# Unit-II

## Conventional and Symmetric Cryptography

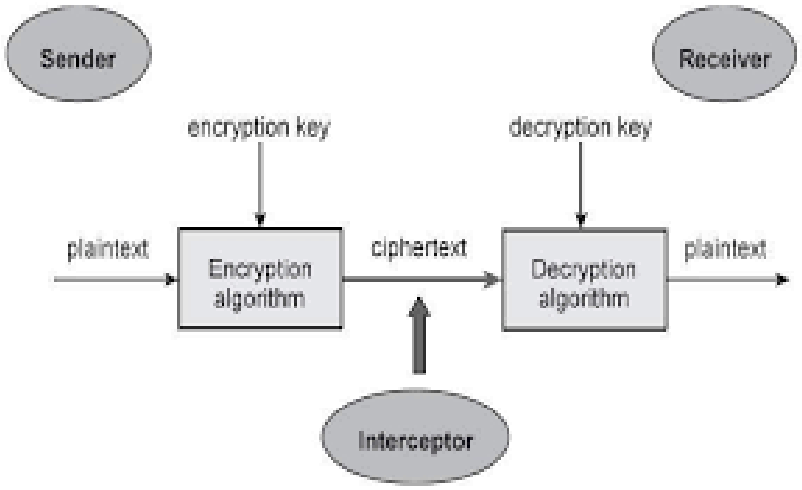
### 2.1 Cryptography terms

1. **Plain text**
   - ✓ It is any readable data — including binary files — in a form that can be seen or utilized without the need for a decryption key or decryption device.
   - ✓ Data that can be read and understand without any special measure.
   - ✓ Plaintext would refer to any message, document, file, and the like intended or having been encrypted.
   - ✓ Plaintext is the input to a crypto system, with cipher text being the output.
   - ✓ In cryptography, algorithms transform plaintext into cipher text, and cipher text into plaintext.
2. **Cipher text**
   - ✓ Cipher text is encrypted text transformed from plaintext using an encryption algorithm.
   - ✓ Cipher text can't be read until it has been converted into plaintext (decrypted) with a key.
3. **Cryptography or Cryptology**
   - ✓ Cryptography is a Greek word having the meaning of **"Secret Writing"**. It is the science of using mathematics to encrypt and decrypt data.
   - ✓ **Cryptography** focuses on creating secret codes for providing security to information.
   - ✓ Cryptography is technique of securing information and communications through use of codes so that only that person for whom the information is designed can understand it and process it.

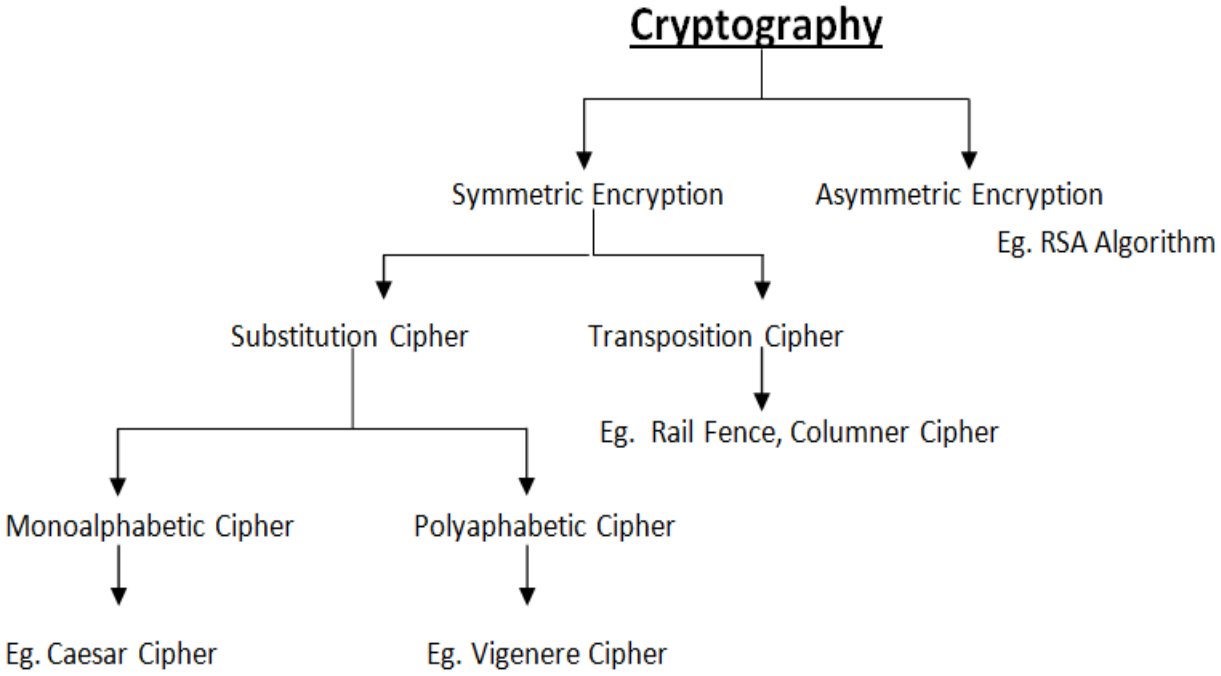

4. **Cryptanalysis**
   - ✓ It is the breaking of "Secret Codes".
   - ✓ It is the science of breaking Encryption.
   - ✓ Cryptanalysis which is the study of the cryptographic algorithm and the breaking of those secret codes.
5. **Encryption**
   - ✓ Encryption is the process by which a readable message is converted to an unreadable form to prevent unauthorized user from reading it.

- ✓ It is an Algorithm for transforming plain text to cipher text.

6. **Decryption**
   - ✓ Decryption is the process of converting an encrypted message back to its original (readable) format. The original message is called the plaintext message.
   - ✓ It is an Algorithm for transforming cipher text to plain text.
7. **Key:** It is used for encryption and decryption of message.




## ❖ Types of Cryptography



| Symmetric key cryptography/Encryption | Asymmetric key cryptography/Encryption |
|---|---|
| It is also known as Conventional Cryptography/Secret Key /Private Key Cryptography. | It is also known as Public key cryptography. |
| Both sender and receiver use single same key for Encryption and Decryption. | It uses two keys:<br>1. Public key known to everyone.<br>2. Private key known to receiver. |
| Example: DES(Data Encryption Standard),AES | Example: RSA algorithm, DSA |
| Key distribution poses serious problem. | Key distribution does not pose serious problem. |
| The encryption process is very fast. | The encryption process is slow. |
| Security is less as only one key is used for both encryption and decryption purpose. | It is more secure as two keys are used here- one for encryption and the other for decryption. |
| Less complexity of algorithm. | More complexity of algorithm. |
| It is efficient as it is used for handling large amount of data. | It is comparatively less efficient as it can handle a small amount of data. |

## 2.2 Substitution and Transposition Techniques

### ❖ Substitution Techniques

- ✓ Substitution technique involves replacing letters with other letters and symbols. In simple terms, the characters present in the initial message are restored by the other characters or numbers or by symbols.
- ✓ There are various types of substitution ciphers which are as follows

**1) Monoalphabetic Cipher**

- ✓ A Monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key.
- ✓ For Example, if a letter A in the plaintext is changed to G then each appearance of A in the plaintext will be restored by G.
- ✓ Examples of Monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key.

**2) Polyalphabetic Cipher**

- ✓ A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

- ✓ For example, letter 'A' can be restored by the letter 'C' and the similar letter 'A' can be restored by 'N' later in the cipher text.
- ✓ The Vigenere cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

| **Monoalphabetic Cipher** | **Polyalphabetic Cipher** |
|---|---|
| The relationship between a character in the plain text and the characters in the cipher text is **one-to-one**. | The relationship between a character in the plain text and the characters in the cipher text is **one-to-many**. |
| It is a simple substitution cipher. | It is multiple substitutions cipher. |
| Monoalphabetic ciphers are not that strong as compared to Polyalphabetic cipher. | Polyalphabetic ciphers are **much stronger**. |
| **Ex. Caesar cipher** | **Ex: Vigenere cipher** |

- ✓ There are various types of substitution ciphers which are as follows:
  1. Caesar Cipher
  2. Playfair Cipher
  3. Hill Cipher
  4. One Time Pad

## A) Caesar Cipher:

- ✓ It is also known as shift cipher or additive cipher.
- ✓ It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet.
- ✓ For example, with a shift of 1, A would be replaced by B, B would become C, and so on.
- ✓ First translate all of characters to numbers, 'a'=0, 'b'=1, 'c'=2, ... , 'z'=25.
- ✓ **For Encryption, C=E(P)=(P+K) mod 26**
- ✓ **For Decryption, P=D(C)=(C-k)mod 26**

**Example:**

Plain Text=HELLO AND Key=3

**Encryption:**

Cipher Text=KHOOR

**Decryption:**

Plain Text=HELLO

**Example :-** ① caesar cipher

Plain Text: "hello" and key = 3

⇒ **Encryption :-** $E(P) = (P + K) \bmod 26$

| 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 |

P.T. = hello, k = 3 (key)

$E(h) = (h + k) \% 26$
$= (7 + 3) \% 26$
$= 10$
$= k$

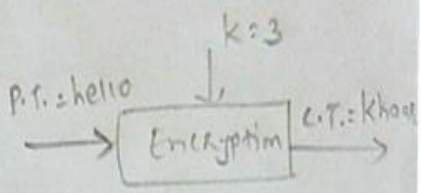
$E(e) = (e + k) \% 26$
$= (4 + 3) \% 26 = 7 = h$

$E(l) = (l + k) \% 26$
$= (11 + 3) \% 26 = 14 = o$

$E(l) = 14 \% 26 = 14 = o$

$E(o) = (o + k) \% 26$
$= (14 + 3) \% 26 = 17 = r$

∴ C.T. = khoor




⇒ **Decryption :-** $D(c) = (c - k) \bmod 26$

C.T. = khoor, key = 3

∴ $D(k) = (k - 3) \% 26 = (10 - 3) \% 26 = 7 = h$

$D(h) = (h - 3) \% 26 = (7 - 3) \% 26 = 4 = e$

$D(o) = (o - 3) \% 26 = (14 - 3) \% 26 = 11 = l$

$D(o) = (o - 3) \% 26 = (14 - 3) \% 26 = 11 = l$

$D(r) = (r - 3) \% 26 = (17 - 3) \% 26 = 14 = o$

∴ P.T. = hello

**Example:**

Our plain text is: WE WILL MEET IN THE MORNING

Encryption key:3

| Plain text | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Position | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Add 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| Cipher text | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |

| Plain text | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|
| Position | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Add 3 | 20 | 21 | 22 | 23 | 24 | 25 | 0 | 1 | 2 |
| Cipher text | U | V | W | X | Y | Z | A | B | C |

Our cipher text: ZH ZLOO PHHW LO WKH PRUQLQ

## B) Playfair Cipher

- ✓ The Playfair cipher is also known as Playfair Square.
- ✓ The Playfair cipher is a symmetric cipher
- ✓ It is a cryptographic technique used for manual encryption of information.
- ✓ The Playfair cipher has a key and plaintext.
- ✓ The key is in the form of a word which can be any sequence of 25 letters without repeats.

- **Rules to make Playfair matrix of KEY.**
  - Arrange in 5*5 matrixes.
  - Double characters are not repeated.
  - Write down other letters of the character set.
  - I/J should be on the same position.

**Example:**

**Playfair matrix (key matrix):**

Key=MONARCHY

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

- **Steps of algorithm:**
  1. Make a Playfair matrix.
  2. Split the message (Plain Text) in pair of characters.
     - If a pair is a repeated letter, insert filler like 'X'

     Example: TEXT→ TE XT

     HELLO →HE LL O →HE LX LO
  3. Follow the rules for encryption as given below.
- **Rules:**

1. If **both letters fall in the same row**, replace each with letter to right. (wrapping back to start from end)

   For example, AR is encrypted as RM

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

2. If **both letters fall in the same column**, replace each with the letter below it (wrapping to top from bottom)

   For example, MU is encrypted as CM
3. **Otherwise** each letter is replaced by the letter in the same row and in the column of the other letter of the pair

For Example SH becomes PB and EA becomes IM.

**Examples: (solve it)**

1. key="summer" then write Playfair matrix(table)
2. key="computer" then write Playfair matrix(table)
3. key="colgate" then write Playfair matrix(table)
4. key="hello" and plaintext="university" then write Playfair matrix (table) and Encrypt message using Playfair cipher.
5. key="security" and plaintext="cryptography" then write Playfair matrix (table) and Encrypt message using Playfair cipher.

**Example:**

Key: KEYWORD

Our message to encrypt is : SECRET MESSAGE

Step 1: First of all divide a message in Diagraph (Pair of Character).ADD X to separate duplicate characters.

SE CR ET ME SX SA GE

Step 2: Create Playfair table. First write down Key and then write other Alphabets.

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

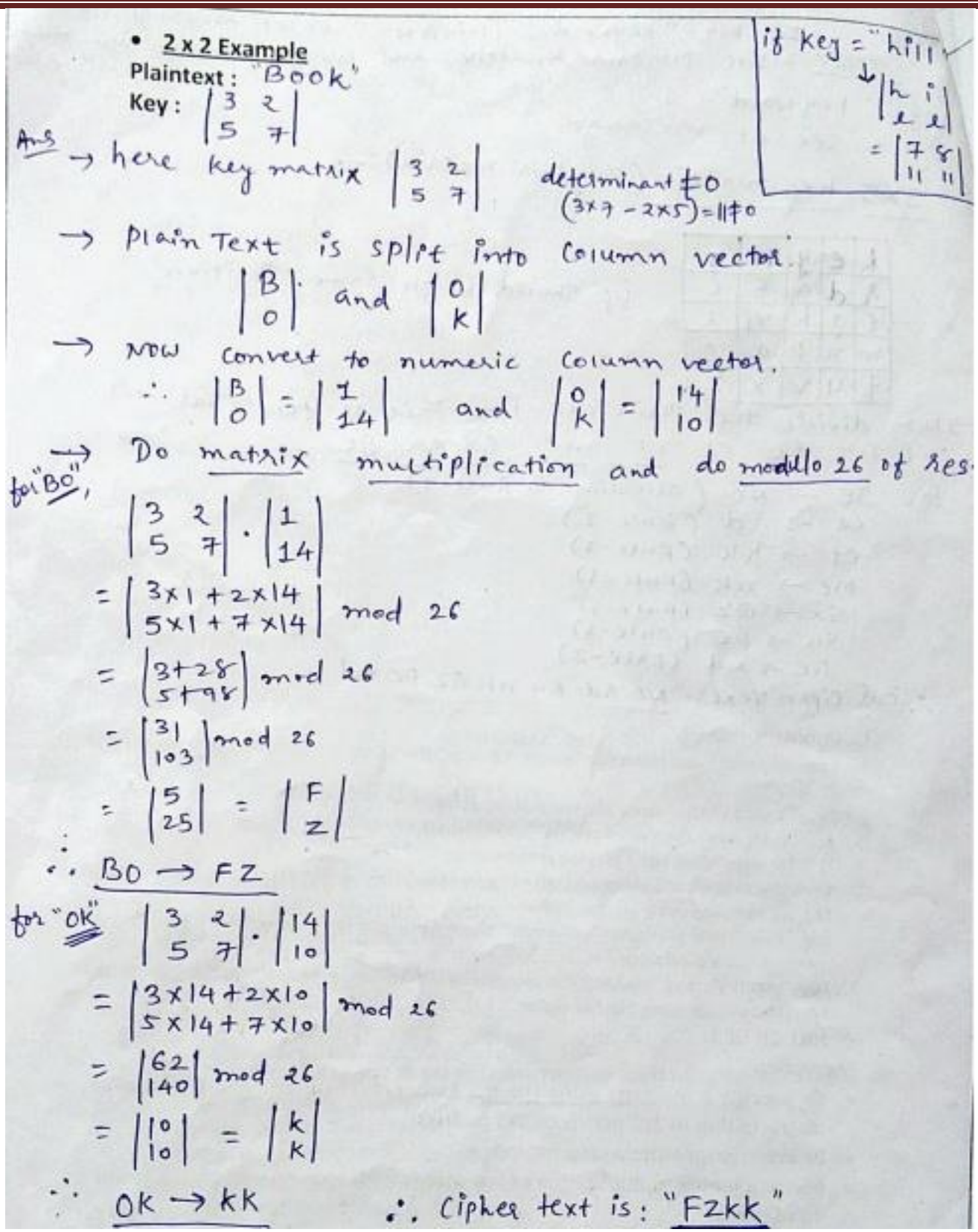
Step 3: By following above rule(Rule no.3).code for SE is No. Same way byfollowing rule-1,we can get code for CR is RD

So our message is encrypted as : NORDKUNKQZPCND

## C) Hill Cipher

- ✓ Hill cipher is a polygraphic substitution cipher based on linear algebra.
- ✓ Each letter is represented by a number modulo 26.
- ✓ It was invented by Lester S. Hill in the year 1929.
- ✓ In simple words, it is a cryptography algorithm used to encrypt and decrypt data for the purpose of data security.

- **Rules for Encryption in Hill Cipher**
  - To encrypt a message using the Hill Cipher, first turn keyword into a key matrix (either in 2x2 matrix or 3x3 matrix).
  - Plaintext is split into a column vector.
  - Perform matrix multiplication of key matrix with column vector. Do modulo 26 of result.



- **2 x 2 Example**

Plaintext : "Book"

Key : $\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix}$

Ans → here key matrix $\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix}$ determinant $\neq 0$

$(3\times7 - 2\times5) = 11 \neq 0$

→ Plain Text is split into column vector.

$\begin{vmatrix} B \\ O \end{vmatrix}$ and $\begin{vmatrix} O \\ K \end{vmatrix}$

→ Now convert to numeric column vector.

$\therefore \begin{vmatrix} B \\ O \end{vmatrix} = \begin{vmatrix} 1 \\ 14 \end{vmatrix}$ and $\begin{vmatrix} O \\ K \end{vmatrix} = \begin{vmatrix} 14 \\ 10 \end{vmatrix}$

→ Do matrix multiplication and do modulo 26 of res.

for "BO",

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 14 \end{vmatrix}$$

$$= \begin{vmatrix} 3\times1 + 2\times14 \\ 5\times1 + 7\times14 \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} 3+28 \\ 5+98 \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} 31 \\ 103 \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} 5 \\ 25 \end{vmatrix} = \begin{vmatrix} F \\ Z \end{vmatrix}$$

$\therefore$ BO → FZ

for "OK"

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \cdot \begin{vmatrix} 14 \\ 10 \end{vmatrix}$$

$$= \begin{vmatrix} 3\times14 + 2\times10 \\ 5\times14 + 7\times10 \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} 62 \\ 140 \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} 10 \\ 10 \end{vmatrix} = \begin{vmatrix} K \\ K \end{vmatrix}$$

$\therefore$ OK → KK

$\therefore$ Cipher text is: "FZKK"

if Key = "hill"

$\downarrow \begin{vmatrix} h & i \\ l & l \end{vmatrix} = \begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix}$

- **EXAMPLES**:

1. Plain text = SUMMER and key is

| | | |
|---|---|---|
| 17 | 17 | 5 |
| 21 | 18 | 21 |
| 2 | 2 | 19 |

2. Plain text = WINTER and key is

| | | |
|---|---|---|
| 2 | 1 | 3 |
| 4 | 2 | 1 |
| 3 | 6 | 7 |

3. Plain text = ATT and key is

| | | |
|---|---|---|
| 2 | 4 | 5 |
| 9 | 2 | 1 |
| 3 | 17 | 7 |

## D) VIGNER CIPHER/ **Polyalphabetic** cipher

- ✓ Vigenere Cipher is a method of encrypting alphabetic text.
- ✓ It uses a simple form of Polyalphabetic substitution.
- ✓ A Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
- ✓ The encryption of the original text is done using the Vigenere square or Vigenere table.
- ✓ For Vigenere Cipher, use Vigenere Table.
- ✓ The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- ✓ At different points in the encryption process, the cipher uses a different alphabet from one of the rows.The alphabet used at each point depends on a repeating keyword..

- **Rules for Encryption in Vigenere Cipher**
  1. To encrypt a message using the Vigenere Cipher you first need to choose a key.
  2. Repeat your key until the length of plaintext. Find corresponding row and column from Vigenere table.
  3. Where these two lines cross in the table, is the cipher text letter you use.

| 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 |

1) **EXAMPLE:**
**Plaintext:** secret
**Keyword:** bcd

**ENCRYPTION**:
First we must generate the keystream, by repeating the letters of the key until it is the same length as the plaintext.

| PT | S | E | C | R | E | T |
|---|---|---|---|---|---|---|
| KEY | B | C | D | B | C | D |
| CT | T | G | F | S | G | W |

**DECRYPTION**:

- Now for decryption, you find T in row of B(Key).
- Means find Cipher Text letter in the row of key. And then consider corresponding letter of column header for getting plain text back.

Find T in row of B(Key).the answer is S.(first letter of P.T.)

| CT | T | G | F | S | G | W |
|---|---|---|---|---|---|---|
| KEY | B | C | D | B | C | D |
| PT | S | E | C | R | E | T |

**2) EXAMPLE**

**Plaintext:** VIGENERE CIPHER

**KEY:** COUNTON

| PT | V | I | G | E | N | E | R | E | C | I | P | H | E | R |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| KEY | C | O | U | N | T | O | N | C | O | U | N | T | O | N |
| CT | X | W | A | R | G | S | E | G | Q | C | C | A | S | E |

## E) One Time Pad (OTP) (VERNAM (VERMIN/VERMAN) CIPHER)

- ✓ The one-time pad (OTP) or Vernam cipher is the strongest form of encryption at the time.
- ✓ It is unbreakable, solid encryption technique this is why it became known as the perfect cipher. It uses keys with randomly generated letters to replace letters in messages.
- ✓ Vernam cipher is a stream cipher where the plain text is added with a random stream of data of the same length to generate the encrypted data.

- **Key characteristics:**
  - Key must truly random.
  - key must be as long as the plaintext, and not repeating
  - Key must be used once.
  - There should be two copies of the key: One for sender and other for receiver.
  - It is also known as One Time Pad (OTP).

**1) Example**:

- To encrypt the simple message "**hello**" using the random keystream ***jqxyt***.
- Cipher Text will be "**QUIJH**"

| Plaintext | h | e | l | l | o |
|---|---|---|---|---|---|
| Keystream | J | Q | X | Y | T |
| Ciphertext | Q | U | I | J | H |

**2) Example :**

**Plaintext:** HOW ARE YOU

**Onetime pad (Key):** NCB TZQ ARX

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. Plain text | H<br>7 | O<br>14 | W<br>22 | A<br>0 | R<br>17 | E<br>4 | Y<br>24 | O<br>14 | U<br>20 |
| + | | | | | | | | | |
| 2. One-time pad | 13<br>N | 2<br>C | 1<br>B | 19<br>T | 25<br>Z | 16<br>Q | 0<br>A | 17<br>R | 23<br>X |
| 3. Initial Total | 20 | 16 | 23 | 19 | 42 | 20 | 24 | 31 | 43 |
| 4. Subtract 26, if > 25 | 20 | 16 | 23 | 19 | 16 | 20 | 24 | 5 | 17 |
| 5. Cipher text | U | Q | X | T | Q | U | Y | F | R |

Note: [For Decryption: Do **(C.T. - Key) Modulo26** for getting P.T.]

## 2.2 Transposition Techniques

### ❖ Transposition Techniques

- ✓ Transposition technique is an encryption method which is achieved by performing permutation over the plain text.
- ✓ Mapping plain text into cipher text using transposition technique is called transposition cipher.
- ✓ Transposition Cipher Technique rearranges the position of the plain text's characters. In transposition Cipher Technique, The position of the character is changed but character's identity is not changed.
- ✓ Types of Transposition Techniques are as follow
  - A. Rail Fence Transposition
  - B. Columnar Transposition

### A) Rail fence cipher

- ✓ The rail fence cipher is the simplest transposition cipher.
- ✓ It's a type of cryptographic algorithm that rearranges the positions of the letters in a message to create a new, seemingly unrelated message.
- ✓ The technique gets its name from the way we write the message.
- ✓ Here, Plaintext symbols are rearranged to produce Cipher text.(reordering of letters of Plaintext to calculate Cipher text –in transposition techniques)

- **Rail fence cipher(Explain with example)**
  - Rail fence cipher is a type of transposition cipher.
  - It involves rearranging of letters in plain text to encrypt the message.

**Example,**

**Encryption**

✓ Suppose we want to encrypt the message "INFORMATION SECURITY" using a rail fence cipher with encryption key 3. Here is how we would proceed.
Plain Text: - INFORMATION SECURITY

Number of Rails/Key: - 3

i. Arrange the plain text characters in an array with 3 rows(the key determines the number of rows), forming a zig-zag pattern:

| I | N | F | O | R | M | A | T | I | O | N | S | E | C | U | R | I | T | Y |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| I | | | | R | | | | I | | | | E | | | | I | | |
| | N | | O | | M | | T | | O | | S | | C | | R | | T | |
| | | F | | | | A | | | | N | | | | U | | | | Y |

ii. Then concatenate the non-empty characters from the rows to obtain the ciphertext: -

**Decryption:**

✓ Determine the Zigzag Pattern: - The number of columns in the rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.
✓ Hence, the rail matrix can be constructed accordingly. Once we've got the matrix we can figure-out the spots where texts should be placed.
✓ **Fill in the Encrypted Message: -** Fill the cipher-text row wise.
✓ **Read the Decrypted Message:** -Read the characters diagonally from the top-left corner to the bottom-right corner, reversing direction when needed. The resulting sequence is the decrypted message.

**Example:**

✓ **Ciphertext: - IRIEINOMTOSCRTFANUY**

| I | | | | R | | | | I | | | | E | | | | I | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | N | | O | | M | | T | | O | | S | | C | | R | | T | |
| | | F | | | | A | | | | N | | | | U | | | | Y |

**Decrypted Message: - INFORMATION SECURITY**

### ❖ Difference between the Substitution Technique and Transposition Technique

| Substitution Cipher Technique | Transposition Cipher Technique |
|---|---|
| In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols. | In transposition Cipher Technique, plain text characters are rearranged with respect to the position. |
| Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher. | Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher. |
| In substitution Cipher Technique, character's identity is changed while its position remains unchanged. | While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed. |
| The example of substitution Cipher is Caesar Cipher, Monoalphabetic cipher, and Polyalphabetic cipher. | The example of transposition Cipher is Rail Fence Cipher, columnar transposition cipher, and route cipher. |
| Relatively easy to understand and implement, making it suitable for simple applications. | Can be more difficult to implement and understand, but can be more secure than substitution ciphers for certain applications. |

## 2.3 Steganography

- ✓ A plain text message may be hidden in one of two ways: Stegnography and encryption
- ✓ The word Steganography is derived from two Greek words- 'stegos' meaning 'to hidden' and 'grayfia', meaning 'writing', thus translating to 'covered writing', or 'hidden writing'.
- ✓ Steganography means hiding a message within another message or image.
- ✓ Steganography is the art of hiding a message, image, or file within another message, image, or file.
- ✓ Example of stegnography,
  - Written message using invisible ink.
  - Character marking: selected letters of printed or typewritten text are over written in pencil.
  - Pin punctures: Small pin punctures on selected letters.
- ✓ Types of Stegnography: There are five main types of stegnography
  1. Text Stegnography: It involves hiding information inside text files.Ex:changing the format of existing text,changing words within a text, generating random character sequences etc.

2. Image Stegnography: It involves hiding information within image files.
3. Video Stenography : It allows large amount of data to be hidden within a moving stream of images and sounds.
4. Audio Stegnography: It involves secret messages being embedded into an audio signal which alters the binary sequences of the audio file.
5. Network Stegnography: It is also known as protocol Stegnography

- ✓ **Digital Steganography:**We can insert date or we can hide data in the image by replacing bits of image.Most common technique are:
  - LSB,
  - DCT and
  - Append type.

- **LSB: Least Significant Bit**
  - ✓ Replace LSB bit with a bit from hidden data.
  - ✓ LSB has smallest effect on the amount of color.
  - ✓ Replacing LSB to hidden data will have small effect on the picture.
- **DCT stands for Discrete Cosine Transform**
  - ✓ It works by calculating the frequencies of the image then replace some of them.
- **Append:**
  - ✓ Instead of hide the data in the photo by manipulating the picture, Append algorithm appends the data to the end of the file as appending.
  - ✓ This algorithm will change the size of the file.

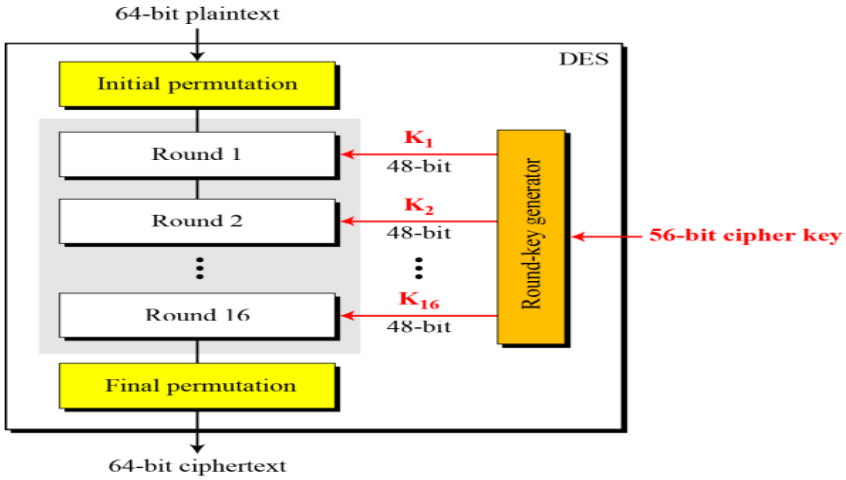
## 2.4 Symmetric Cryptography: Data Encryption Standard- Structure, Advantages and Disadvantages

The Data Encryption Standard (DES) is a **symmetric-key block cipher** published by the National Institute of Standards and Technology (NIST).

**DES Structure:**

- ✓ The Data Encryption Standard (DES) is a block cipher.
- ✓ The encryption process is made of two permutations (P-boxes), which we call initial and final permutations, and sixteen Feistel rounds.

✓ General Structure of DES is shown in figure:

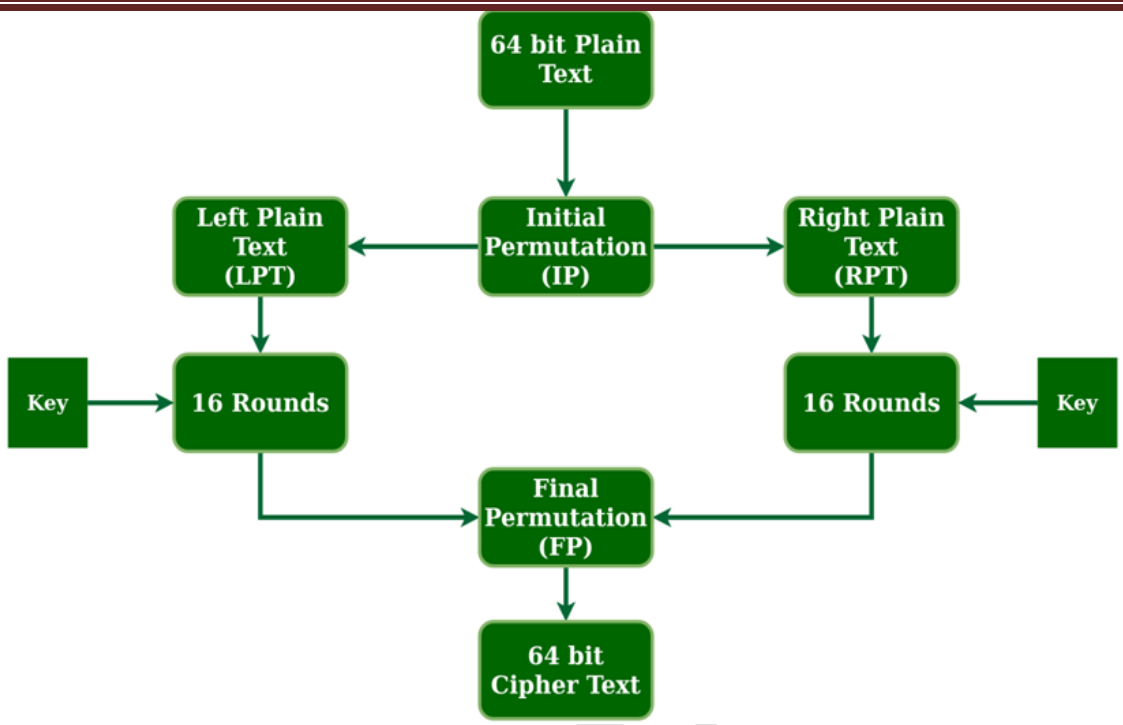



### DES Algorithm Steps

The plain text is divided into smaller chunks of 64-bit size. The IP is performed before the first round. This phase describes the implementation of the transposition process

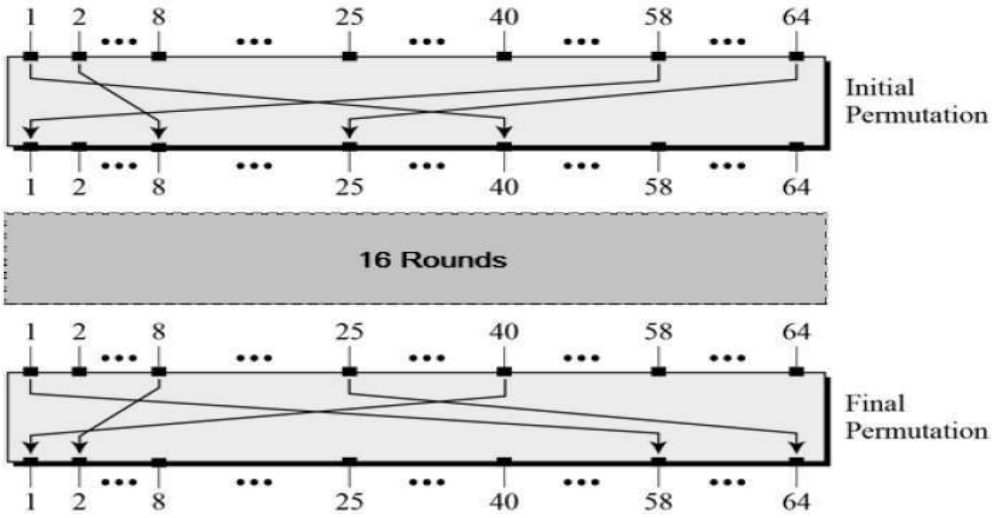
DES takes 64-bit plain text and turns it into a 64-bit ciphertext.

1. The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
2. The initial permutation (IP) is then performed on the plain text.
3. Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
4. Each LPT and RPT goes through 16 rounds of the encryption process.
5. Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.
6. The result of this process produces the desired 64-bit ciphertext.




**Initial and Final Permutation**

- ✓ The plain text is divided into smaller chunks of 64-bit size.
- ✓ The IP is performed before the first round.
- ✓ This phase describes the implementation of the transposition process. For example, the 58th bit replaces the first bit, the 50th bit replaces the second bit, and so on.
- ✓ The initial and final permutations are shown as follows −



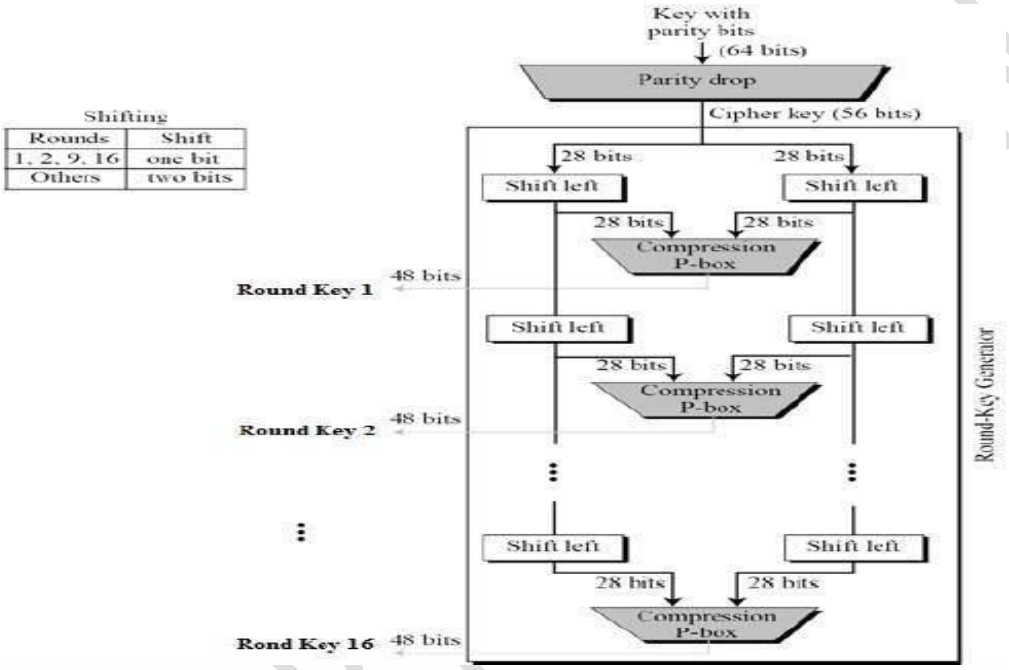
**The encryption process step (step 4, above) is further broken down into five stages:**

- ✓ Key transformation
- ✓ Expansion permutation
- ✓ S-Box permutation
- ✓ P-Box permutation
- ✓ XOR and swap

For decryption, we use the same algorithm, and we reverse the order of the 16 round keys.

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.

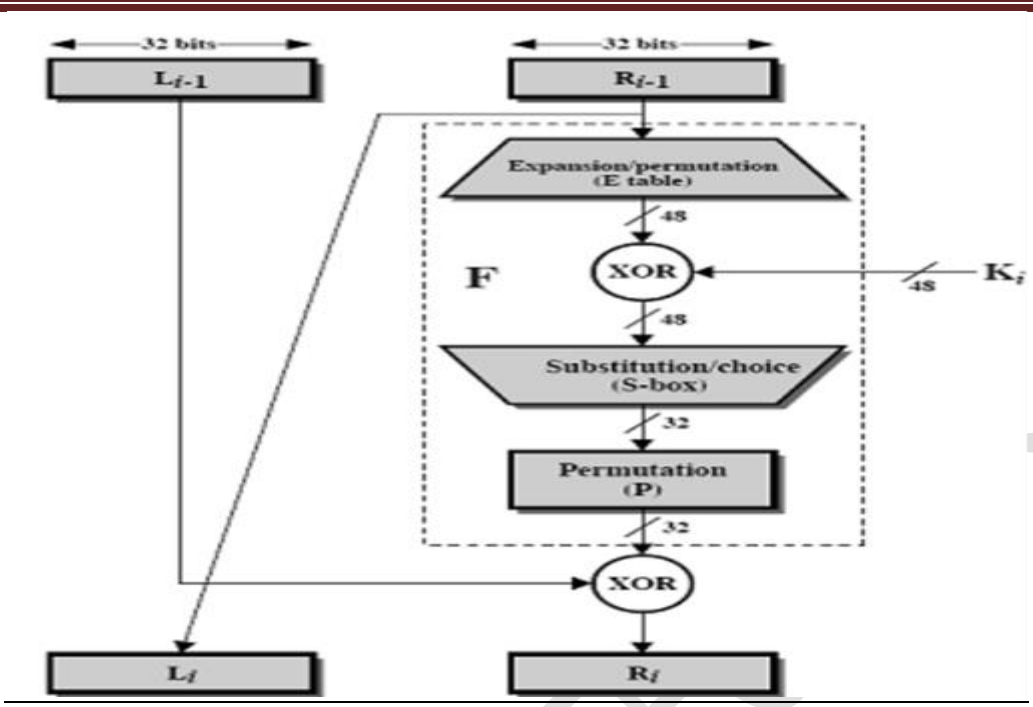



Shifting

| Rounds | Shift |
|---|---|
| 1, 2, 9, 16 | one bit |
| Others | two bits |

Round Function

The DES function f applies a 48-bit key to the rightmost 32 bits of plain text to produce a 32-bit output. Below figure display round 1.




**Advantage of DES**

- ✓ DES uses the symmetric-key algorithm, thus, it is possible to perform encryption and decryption by a single key with the same algorithm.
- ✓ It is more efficient in hardware, showing a higher and faster implementation.
- ✓ DES is relatively fast and efficient, making it suitable for use in a wide range of.
- ✓ DES has a relatively small key size, which makes it easier to use and store.
- ✓ It's not a group cipher, hence DES instances can be applied many times to a plaintext.(2DES 3DES).
- ✓ The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.
  - Avalanche effect − A small change in plaintext results in the very great change in the ciphertext.
  - Completeness − Each bit of ciphertext depends on many bits of plaintext.

**Disadvantage of DES**

- ✓ Because DES uses a smaller key, it is less secure.
- ✓ The DES algorithm is less efficient when implemented in software, resulting in slower performance.
- ✓ DES offers a lower level of security due to its 56-bit key, which can be feasibly broken by a brute-force attack.
- ✓ Now in the age of parallel computing, breaking DES has become easy with the help of brute force attack which was impossible during that time.( it's possible to brute-force in finite time on modern processors).
- ✓ In a new technology, it is improving a several possibility to divide the encrypted code, therefore AES is preferred than DES.