Unit I :Classical Encryption Techniques and DES:

Contents:

I. The OSI Security Architecture

II. Symmetric Cipher Models

III. Substitution Techniques

IV. Transposition Techniques

V. Block Cipher Principles

VI. The Data Encryption Standard.

Basics of Information and Network Security

- In daily life we use information for various purposes and use network for communication and exchange information between different parties.
- In many cases these information are sensitive so we need to take care that only authorized party can get that information.
- For maintaining such privacy we require some mechanism or physical device which ensures that it is safe. Such mechanism or physical devices are known as **security system**.
- **Computer Security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability**, and **confidentiality** of information system resources.
- This definition of computer security introduces three key objectives that are at the heart of computer security:

1. **Confidentiality:** It covers two concepts

   Data Confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

   Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

2. **Integrity:** It covers two concepts

Data Integrity: Assures that information and programs are changedauthorize manner.

only in a specified and

System Integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

3. **Availability:** Assures that systems work promptly and service is not denied to authorize user.

- **Unconditionally secure algorithm:** An algorithm or an encryption scheme is unconditionally secure if the attacker cannot obtain the corresponding plaintext from ciphertext no matter how much ciphertextis available.
- **Computationally secure algorithm:** An encryption scheme is said to be computationally secure if either of the following criteria is met:
  - The cost of breaking the cipher exceeds the value of the encrypted information.
  - The time required to break the cipher exceeds the useful lifetime of the information.
  - **Threat:** A potential for violation of security, which exists when there is a circumstance, capabilit

action, or event that could breach security and cause harm. That is, a threat is a possible danger thatmight exploit vulnerability.

❖ The OSI Security Architecture

Security Attacks

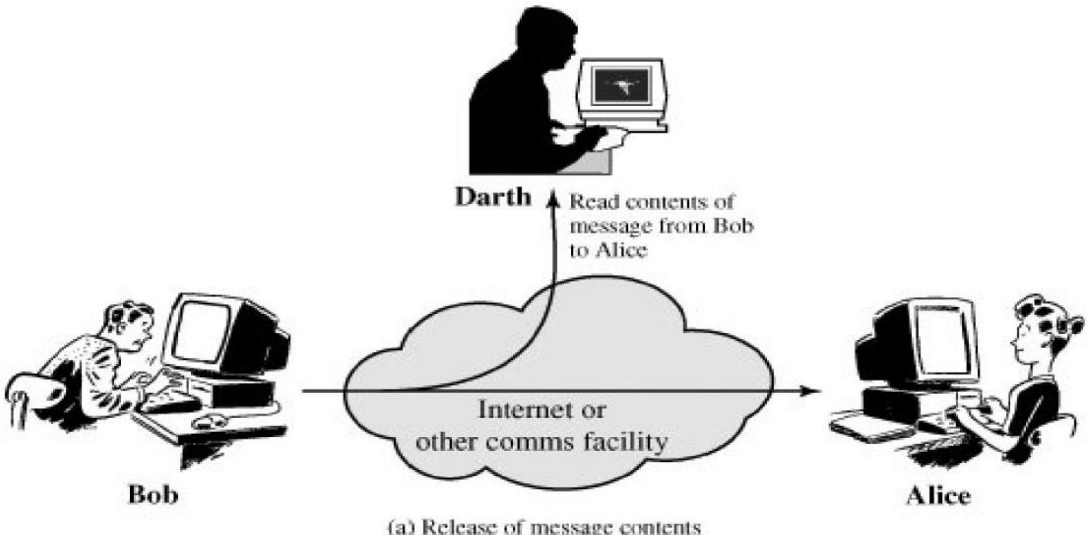
- **Security Attacks:** An attack is an action that comprises the information or network security.
- There are two types of attacks:
  1. Passive Attack
  2. Active Attack

1. Passive Attack

The attacker only monitors the traffic attacking the confidentiality of the data. It contains release of message contents and traffic analysis (in case of encrypted data).

I.. Release of message contents:

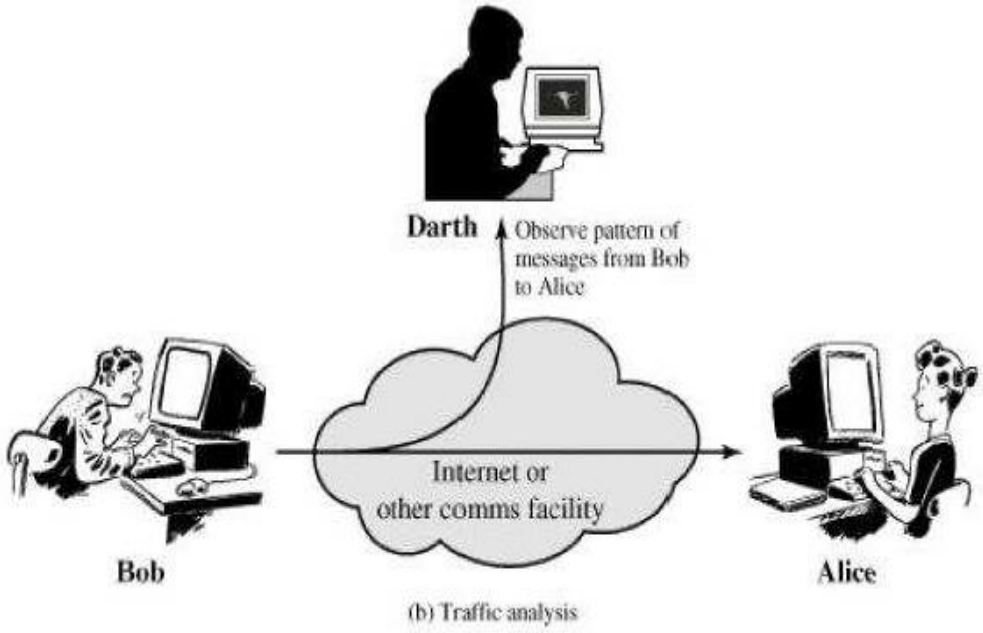
- The release of message contents is easily understood.
- We would like to prevent an opponent from learning the contents of these transmissions.
- A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.



(a) Release of message contents

II.Traffic analysis:

- A second type of passive attack, traffic analysis.
- Suppose that we had a way of masking the contents of messages or other information.
- Even if they captured the message, could not extract the information from the message.
- The common technique for masking contents is encryption.
- If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages.
- The opponent could determine the location and identity of communicating hosts and couldobserve the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of the communication that was takingplace.
- Passive attacks are very difficult to detect because they do not involve any alteration of the data.
- Typically, the message traffic is send and received in an apparently normal fashion and the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

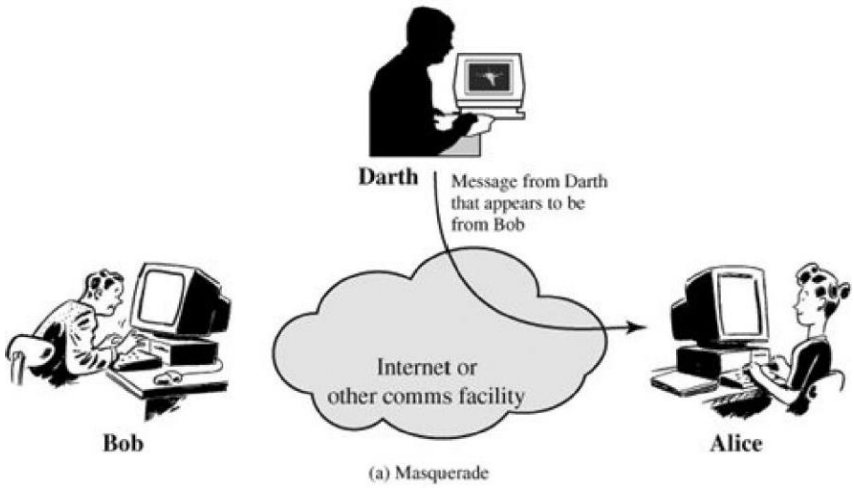


(b) Traffic analysis

2. Active attack

Attacker tries to alter transmitted data. It includes masquerade, modification, replay and denial of service.

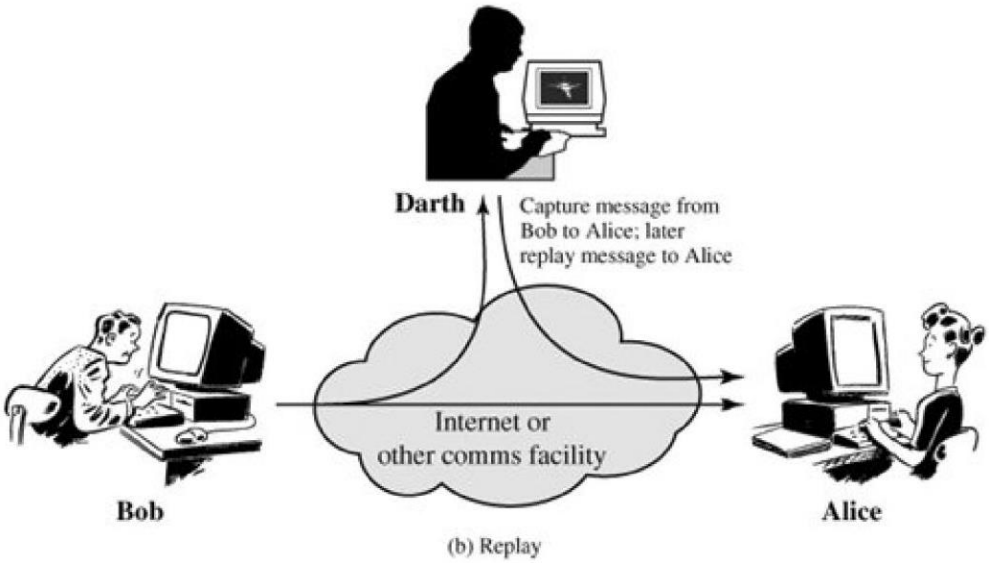
i. **Masquerade:** A masquerade takes place when one entity pretends to be a different entity (Figurea). A masquerade attack usually includes one of the other forms of active attack.



(a) Masquerade

ii. **Replay:**

- Replay involves the passive capture of a data unit and its subsequent retransmission toproduce an unauthorized effect.
- In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.

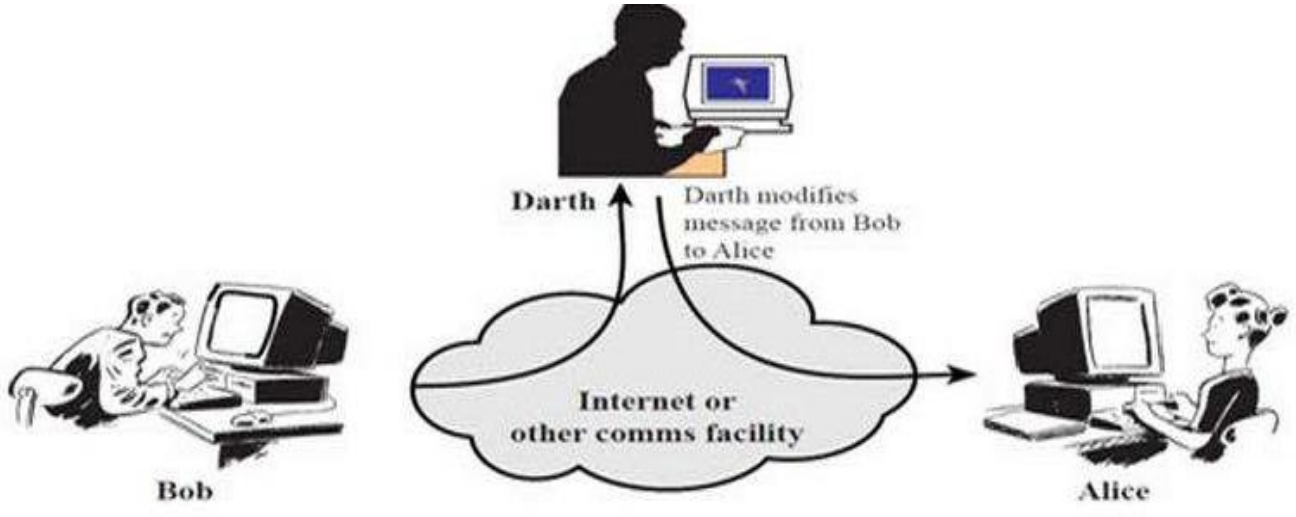


(b) Replay

iii. Modification of messages:

a. Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure c).

b. For example, a message meaning "Allow John Smith to read confidential file accounts" ismodified to mean "Allow Fred Brown to read confidential file accounts."



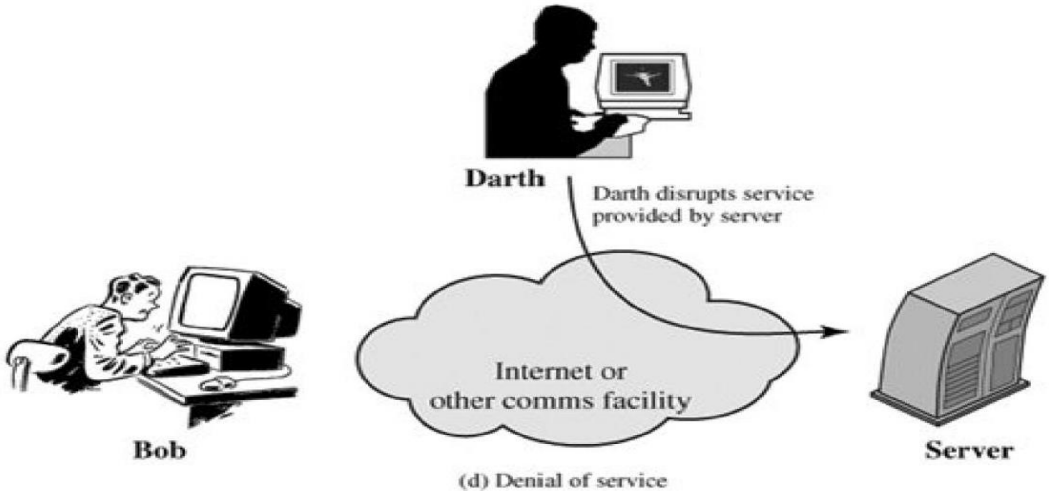
(c) Modification of messages

iv. Denial of service:

a. The denial of service prevents or inhibits the normal use or management of communicationsfacilities.

This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).

b. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance. In a DoS attack, an attacker floods a target system or network with traffic or requests in order to consume its resources, such as bandwidth, CPU cycles, or memory, and prevent legitimate users from accessing it.



(d) Denial of service

Security services

- A security service is a processing or communicating service that can prevent or detect the above-mentioned attacks. Various security services are:
    - **Authentication:** the recipient should be able to identify the sender, and verify that the sender, who claims to be the sender, actually did send the message.
    - **Data Confidentiality:** An attacker should not be able to read the transmitted data or extract data in case of encrypted data. In short, confidentiality is the protection of transmitted data from passive attacks.
    - **Data Integrity:** Make sure that the message received was exactly the message the sender sent.
    - **Nonrepudiation:** The sender should not be able to deny sending the should not be able to deny receiving the message.

❖ A MODEL FOR NETWORK SECURITY

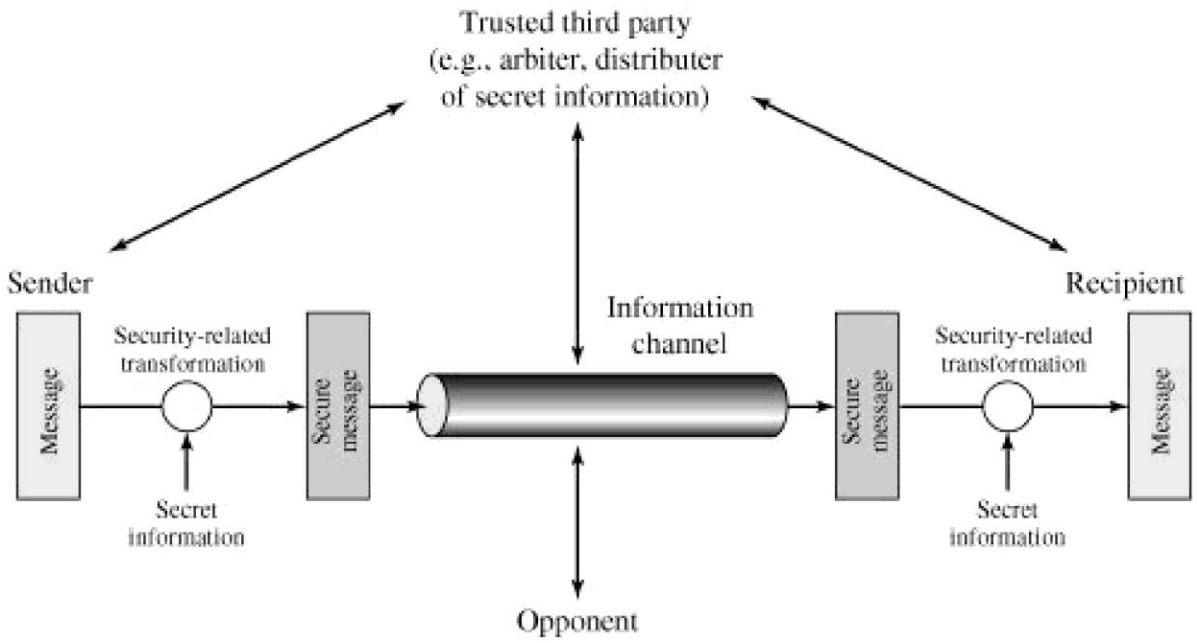


Figure. Model for Network Security

A message is to be transferred from one party to another across some sort of internet. The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.

All the techniques for providing security have two components:

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by

An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

The general model shows that there are four basic tasks in designing a particular securityservice:

1. Design an algorithm for performing the security-related transformation. Thealgorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the securityalgorithm and the secret information to achieve a particular security service.

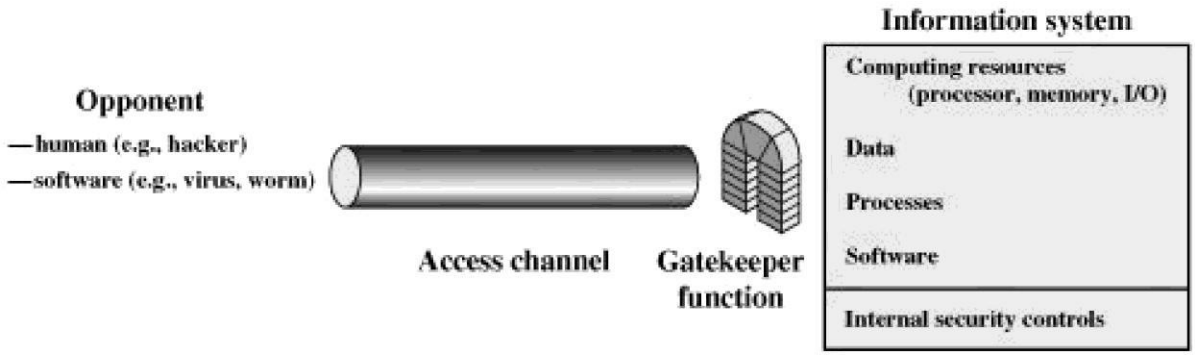


Figure: 1.6 Network Access Security Model

A general model is illustrated by the above Figure 1.6, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. Or, the intruder can be a disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computerassets for financial gain.

❖ Security Mechanism:

I. **Encipherment:** Encipherment is hiding or covering data and can provide confidentiality. It makes use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys. Cryptography and Steganography techniques are used for enciphering.

II. **Data integrity:** The data integrity mechanism appends a short check value to the data which is created by a specific process from the data itself. The receiver receives the data and the check value. The receiver then creates a new check value from the received data and compares the newly created check value with the one received. If the two check values match, the integrity of data is being preserved.

III. **Digital Signature:** A digital signature is a way by which the sender can electronically sign the data and the receiver can electronically verify it. The sender uses a process in which the sender owns a private key related to the public key that he or she has announced publicly. The receiver uses the sender's public key to prove the message is indeed signed by the sender who claims to have sent the message.

IV. **Authentication exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange. The two entities exchange some messages to prove their identity to each other. For example the three-way handshake in TCP.

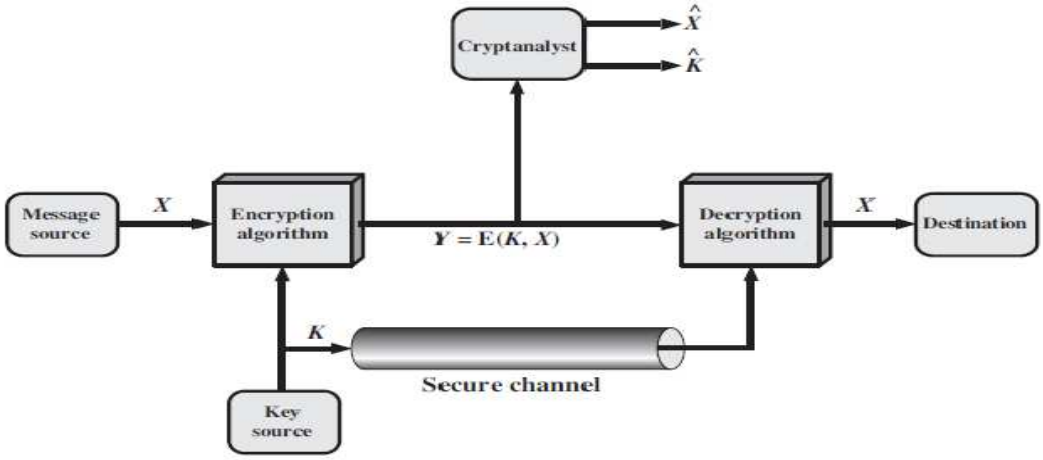
V. **Traffic padding:** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

VI. **Routing control**: Enables selection of particular physically secure routes for certain data and allows routing changes which means selecting and continuously changing different available routes between the sender and the receiver to prevent the attacker from traffic analysis on a particular route.

VII. **Notarization:** The use of a trusted third party to control the communication between the two parties. It prevents repudiation. The receiver involves a trusted third party to store the request to prevent the sender from later denying that he or she has made such a request.

VIII. **Access Control:** A variety of mechanisms are used to enforce access rights to resources/data owned by a system, for example, PINS, and passwords

❖ Symmetric Cipher Model



- A symmetric cipher model are broadly contains five parts.
- **Plaintext:** This is the original intelligible message.
- **Encryption algorithm:** The

encryption algorithm performs various substitutions and

transformations on the plaintext. It takes in plaintext and key and gives the ciphertext.

- **Secret key:** The key is a value independent of the plaintext and of the algorithm. Different keys willyield different outputs.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and thesecret key.
    - **Decryption algorithm:** Runs on the ciphertext and the key to produce the plaintext. This is essentially the encryption algorithm run in reverse.
- Two basic requirements of encryption are:
    1. Encryption algorithm should be strong. An attacker knowing the algorithm and having any number ofciphertext should not be able to decrypt the ciphertext or guess the key.
    2. The key shared by the sender and the receiver should be secret.
- Let the plaintext be $X = [X1, X2,\ldots, X_M]$, key be $K = [K1, K2,\ldots, K_J]$ and the ciphertext produced be $Y = [Y1, Y2,\ldots, Y_N]$. Then, we can write

$$Y = (K, X)$$

- Here E represents the encryption algorithm and is a function of plaintext X and key K.
- The receiver at the other ends decrypts the ciphertext using the key.

$$X = (K, Y)$$

- Here D represents the decryption algorithm and it inverts the transformations of encryption algorithm.
- An opponent not having access to X or K may attempt to recover K or X or both.
- It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms.
- If the opponent is interested

in only this particular message, then the focus of the effort is to

recover by generating a plaintext estimate $\hat{X}$.

- If the opponent is interested in being able to read future messages as well then he will attempt torecover the key by making an estimate $\hat{K}$

Cryptography

The area of study containing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

- Cryptographic systems are characterized along three independent dimensions.
  1. The types of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles substitution, and transposition. Basic requirement is that no information be lost. Most systems referred to as product system, involves multiple stages of substitutions and transpositions.
  2. The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys the system is referred to as asymmetric, two-key, or public-key encryption.
  3. The way in which the plaintext is processed. A block cipher process a block at a time and produce an output block for each input block. A stream cipher process the input element continuously, producing output one element at a time, as it goes along.=

Cryptanalysis and Brute-Force Attack

- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some simple plaintext-ciphertext pairs. This type of attack finds characteristics of the algorithm to find a specific plaintext or to find key.
- **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until plaintext is obtained. On average, half of all possible keys must be tried to achieve success.
- Based on the amount of information known to the cryptanalyst cryptanalytic attacks can be categorized as:

- **Cipher text Only Attack:** The attacker knows only cipher text only. It is easiest to defend.
- **Known plaintext Attack:** In this type of attack, the opponent has some plaintext-cipher text pairs. Or the analyst may know that certain plaintext patterns will appear in a message. For example, there may be a standardized header or banner to an electronic funds transfer message andthe attacker can use that for generating plaintext-cipher text pairs.
- **Chosen plaintext:** If the analyst is able somehow to get the source system to insert into the system a message chosen by the analyst, then a *chosen-plaintext* attack is possible. In such a case, the analyst will pick patterns that can be expected to reveal the structure of the key.
- **Chosen Cipher text:** In this attack, the analyst has cipher text and some plaintext-cipher text pairs where cipher text has been chosen by the analyst.
- **Chosen Text:** Here, the attacker has got cipher text, chosen plaintext-cipher text pairs and chosen cipher text-plaintext pairs.

- Chosen cipher text and chosen text attacks are rarely used.
- It is assumed that the attacker knows the encryption and decryption algorithms.
- Generally, an encryption algorithm is designed to withstand a known-plaintext attack.

Brute-force attack

This type of attack become impractical as the key size increases as trying all the possible alternative keys for a very large key may take a huge amount of time.

- For example, for a binary key of 128 bits, 2^{128} keys are possible which would require around $5 \ X10^{24}$ years at the rate of 1 decryption per microsecond (current machine's speed).
- The Data Encryption Standard (DES) algorithm uses a 56-bit key a 128-bit key is used in AES.
- With massively parallel systems, even DES is also not secure against Brute Force attack.
- AES with its 128-bit key is secure since the time required to break it makes it impractical to try Brute-Force attack

❖ Substitution Techniques

- Various conventional encryption schemes or substitution techniques are as under:

1. Caesar cipher

- The encryption rule is simple; replace each letter of the alphabet with the letter standing 3 placesfurther down the alphabet.
- The alphabet is wrapped around so that Z follows A.
- Example:

  Plaintext: MEET ME AFTER THE
  PARTY Ciphertext: PHHW PH
  DIWHU WKH SDUWB

- Here, the key is 3. If different key is used, different substitution will be obtained.
- Mathematically, starting from a=0, b=1 and so on, Caesar cipher can be written as:

$$E(p) = (p + k) \bmod (26)$$
$$D(C) = (C - k) \bmod (26)$$

- This cipher can be broken
  - If we know one plaintext-cipher text pair since the difference will be same.
  - By applying Brute Force attack as there are only 26 possible keys.

2. Monoalphabetic Substitution Cipher

- Instead of shifting alphabets by fixed amount as in Caesar cipher, any random permutation is assigned tothe alphabets. This type of encryption is called monoalphabetic substitution cipher.
- For example, A is replaced by Q, B by D, C by T etc. then it will be comparatively stronger than Caesarcipher.
- The number of alternative keys possible now becomes 26!.
- Thus, Brute Force attack is impractical in this case.
- However, another attack is possible. Human languages are redundant i.e. certain characters are usedmore frequently than others. This fact can be exploited.
- In English ‘e’ is the most common letter followed by ‘t’, ‘r’, ‘n’, ’o’, ‘a’ etc. Letters like ‘q’, ‘x’, ‘j’ are lessfrequently used.
- Moreover, digrams like ‘th’ and trigrams like ‘the’ are also more frequent.

- Tables of frequency of these letters exist. These can be used to guess the plaintext if the plaintext is inuncompressed English language.

3. Playfair Cipher

- In this technique multiple (2) letters are encrypted at a time.
- This technique uses a 5 X 5 matrix which is also called key matrix.

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**

- The plaintext is encrypted **two letters at a time**:
  - Break the plaintext into pairs of two consecutive letters.
  - If a pair is a repeated letter, insert a filler like ‘X‘in the plaintext, eg. "Balloon" is treated as "ba lx loon".
  - If both letters fall in the same row of the key matrix, replace each with the letter to its right(wrapping back to start from end), eg. “AR" encrypts as "RM".
  - If both letters fall in the same column, replace each with the letter below it (again wrapping to topfrom bottom), eg. “MU" encrypts to "CM".
  - Otherwise each letter is replaced by the one in its row in the column of the other letter of thepair, eg. “HS" encrypts to "BP", and “EA" to "IM" or "JM" (as desired)
- Security is much improved over monoalphabetic as here two letters are encrypted at a time andhence there are 26 X 26 =676 diagrams and hence it needs a 676 entry frequency table.
- However, it can be broken even if a few hundred letters are known as much of plaintext structure isretained in cipher text

4. Hill Cipher

- This cipher is based on linear algebra.

Each letter is represented by numbers from 0 to 25 and calculations are done m dulo 26.

- This encryption algorithm takes m successive plaintext letters and substitutes them with m cipher textletters.

- The substitution is determined by m linear equations. For m = 3, the system can be described as:

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$

$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$

$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

- This can also be expressed in terms of row vectors and matrices.

$$(c_1\ c_2\ c_3) = (p_1\ p_2\ p_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

  Where **C** and **P** are row vectors of length 3 representing the plaintext and cipher text, and **K** is a 3 X 3matrix representing the encryption key

- Key is an invertible matrix K modulo 26, of size m. For example:

- $$K = \begin{pmatrix} 17 & 17 & 5 \\ 4 & 19 & 15 \\ 21 & 18 & 21 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 15 & 17 & 6 \\ 2 & 2 & 19 \\ 24 & 0 & 17 \end{pmatrix}$$

- Encryption and decryption can be given by the following formulae:Encryption: $C = PK \bmod 26$

  Decryption: $P = CK^{-1} \bmod 26$

- The strength of the Hill cipher is that it completely hides single-letter frequencies.
- Although the Hill cipher is strong against a cipher text-only attack, it is easily broken with a knownplaintext attack.
  - Collect m pair of plaintext-cipher text, where m is the size of the key.
  - Write the m plaintexts as the rows of a square matrix P of size m.
  - Write the m cipher texts as the rows of a square matrix C of size m.
  - We have that C=PK mod 26.
  - If P is invertible, then $K=P^{-1}C \bmod 26$,
  - If P is not invertible, then collect more plaintext-cipher text pairs until an invertible P is obtained.

5. The Vigenère cipher

- This is a type of polyalphabetic substitution cipher (includes multiple substitutions depending on thekey). In this type of cipher, the key determines which particular substitution is to be used.
- To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeatingkeyword.
- For example, if the keyword is *deceptive*, the message "we are discovered save yourself" is encrypted asfollows:

  Key: *deceptivedecept*

  Plaintext: wearediscovered
  Ciphertext:
  ZICVTWQNGRZGVTW

- Encryption can be done by looking in the Vigenere Table where ciphertext is the letter key's row andplaintext's column or by the following formula:

$$C_i = (P_i + K_i \bmod m) \bmod 26$$

- Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letterin that row determines the column, and the plaintext letter is at the top of that column.
- The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword.
- Thus, the letter frequency information is obscured however, not all knowledge of the plaintext structure is lost.

6. Vernam Cipher

- This system works on binary data (bits) rather than letters.
- The technique can be expressed as follows:

$$C_i = P_i \oplus K_i$$

  Where

  P_i = i^{th} binary digit of plaintext.

  K_i = i^{th} binary digit of key.

  C_i = i^{th} binary digit of ciphertext.

  $\oplus$ = exclusive-or (XOR) operation

- Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key.
- Decryption simply involves the same bitwise operation:

$$P_i = C_i \oplus K_i$$

- The essence of this technique is the means of construction of the key.
- It was produced by the use of a running loop of tape that eventually repeated the key, so that in fact thesystem worked with a very long but repeating keyword.
- Although such a scheme has cryptanalytic difficulties, but it can be broken with a very long ciphertext orknown plaintext as the key is repeated.

7. One-Time Pad

- In this scheme, a random key that is as long as the message is used.
- The key is used to encrypt and decrypt a single message, and then is discarded. Each new messagerequires a new key of the same length as the new message.
- This scheme is unbreakable.
- It produces random output that bears no statistical relationship to the plaintext.
- Because the ciphertext contains no information whatsoever about the plaintext, there is simply no wayto break the code.
- For any plaintext of equal length to the ciphertext, there is a key that produces that plaintext.
- Therefore, if you did an exhaustive search of all possible keys, you would eplaintexts, with no way of knowing which the intended plaintext was.
- Therefore, the code is unbreakable.
- The security of the one-time pad is entirely due to the randomness of the key.

d up with many legible

- The one-time pad offers complete security but, in practice, has two fundamental difficulties:
    - There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
    - Another problem is that of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver.
- Because of these difficulties, the one-time pad is used where very high security is required.
- The one-time pad is the only cryptosystem that exhibits **perfect secrecy**.

❖ Transposition Techniques

- A very different kind of mapping is achieved by performing some sort of permutation on the plaintextletters. This technique is referred to as a transposition cipher.
- The simplest such cipher is the **rail fence** technique.

i. Rail Fence Technique

- Encryption involves writing plaintext letters diagonally over a number of rows, then read off cipher rowby row.
- For example, the text "meet me after the party" can be written (in 2 rows) as:

m e m a t r h p r

ye t e f e t e o a t

Ciphertext is read from the above row-by-row:MEMATRHPRYETEFETEAT

- This scheme is very easy to cryptanalyze as no key is involved.
- Transposition cipher can be made significantly more secure by performing more than one stage oftransposition. The result is a more complex permutation that is not easily reconstructed.

Difference between Symmetric and Asymmetric key cryptography

Symmetric key Cryptography	**Asymmetric Key Cryptography**
Symmetric key cryptography uses the same secret(private) key to encrypt and decrypt its data	Asymmetric key cryptography uses a public and aprivate key to encrypt and decrypt its data
The secret key must be known by both parties.	The public key is known to anyone with which theycan encrypt the data but it can only be decoded by the person having the private key
In key distribution process, key information mayhave to be shared which decreases the security.	Here, the need for sharing key with key distributioncenter is eliminated.
Symmetric key encryption is faster than asymmetrickey.	It is Slower than symmetric key encryption.
Basic operations used in encryption/ decryptionare transposition and substitution.	It uses mathematical functions.

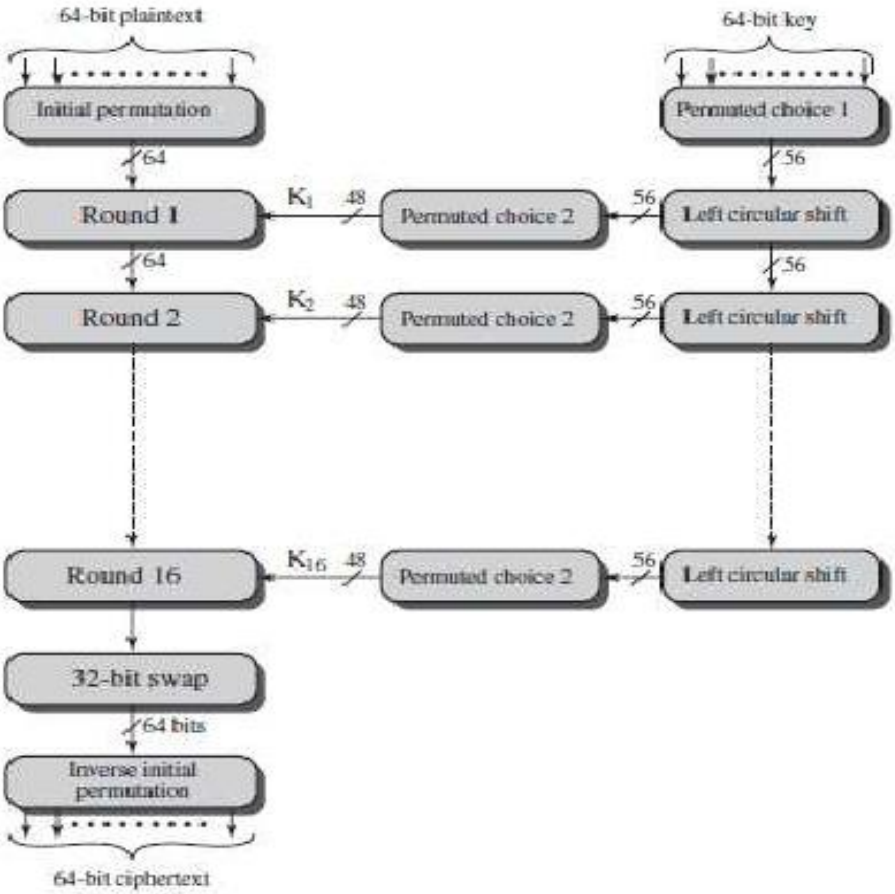
❖ The Data Encryption Standard

- SDES encrypts 64-bit blocks using a 56-bit key and produces a 64-bit ciphertext.
- Same steps, with the same key, are used to reverse the encryption withreversed.
- The DES is widely used.

DES Encryption

- The DES encryption is shown in the figure below:

the order of the keys



- Encryption function has two inputs: the plaintext to be encrypted and the key.
- The processing of the plaintext proceeds in three phases.

- The 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to producethe permuted input.
- The permuted output is then passed through sixteen rounds of the same function, which involves

  both permutation and substitution functions. The left and right halvesswapped to produce preoutput.
- The preoutput is passed through a permutation that is thepermutation function, to produce the 64-bit cipher text. from the last round are inverse of theinitial

- The right-hand portion of the figure shows the way in which the 56-bit key is used.
  - Initially, the key is passed through a permutation function.
  - Then, a sub key (k_i) is produces for each of the sixteen rounds by the combination of a left circularshift and a permutation.
  - The permutation function is the same for each round, but a different sub key is produced becauseof the repeated shifts of the key bits.

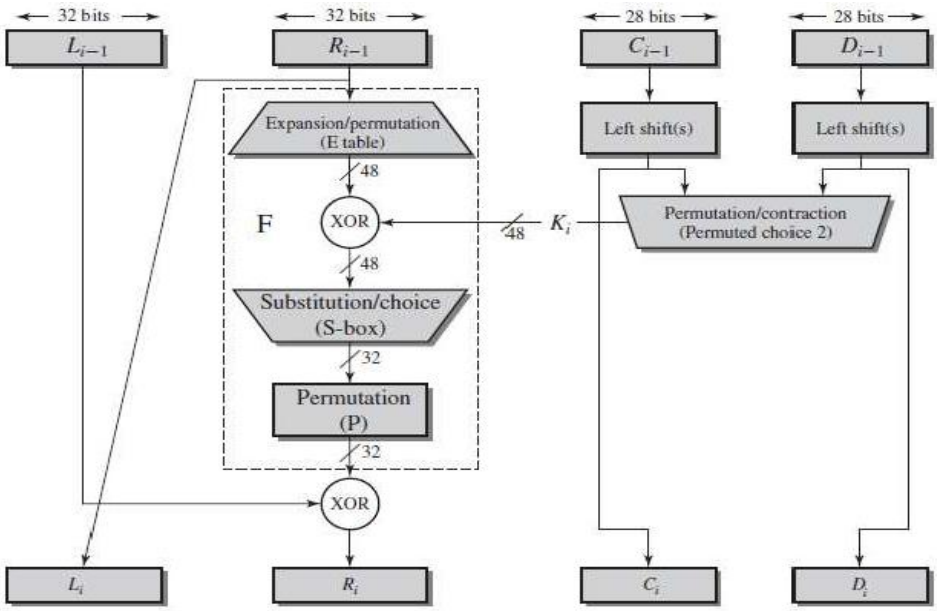
IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-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

Initial Permutation (IP) and Inverse Initial Permutation (IP^{-1})

- The initial permutation and its inverse are defined by tables.
- The tables are to be interpreted as follows.
  - The input to a table consists of 64 bits numbered from 1 to 64.
  - The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64.
  - Each entry in the permutation table indicates the position of a input bit in the output.
- Inverse permutation table nullifies the effect of initial permutation.

Details of Single Round



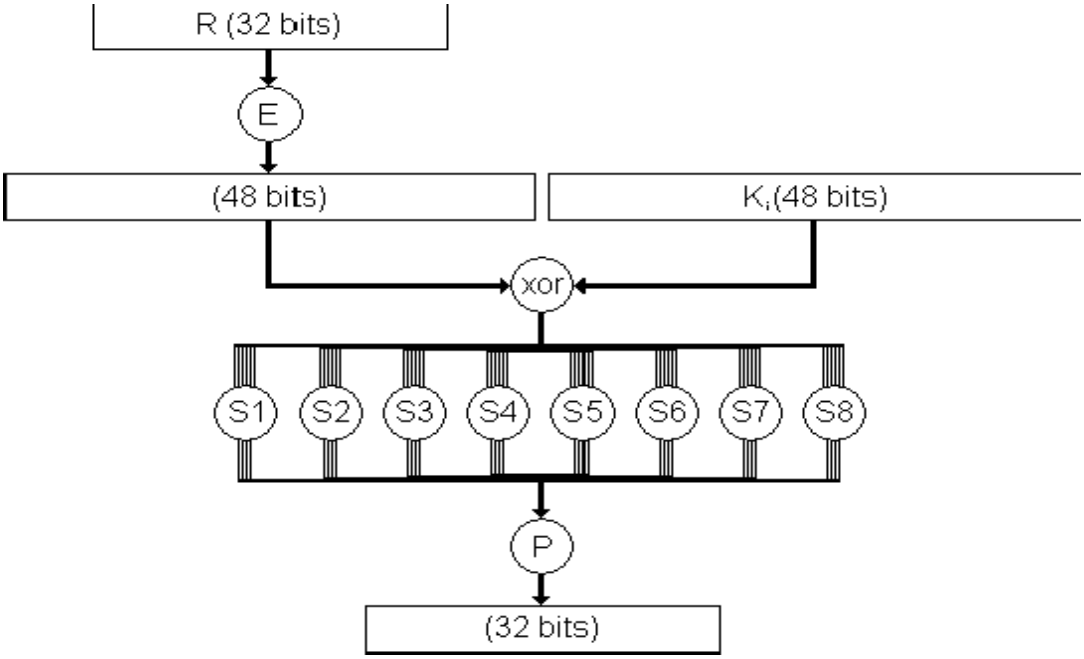
- Figure shows the internal structure of a single round.
- The left and right halves are treated as separate 32-bit quantities, labeled L (left) and R (right).
- The overall processing at each round can be summarized as:

  $L_i = R_{i-1}$

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

Expansion (E)

- The 32-bit input is first expanded to 48 bits.
  - Bits of input are split into groups of 4 bits.



- Each group is written as groups of 6 bits by taking the outer bits from theexample wo adjacent groups. For

... efgh ijkl mnop ... is expanded to

... defghi hijklmnl nopq ...

32	01	02	03	04	05
04	05	06	07	08	09
08	09	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	31	31	32	01

- The resulting 48 bits are XORed with K_i.

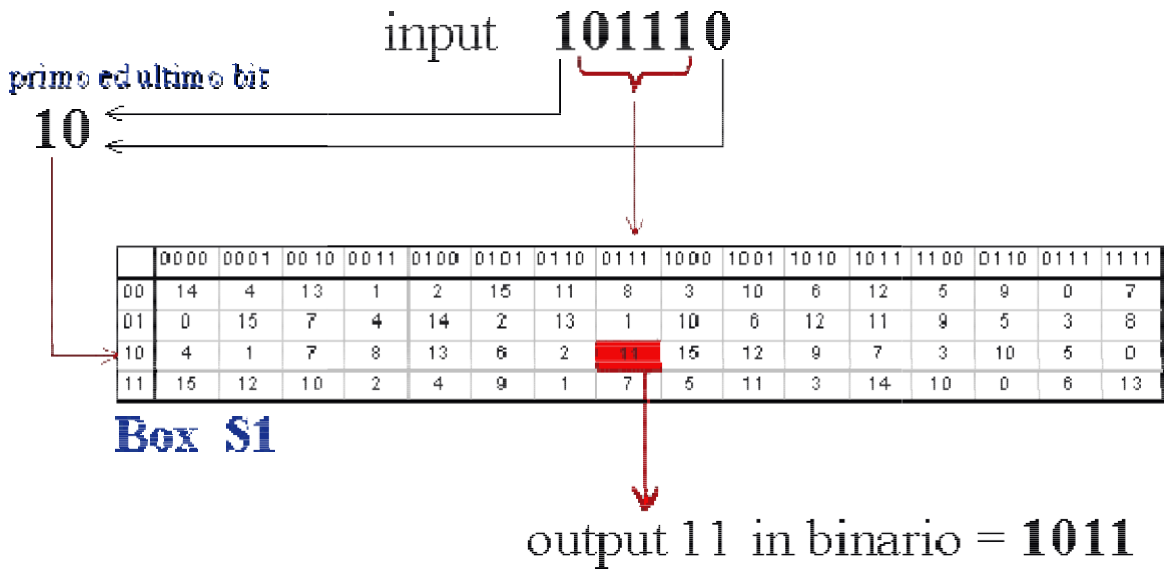
Substitution (S-Box)

- This 48-bit result is input tooutput.

S-Boxes that perform a substitution on input and produces a 32-bit

- It is easy to understand S-Box by following figure.

- DES consists of a set of eight S-boxes.
- Each S-Box takes 6 bits as input and produces 4 bits as output.
- The first and last bits of the input to box form a 2-bit binary number which gives the binary value ofrow number.
- The middle four bits select one of the sixteen columns.
- The decimal value in the cell selected by the row and column is then converted to its 4-bit binarynumber to produce the output.
- For example, in S1, for input 101110, the row is 10 (row 2) and the column is 0111 (column 7).Thevalue in row 2, column 7 is 11, so the output is 1011.



	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	0110	0111	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	7	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	10	2	4	9	1	7	5	11	3	14	10	0	6	13

- **Permutation (P)**

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

- The result is again permuted using a permutation table.

Key Generation

- A 64-bit key is used as input to the algorithm while only 56 bits are actually used. Every eighth bit isignored. Sub-keys at each round are generated as given below:
  - The key is first permuted using a table named Permuted Choice One.

- The resulting 56-bit key is divided into two 28-bit quantities, C_0 and D_0. At each round, C_{i-1} and D_{i-1} are separately subjected to a circular left shift of 1 or 2 bits, as governed by a table.
- These shifted values are forwarded to the next round. They are also input to a permutation table-Permuted Choice Two.
- The table produces a 48-bit output that serves as the round key k_i.

(a) Input Key

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

(b) Permuted Choice One (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

(c) Permuted Choice Two (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

(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES Decryption

- Decryption in DES is same as encryption, except that the sub keys are used in reverse order.

Strength of DES

The Use of 56-Bit Keys

- DES has been developed from LUCIFER which used 128-bit keys.
- As a result, DES with only 56-bit key-length is considered insecure and devices have been proposedtime and again showing that DES is no longer secure.

The Nature of the DES

- The only non-linear part of DES is the S-Boxes, design of which was not made public.
- If someone is able to find weakness in S-Box, then attack on DES is possible.
- Characteristics of the algorithm can be exploited as the algorithm is based on linear functions.

Algorithm Timing Attacks

- In this type of attack, the attacker exploits the fact that any algorithm takes different amount of timefor different data.

A DES Example

Let see example of DES and consider some of its implications. Although you are not expected to duplicate the example by hand, you will find it informative to study the hex patterns that occure fromone step to the next.

Plaintext:	02468aceeca86420
Key:	0f1571c947d9e859
Ciphertext:	Da02ce3a89ecac3b

- **Result:** Above table shows plain text, key and cipher text when we apply all the steps of DES we will getcipher text as shown.
- **The Avalanche Effect:** A desirable property of any encryption algorithm is that a small change in eitherthe plaintext or the key should produce a significant change in cipher text.
- In particular, a change in one bit of plaintext or one bit of the key should produce a change in many bitsof the ciphertext. This is referred to as the avalanche effect.
- In DES 1 bit change in input will affect nearly 32 bit of output after all rounds.

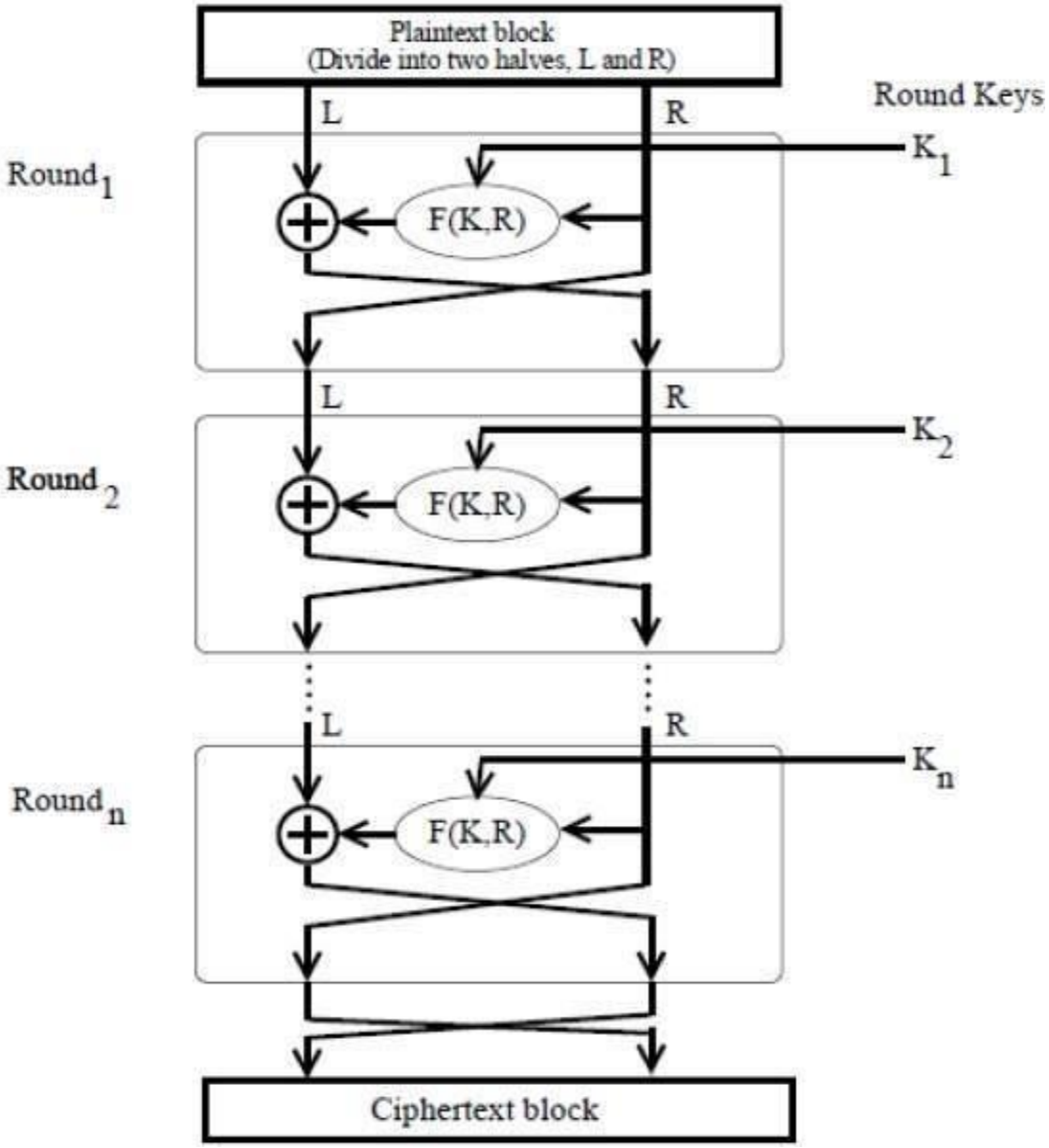
❖ Feistel Block Cipher

Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.

Encryption Process

The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.

Feistel Structure is shown in the following illustration −


Plaintext block
(Divide into two halves, L and R)
Round Keys
L
R
Round 1
K1
F(K,R)
L
R
Round 2
K2
F(K,R)
L
R
Round n
Kn
F(K,R)
Ciphertext block

- The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- 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 input − the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
- 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 subkey) 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.
- 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 be the output L of the current round.
- Above substitution and permutation steps form a 'round'. The number of rounds are specified by the algorithm design.
- Once the last round is completed then the two sub blocks, 'R' and 'L' are concatenated in this order to form the ciphertext block.

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 that are beyond the scope of our discussion.

Decryption Process

The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext 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 subkeys 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. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.