1	61/1	53/0	45/0	37/1	29/1	21/0	13/1	5/1	28/0	20/1	12/0	4/1

Split into two 28-bits halves.....

L_i / C_0	57/0	49/0	41/0	33/0	25/1	17/0	9/1
	1/0	58/0	50/0	42/1	34/0	26/0	18/1
	10/0	2/1	59/0	51/0	43/0	35/0	27/0
	19/0	11/1	3/1	60/0	52/0	44/0	36/1

R_i / D_0	63/1	55/0	47/0	39/1	31/1	23/0	15/1
	7/1	62/0	54/0	46/0	38/1	30/1	22/1
	14/0	6/1	61/1	53/0	45/0	37/1	29/1
	21/0	13/1	5/1	28/0	20/1	12/0	4/1

$L_i / C_0 = 0000101\ 0001001\ 0100000\ 0110001$

$R_i / D_0 = 1001101\ 1000111\ 0110011\ 0110101$

Shift each key to the left (a number of bits) here the shifting depend on the round number, and since we are in round one, so these bits must shifting one bit only as shown below:-

$L_1 / C_1 = 000101\ 0001001\ 0100000\ 01100010$

$R_1 / D_1 = 001101\ 1000111\ 0110011\ 01101011$

The two blocks are then grouped together to get 56-bits as shown:-

L_1 / C_1	1/0	2/0	3/0	4/1	5/0	6/1	7/0
	8/0	9/0	10/1	11/0	12/0	13/1	14/0
	15/1	16/0	17/0	18/0	19/0	20/0	21/0
	22/1	23/1	24/0	25/0	26/0	27/1	28/0
R_1 / D_1	29/0	30/0	31/1	32/1	33/0	34/1	35/1
	36/0	37/0	38/0	39/1	40/1	41/1	42/0
	43/1	44/1	45/0	46/0	47/1	48/1	49/0
	50/1	51/1	52/0	53/1	54/0	55/1	56/1

This passes through a permutation, denoted **PC-2 (permutation choice-2)**, giving a 48-bit block as output, representing the key K_i

PC-2	14	17	11	24	1	5
	3	28	15	6	21	10
	23	19	12	4	26	8
	16	7	27	20	13	2
	41	52	31	37	47	55
	30	40	51	45	33	48
	44	49	39	56	34	53
	46	42	50	36	29	32



PC-2	0	0	0	0	0	0
	0	0	1	1	0	1
	1	0	0	1	0	0
	0	0	1	0	1	0
	1	0	1	0	1	1
	0	1	1	0	0	1
	1	0	1	1	1	1
	0	0	1	0	0	1

The output from the previous step represents the key in round₁ which is XOR_{ed} with the R₁ after it is expanded as shown below:-

1	0	0	1	0	0	XOR	0	0	0	0	0	0
0	0	0	1	1	0		0	0	1	1	0	1
1	0	0	0	1	0		1	0	0	1	0	0
1	0	0	0	0	0		0	0	1	0	1	0
0	0	0	1	0	0		1	0	1	0	1	1
0	0	0	1	0	0		0	1	1	0	0	1
0	0	0	0	0	0		1	0	1	1	1	1
0	0	0	0	1	0		0	0	1	0	0	1
Expansion to the right half						PC-2						

The resulted XOR operation=

1	0	0	1	0	0	→ S ₁ = 100100
0	0	1	0	1	1	→ S ₂ = 001011
1	0	0	1	1	0	→ S ₃ = 000110
1	0	1	0	1	0	→ S ₄ = 101010
1	0	1	1	1	1	→ S ₅ = 101111
0	1	1	1	0	1	→ S ₆ = 011101
1	0	1	1	1	1	→ S ₇ = 101111
0	0	1	0	1	1	→ S ₈ = 001011

This will enter to S-Boxes.

S ₁ :-	1	0	0	1	0	0	Row=10 = 2	Col. =0010 = 2
-------------------	---	---	---	---	---	---	------------	----------------

S ₁	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

∴ S₁=14 = 1110

S_2 :-	0	0	1	0	1	1	Row=01 = 1	Col. =0101 = 5
----------	---	---	---	---	---	---	------------	----------------

S_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
1	03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
2	00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
3	13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09

$\therefore S_2=2=0010$

S_3 :-	0	0	0	1	1	0	Row=00 = 0	Col. =0011 = 3
----------	---	---	---	---	---	---	------------	----------------

S_3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

$\therefore S_3=14=1110$

S_4 :-	1	0	1	0	1	0	Row=10 = 2	Col. =0101 = 5
----------	---	---	---	---	---	---	------------	----------------

S_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	07	13	14	03	00	06	09	10	01	02	08	05	11	12	04	15
1	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
2	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
3	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

$\therefore S_4=11=1011$

S ₅ :-	1	0	1	1	1	1	Row=11 = 3	Col. =0111 = 7
-------------------	---	---	---	---	---	---	------------	----------------

S ₅	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
1	14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
2	04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
3	11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03

∴ S₅=13=1101

S ₆ :-	0	1	1	1	0	1	Row=01 = 1	Col. =1110 =14
-------------------	---	---	---	---	---	---	------------	----------------

S ₆	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	01	10	15	09	02	06	08	00	13	03	04	14	07	05	11
1	10	15	04	02	07	12	09	05	06	01	13	14	00	11	03	08
2	09	14	15	05	02	08	12	03	07	00	04	10	01	13	11	06
3	04	03	02	12	09	05	15	10	11	14	01	07	06	00	08	13

∴ S₆=3=0011

S ₇ :-	1	0	1	1	1	1	Row=11 = 3	Col. =0111 = 7
-------------------	---	---	---	---	---	---	------------	----------------

S ₇	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	04	11	02	14	15	00	08	13	03	12	09	07	05	10	06	01
1	13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
2	01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
3	06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12

∴ S₇= 7 = 0111

S₈ :-	0	0	1	0	1	1	Row=01 = 1	Col. =0101 = 5
-------------------------	---	---	---	---	---	---	-------------------	-----------------------

S₈	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	02	08	04	06	15	11	01	10	09	03	14	05	00	12	07
1	01	15	13	08	10	03	07	04	12	05	06	11	00	14	09	02
2	07	11	04	01	09	12	14	02	00	06	10	13	15	03	05	08
3	02	01	14	07	04	10	08	13	15	12	09	00	03	05	06	11

∴ S₈ = 3 = 0011

S₁= 1110 S₂= 0010 S₃=1110 S₄=1011
 S₅=1101 S₆=0011 S₇= 0111 S₈= 0011

1/1 2/1 3/1 4/0

5/0 6/0 7/1 8/0

9/1 10/1 11/1 12/0

13/1 14/0 15/1 16/1

17/1 18/1 19/0 20/1

21/0 22/0 23/1 24/1

25/0 26/1 27/1 28/1

29/0 30/0 31/1 32/1

Permutation:-

P	16	7	20	21	29	12	28	17
	1	15	23	26	5	18	31	10
	2	8	24	14	32	27	3	9
	19	13	30	6	22	11	4	25

1	1	1	0	0	0	1	1	P
1	1	1	1	0	1	1	1	
1	0	1	0	1	1	1	1	
0	1	0	0	0	1	0	0	

Exclusive OR:-

All of these results output from **P** are subject to an *Exclusive OR* with the starting **L₀** (as shown on the first diagram) to give **R₁**

0	0	0	0	0	0	0	0	L₀
0	0	0	0	0	0	0	0	
0	1	1	1	0	1	1	1	
1	0	0	0	0	1	0	0	

$P \oplus L_0 \rightarrow R_1$



1	1	1	0	0	0	1	1	R ₁
1	1	1	1	0	1	1	1	
1	1	0	1	1	0	0	0	
1	1	0	0	0	0	0	0	

Steganography

Introduction:-

The word steganography is derived from the Greek words “*stegos*” meaning “cover” and “*grafia*” meaning “writing” defining it as “covered writing”.

Steganography is one such pro-security innovation in which secret data is embedded in a cover.

Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention.

The study of hiding information is called **Cryptography**. When communicating over an untrusted medium such as internet, it is very important to protect information and **Cryptography** plays an important role in this. Today, **Cryptography** uses principles from several disciplines such as mathematics, computer science, etc. **Steganography** deals with composing hidden messages so that only the sender and the receiver know that the message even exists.

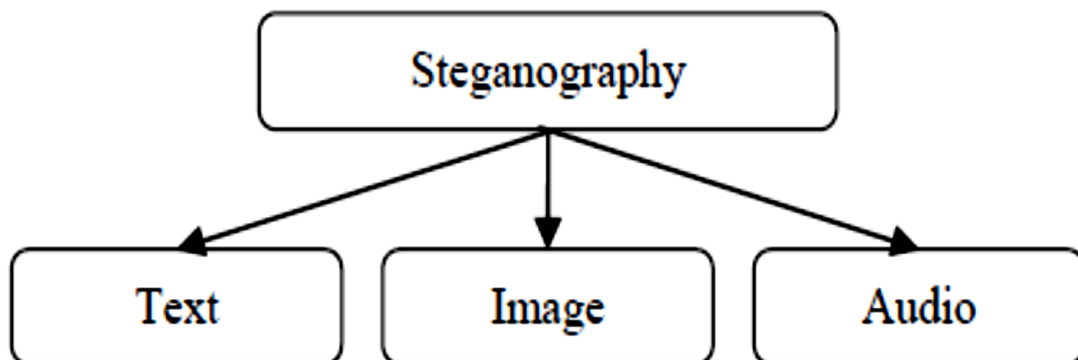
Steganography and **Cryptography** are closely related. **Cryptography** scrambles (تخلط) messages so they cannot be understood.

Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion (تثير الشك) while an

"invisible" message will not do so. Both sciences can be combined to produce better protection of the message. In this case, when the **Steganography** fails and the message can be detected, it is still of no use as it is encrypted using **Cryptography** techniques.

There exist two types of materials in steganography: message and carrier. Message is the secret data that should be hidden and carrier is the material that takes the message in it.

Figure below shows the different categories of file formats that can be used for steganography techniques.



Differences between Steganography and Cryptography:-

1. Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists.
2. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message.
3. Steganography hides a message within another message normally called as a cover and looks like a normal graphic, video, or sound file. In cryptography, encrypted message looks like meaningless jumble of characters.

4. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content.
5. Steganography requires caution when reusing pictures or sound files. In cryptography caution is required when reusing keys.

By combining Steganography and Cryptography one can achieve better security.

Types of Steganography:-

1. Hiding a message inside text.
2. Hiding a message inside images.
3. Hiding a message inside audio or video files.

University:- Baghdad

College:- Education for Pure Science Ibn Al-Haithem

Department:- Computer Science

Stage:- Fourth Class

Subject:- Computer Security/ Fourth Class

Lecturer Name:- Shaimaa Abbas Al-Obaidy

Academic Status:- Instructor

Qualification:- M.SC. Computer

Computer Security

References:-

1. William Stallings, "Cryptography and Network Security", Prentice Hall, 2006.
2. Matt Bishop, Computer Security, Addison Wesley, 2003.

Topics Covered (2018-2019)

Chapter One:-

- **Computer Security**
- **Data Security**
- **Privacy**
- **Integrity**
 - **Data Integrity**
 - **System Integrity**
- **Authentication**
- **Confidentiality**
- **Identification**
- **Good Security Standards**
- **The Effective Security**
- **The Consequences of Security Violation**
- **Internet Privacy and Security**
 - **Privacy on internet**
 - **Internet Security**
- **Cautions when using Social Network**
- **Security Involving Programs**
- **Information Access Problems**
 - **Trapdoors (Definition and Causes of Trapdoors)**
 - **Trojan Horse**
 - **Salami Attack**
- **Programs that leak information**
 - **Covert Channel**

- How to Create Covert Channels
- **Service Problems**
 - Greedy Programs
 - Viruses
 - Worms
- **Program Development Controls against Program Attacks**
 - (a) Modularity (b) Encapsulation (c) information Hiding

Chapter Two:-

- **Cryptology**
- **Cryptography**
- **Plaintext**
- **Ciphertext**
- **Cipher**
- **Encipherment (Encryption)**
- **Decipherment (Decryption)**
- **Key**
- **Cryptanalysis**
- **Components of Cryptographic System**
- **General Requirements of Cryptographic System**
- **Types of Cryptanalysis Attacks**
 - Cipher text only attack
 - Known Plaintext attacks
 - Chosen Plaintext attacks

- Adaptive Chosen Plaintext attacks
- Chosen Ciphertext attacks
- Chosen Key attacks
- Rubber hose Cryptanalysis
- Threats types
 - Passive
 - Active
- Types of Cryptosystem depends on key
 - Passive
 - Active
- Mathematical Background
 - Number Theory
 - Greatest Common Divisor
 - 1- by using Subtraction
 - 2- by using Euclid's Algorithm
 - Computing Inverse for 2-Dim matrix
 - Matrix multiplication

Chapter Three:-

- Traditional Systems for Cipherring
- Transposition Cipher
 - 1- Simple Transposition
 - a- Columnar Transposition
 - b- Fixed Period Transposition
 - 2- Double Transposition

- **Substitution Cipher**
 - a- **Simple Substitution Cipher**
 - 1- **Standard-Standard**
 - 2- **Standard-Reverse**
 - 3- **Mixed Alphabet**
 - 3.1 **Keywords**
 - 3.2 **Multiplicative**
 - 3.3 **Shift-Multiplicative (Affine)**
 - 4- **Randomly**
 - b- **Homophonic Substitution Cipher**
 - 1- **Beal Cipher**
 - 2- **Multi-Equivalent Substitution**
 - c- **Polyalphabetic Substitution Cipher**
 - 1- **Vigenere Cipher**
 - 2- **Beaufort Cipher**
 - 3- **Running Key Cipher**
 - 4- **One-Time Pad (OTP) Verman Cipher**
 - d- **Polygram Substitution Cipher**
 - 1- **Playfair Cipher**
 - 2- **Hill Cipher**

Chapter Four:-

- **Symmetric and Asymmetric System**
- **Block Cipher System**

- 1- Advantages
 - 2- Disadvantages
 - 3- Cipher Block Chaining Mode (CBC)
- **Stream Cipher System**
 - 1- Synchronous
 - 2- Asynchronous

 - **Block Cipher & Stream Cipher Comparison**
 - **Feistel Cipher Structure**
 - **Feistel Cipher Design Elements**
 - **Product Cipher (Data Encryption Standard DES)**
 - 1- Overview
 - 2- DES Steps
 - 3- Key Transformation
 - 4- DES Round Structure
 - 5- Substitution function (*Compression Functions S-Boxes*)
 - 6- Generation of keys
 - 7- DES Example

 - **Steganography**
 - 1- Introduction
 - 2- Differences between Steganography and Cryptography
 - 3- Types of Steganography

العملي

- Euclid's Algorithm
- Columnar Algorithm
- fixed period Algorithm
- Double Algorithm
- Simple standard-standard Algorithm
- Simple standard-Reverse Algorithm
- Simple Mixed alphabet/Keyword Algorithm
- Simple Mixed alphabet/Multiplicative Algorithm
- Simple Mixed alphabet/Shift + Multiplicative Algorithm
- Simple Randomly Algorithm
- Simple Homophonic Substitution/Beale Algorithm
- Polyalphabetic Substitution /Vigenere Cipher Algorithm
- Polyalphabetic Substitution /Beaufort Cipher Algorithm
- Polyalphabetic Substitution /Running-key Cipher Algorithm
- The Polygram Substitution Ciphers/ Play Fair Algorithm
- The Polygram Substitution Ciphers/ Hill Cipher Algorithm