UNIT-I

Cryptography & Network Security (Jawaharlal Nehru Technological University, Hyderabad)

Network Security

Introduction :-

Computer data often travels from one computer to another, leaving the safety of its protected physical sorroundings. Once the data is out of hand, people with bad intension could modify or forge your data for their own benefit.

The OSI security architecture provides a systematic frame work for defining security attacks, mechanisms and services.

Computer security :- generic name for the collection of tools designed to protect data and to thwart (prevent) hackers.
Ex:- Anti Virus

Network Security :- measures to protect data during their transmission. Ex:- Firewalls.

Internet security :- measures to protect data during their transmission over a collection of interconnected networks.
Ex:- Bank transactions.

To assess the Security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy these requirements.

One approach is to consider three aspects of information security, The ITU recommendation X.800, Security Architecture for OSI. It focuses on the following.

Security attack :-

Any action that comprises the security of information owned by an organization.

Security mechanism:-

A mechanism that is designed to detect, prevent or recover from a security attack.

Security service :-

A service that enhances the security of the data processing systems and the information transfers of an organization.

Basic concepts:-

Cryptography:-

To provide the security and protect the valuable information we can use cryptography.

The art of protecting the information by transforming it into an unreadable format is called cryptography.
(intelligible message into one that is unintelligible).

plaintext:- The original intelligible message.

Ciphertext:- The transformed message/encrypted text.

Cipher:- An algorithm for transforming an intelligible message into one that is unintelligible by transposition and / or substitution methods.

Key :- A string of bits used by a cryptographic algorithm, known only to the sender & receiver.

Encipher (encode) :- The process of converting plaintext to ciphertext using a cipher and a key.

Decipher (decode) :- the process of converting cipher text back into plaintext using a cipher and a key.

Cryptanalysis :-
The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called Code breaking.

* The basic intention of an attacker is to break a cryptosystem & to find the P.T from the C.T.

Security Attacks :-

our goals of security - confidentiality, integrity and ~~available~~ availability - can be threatened by security attacks.

They are classifing into two types. 1) passive attacks
2) Active attacks.

Security attacks.

passive attacks. { Snooping, Traffic analysis.

Threat to confidentiality.
(To protect the data from unauthorised users, it is a part of n/w security)

active attacks { Modification, Masquerading, Replaying, Repudiation.

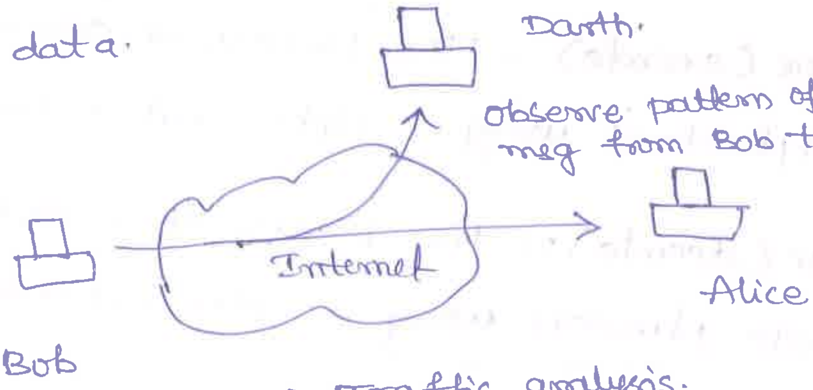
Threat to integrity. It means (that changes need to be done only be authorized entities & through authorized mechanisms).

Denial of Service.

Threat to availability.
(The data, n/w resources are continuously available to legitimate users).

(1) In general, 2 types of attacks threaten the confidentiality of information: snooping & Traffic analysis

1 (a)
* snooping refers to unauthorized access to or interception of data.



a) Traffic analysis.

* passive attacks are very difficult to detect, because they don't involve any alteration of data.

(2) The integrity of data can be threatened by several kinds of attacks :

* Modification of msgs:- After accessing information, the attacker modifies the information to make it beneficial to herself. ex:- bank transactions.

* Masquerading :- ~~The~~ attacker impersonates somebody else. ex:- an attacker might steal the bank card and PIN of a bank customer and pretend that she is that customer.

* Replaying :- The attacker obtains a copy of a msg sent by a user and later tries to replay it.

(3) * Denial of service:- It is a very common attack. It may slow down or totally interrupt the service of a system.

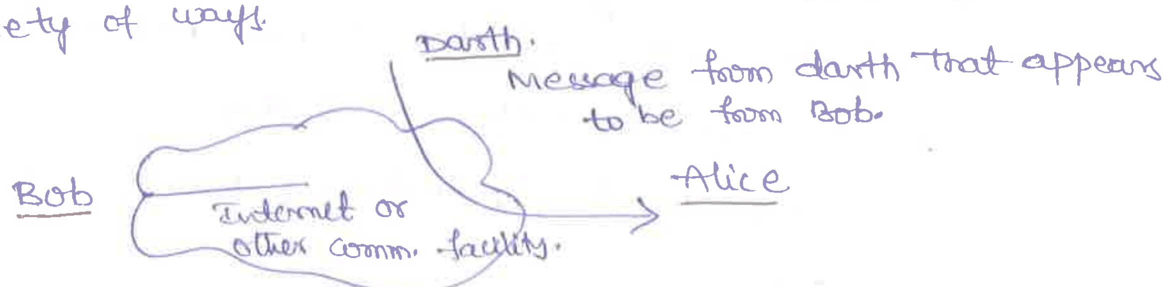
1 (b) Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

category of passive and attack active.

Attacks	passive / Active	Threatening
Snooping Traffic Analysis.	passive	confidentiality
Modification Masquerading Replaying. Repudiation	Active	Integrity.
Denial of Service.	Active	Availability.

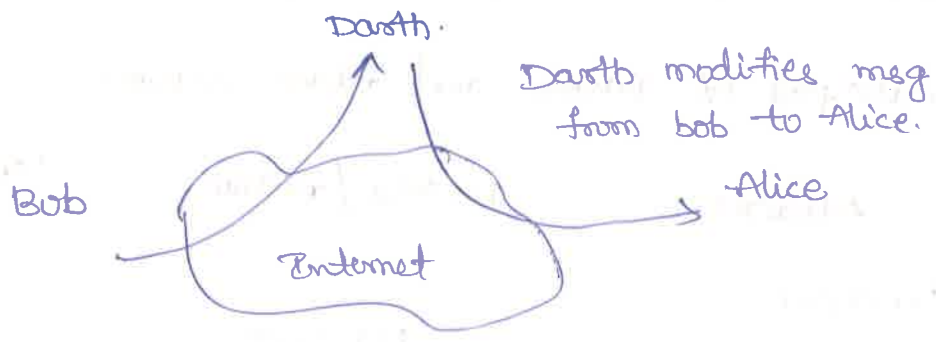
* In a passive attacks, the attacker's goal is just to obtain information. i.e The attack does not modify data or harm the system.

* An active attacks may change the data or harm the system. Active attacks are normally easier to detect than to prevent, because an attacker can launch them in a variety of ways.

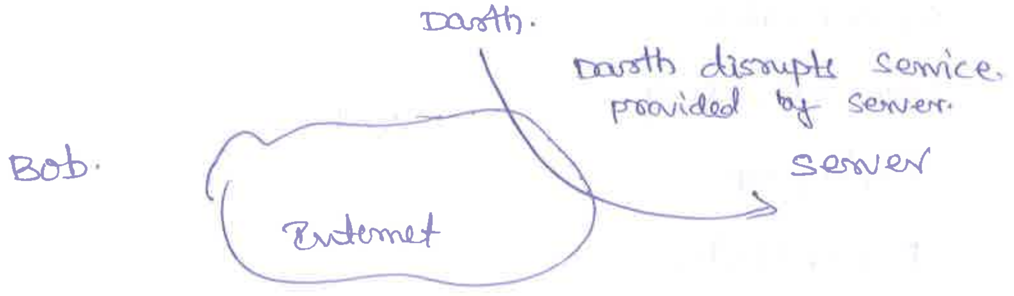


a) Masquerade.

b) Replay



c) modification of messages.



d) Denial of service.

Services and Mechanisms :-

The International Telecommunication Union - Telecommunication standardization Sector (ITU-T) provides some security services and mechanisms.

Security services :-

The classification of security services are as follows:

1) confidentiality :- Ensures that the information in a computer system and transmitted information are accessible for reading by authorized parties.

Eg: printing, displaying and other forms of disclosure

(or)

is the protection of transmitted data from passive attacks.

Authentication :- Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Data Integrity :- Ensures that only authorized parties are able to modify computer system assets and transmitted information.

Non repudiation :- Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control :- Requires that access to information resources may be controlled by or the target system.

Availability :- Requires that computer system assets be available to authorized parties when needed.

Security services (X.800) :-

1) Authentication :- The assurance that the communicating entity is the one that it claims to be.

* peer Entity Authentication :- Used in association with a logical connection to provide confidence in the identity of the entities connected.

* Data origin Authentication :- In a connectionless transfer provides assurance that the source of received data is as claimed.

2) Access control :- The prevention of unauthorized use of a resource.

3) Data Confidentiality :- The protection of data from unauthorized disclosure.

* Connection confidentiality :-
The protection of all user data on a connection.

* Connectionless confidentiality :-
The protection of all user data in a single data block.

* Selective field confidentiality :-
The confidentiality of selected fields within the user data on a connection or in a single data block.

* Traffic flow confidentiality :-
The protection of the information that might be derived from observation of traffic flows.

4) Data Integrity :-
The assurance that data received are exactly as sent by an authorised entity. i.e no modification, insertion, deletion or replay.

* Connection Integrity with Recovery
provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

* Connection Integrity without Recovery :-
As above, but provides only deletion without recovery.

* Selective - Field Connection Integrity.
* Connectionless Integrity
* Selective - Field Connectionless Integrity.

(5) Nonrepudiation

provides protection against denial by one of the entities in a communication of having participated in all or part of the communication.

Nonrepudiation, origin:- proof that the msg was sent by the specified party.

Nonrepudiation, Destination:- proof that the msg was received by the specified party.

Security Mechanisms:- (X.800)

ITU-T(X.800) also recommends some security mechanisms to provide the security services defined above. (i.e OSI security services).

1. Encipherment :- The use of mathematical algorithms to transform data into a form that is not readialy intelligible. The ~~transformation~~ & subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

2. Digital signature:-

A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

3. Access control:-

Access control :- A variety of mechanisms that enforce access rights to resources.

Data Integrity :- (Accuracy & consistency)
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange :- A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic padding :- The insertion of bits into gaps in a data stream.

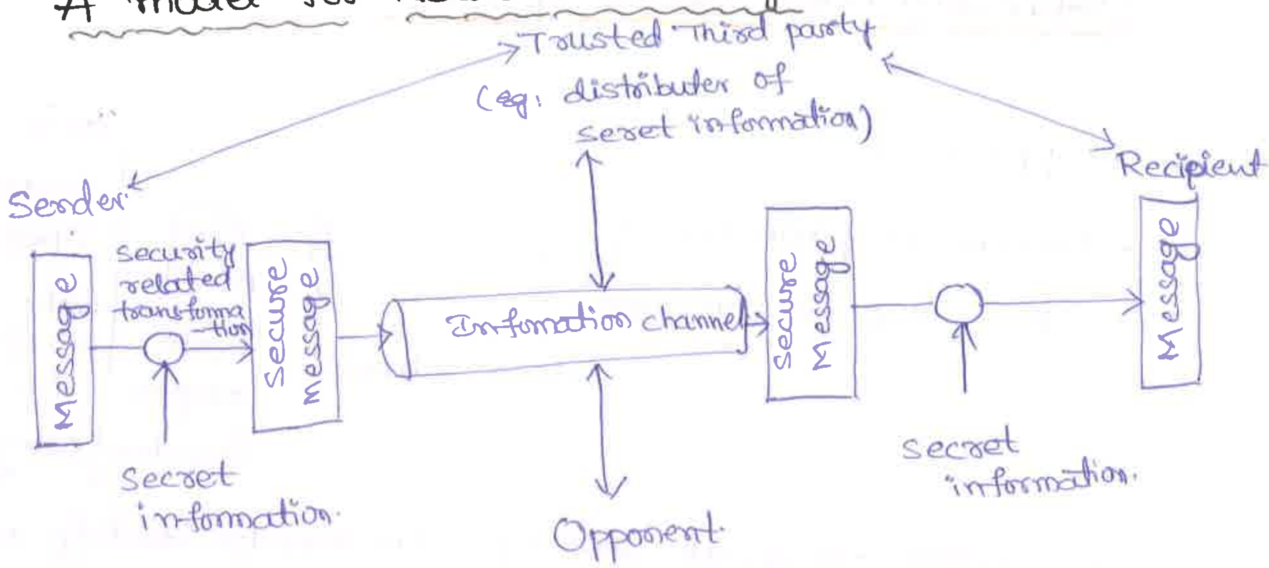
Routing control :- Enables selection of particular physically secure routes for certain data & allows routing changes

Notarization :- The use of a trusted 3rd party to assure certain properties of a data exchange.

* Relation b/n Security Services and Mechanisms.

Service	Encipherment	Digital sign.	Access control	Data Integrity.	Authentication exchange	Traffic padding	RC	N
peers Entity Authentication	Y	Y			Y			
Data origin "	Y	Y						
Access control			Y					
confidentiality	Y						Y	
Traffic flow	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y.
Availability.				Y	Y			

A model for Network Security :-



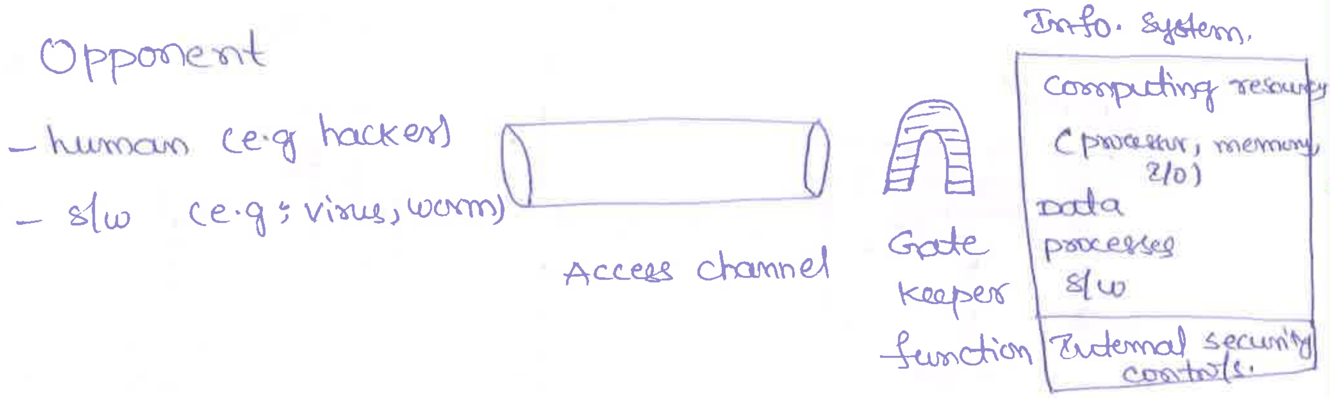
A msg is to be transferred from one party to another across some sort of internet. The 2 parties, who are the principals in this transaction, must cooperate for the exchange to take place.

A logical information channel is established by defining a route through internet from source to destination and by the cooperative use of communication protocols by the two principals.
(eg. TCP/IP)

Using this model requires us to:

* design a suitable algorithm for security transformation.
* generate the secret information (keys) used by the algorithm.
* develop methods to distribute & share the secret information
* specify a protocol enabling the principals to use the transformation and secret information for a security service.

Network Access Security model:-



* select appropriate gatekeeper functions to identify users.
* Implement security controls to ensure only authorized users access designated information or resources.
* Trusted computer systems can be used to implement this model.

Conventional Encryption :- (Symmetric Cipher Model)

It is a cryptographic system that uses the same key used by the Sender & Rx'r.

A symmetric encryption scheme has five ingredients.

plaintext :- This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm :- It performs various substitutions and transformations on the plaintext.

Secret Key :- It is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm.

Cipher text :- This is the scrambled msg produced as output. It depends on the plaintext and the secret key. It is an apparently random stream of data (i.e unintelligible).

Decryption algorithm :- This is essentially the encryption algorithm run in reverse. It takes ciphertext & the secret key and produces the original plaintext.

cryptanalysis (code breaking) :- the study of principles/methods of deciphering cipher text without knowing key.

cryptology :- The field of both cryptography and cryptanalysis.

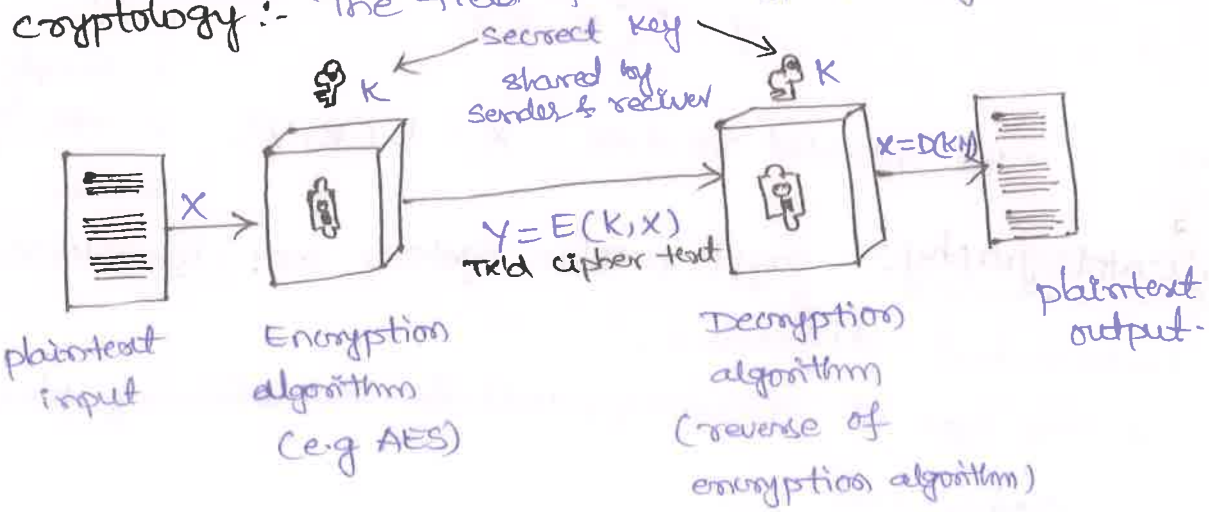


fig: Conventional Encryption Model

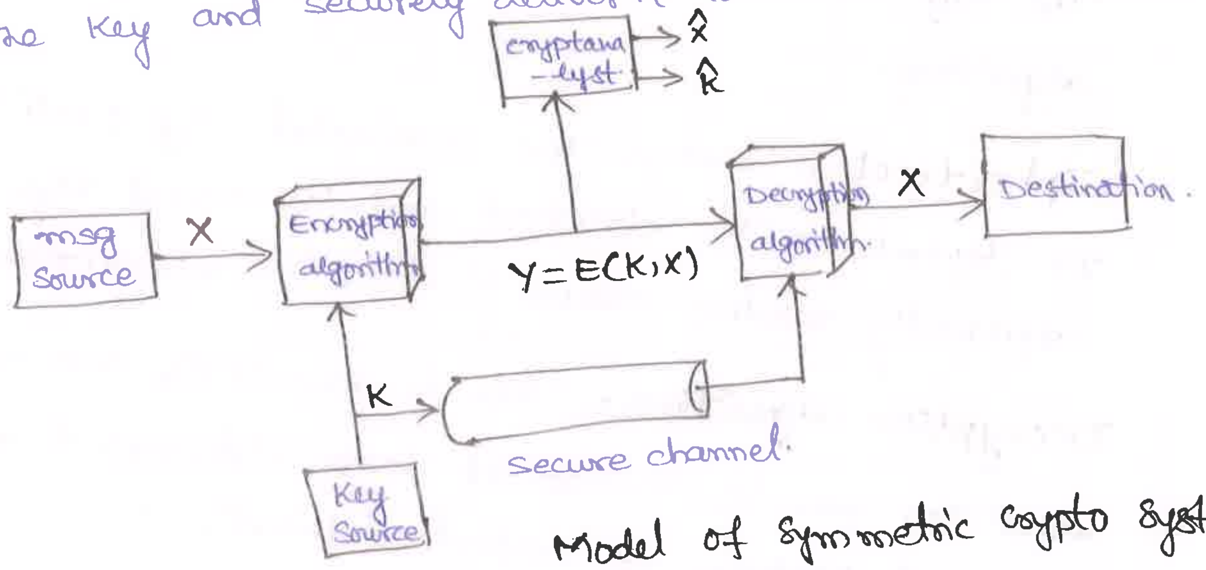
Two requirements of secure use of symmetric encryption:-

1) A strong encryption algorithm

2) A secret key only known to sender/Receiver.

A source produces a message in plain-text, $X = [X_1, X_2, \cdots X_M]$. The M elements of X are in some finite alphabet.

For encryption, a key of the form $K = [K_1, K_2, \ldots K_J]$ is generated. Alternatively, a third party could generate the key and securely deliver it to both source and destination.



Model of symmetric crypto system.

With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext $Y = [Y_1, Y_2, \cdots Y_N]$.

$\therefore Y = E(K, X)$.

The intended receiver $X = D(K, Y)$.

Advantages:-

1. Simple
2. uses fewer computer resources
3. Fast

Cryptography:- cryptographic systems are characterized along 3 independent dimensions.

1) The type of operations used for transforming plain text to cipher text.

2) The number of keys used.

3) The way in which the plaintext is processed.

Classical encryption Techniques:-

There are two basic building blocks of all encryption techniques: 1) Substitution 2) Transposition.

Substitution Techniques:-

In which the letters of plaintext are replaced by other letters or numbers or symbols. If the plain text is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

1) Caesar Cipher :- (shift cipher) :-

which involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

Ex:- plain :- meet me after the toga party

cipher :- PHHW PH DIWHU WKH WRJD SDUWB.

plain :- a b c d . . . . w x y z.

cipher :- D E F G . . . . Z A B C.

with numerical equivalent :-

a	b	c	d	. . . . .	x	y	z
0	1	2	3	. . . . .	23	24	25

Then the algorithm can be expressed as follows:

for each plain-text letter 'p', substitute the cipher text letter, C.

$$C = E(3, P) = (P+3) \bmod 26.$$

The general Caesar algorithm is :

$$C = E(K, P) = (P+K) \bmod 26. \quad K = 1 \text{ to } 25.$$

The decryption algorithm is

$$P = D(K, C) = (C-K) \bmod 26.$$

Play-fair cipher:-

The best known multiple-letter encryption Cipher is the play-fair, which treats diagrams in the plaintext as single units and translates these units into ciphertext diagrams.

The playfair algorithm is based on the use of 5X5 matrix of letters constructed using a keyword.

Ex:. Let The Keyword be "MONARCHY". The matrix is constructed by filling in the letters of keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.

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

① Hello

② balloon

ba ll oo n

ba lx lo on.

Rules for E

1. Digrams
2. Repeating letters - Filler letter
3. Same column |↓| wrap around
4. Same row |→| wrap around
5. Rectangle |⇆| swap

Ex: P.T → attack.
Digrams:- at ta ck
C.T →

① Repeating plaintext letters that are in the same pair are seperated with a filler letter, such as 'x'

Ex:- 'balloon' would be treated as 'ba lx lo on'.

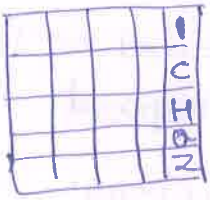
② Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.

Ex:- AR is encrypted as: RM

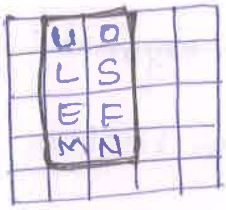
| D | E | F | G | |

→ EF

Strength of playfair Cipher : since there are 26 letters, 26 X 26 = 676 diagrams are possible, so identification of individual diagrams is more difficult.

(3) 

H & I are in same column, hence take letter below Them to replace:- HI → QC.

(4) 

M & O → NU. (opposite corner).

Ex:- plaintext : instruments. Keyword: monarch

After split :- in st ru me nt sz

C.T:- ga tl mz cl rq tx.

Monoalphabetic and Polyalphabetic Cipher :-

↳ It is a substitution cipher in which for a given key, The cipher alphabet for each plain alphabet is fixed Through -out the encryption process.

-for ex:-, if 'A' is encrypted as 'D': for any number of occurrence in That plaintext, 'A' will always get encrypted to 'D'

Polyalphabetic cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during The encryption process.

ex:- play-fair & Vigenere cipher are polyaphabetic.

Vigenere cipher :-

This scheme of cipher uses a text string (a word). as a key, which is Then used for doing a number of shifts on the plaintext.

Key:- deceptivedeceptive deceptive

P.T:- we are discovered save yourself

C.T:- ZICVTWQNGRZGVTW

key	3	4	2	4	15	19	8	21	4
PT	22	4	0	17	4	3	8	18	2
CT	25	8	2	21	19	22	16	13	6

Ex:- let us assume the key is 'point'. Each alphabet of the key is converted to its respective numeric value

i.e: $p \rightarrow 16,\ o \rightarrow 15,\ i \rightarrow 9,\ n \rightarrow 14,\ t \rightarrow 20$.

Thus the key is: 16 15 9 14 20.

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

Vernam Cipher:- This works on binary data rather than letters. In this a cryptanalysis is choose a keyword that is as long as the plaintext & has no stastical relationship to it.

* It is introduced by an AT&T engineer named Gilbert Vernam in 1918.

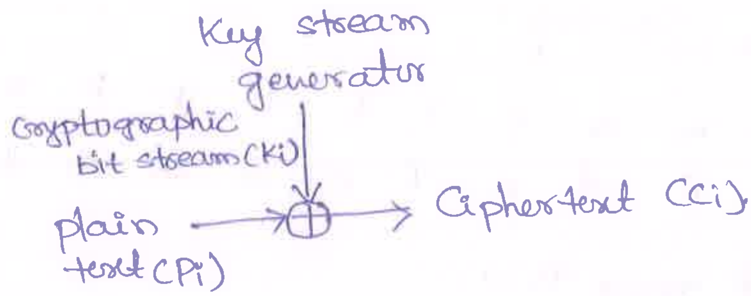
It can be expressed $C_i = P_i \oplus K_i$

P_i = ith binary digit of plaintext

K_i = ith " key

C_i = ith " ciphertext.

$P_i = C_i \oplus K_i$.



One-Time Pad:-

It is an unbreakable crypto system. It represents the message as a sequence of 0's and 1's. This can be accomplished by writing all numbers in binary. The key is a random sequence of 0's and 1's of same length as the message.

* once a key is used, it is discarded and never used again. (i.e each new msg requires a new key of the same length).

This system can be expressed as:

$$C_i = P_i \oplus K_i$$

Transposition Techniques:-

All the techniques studied so far involve the substitution of a ciphertext symbol for a plaintext symbol.

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This is referred to as a transposition cipher.

rail fence:-

It is the simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Ex:- plain text :- meet me after the toga party".

we write the following :

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

The encrypted msg is:-

MEMATRHTGPRYETEFETEOAAT

Row Transposition ciphers:-

Key :-	4	3	1	2	5	6	7
Input :	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	m	l	y	p	e	t	z

output:- NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

Steganography :-

A plaintext msg may be hidden in one of two ways. The methods of steganography conceal the existence of the msg. It is time-consuming to construct.

Various techniques:-

1) character marking :- selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at angle to bright light.

2) Invisible Ink :- no visible trace until heat or some chemical is applied to the paper.

3) Pin punctures :- small pin punctures on selected letters

4) Typewriter correction ribbon:

Drawbacks :- requires a lot of overhead to hide a relatively few bits of information.

BLOCK CIPHERS :-

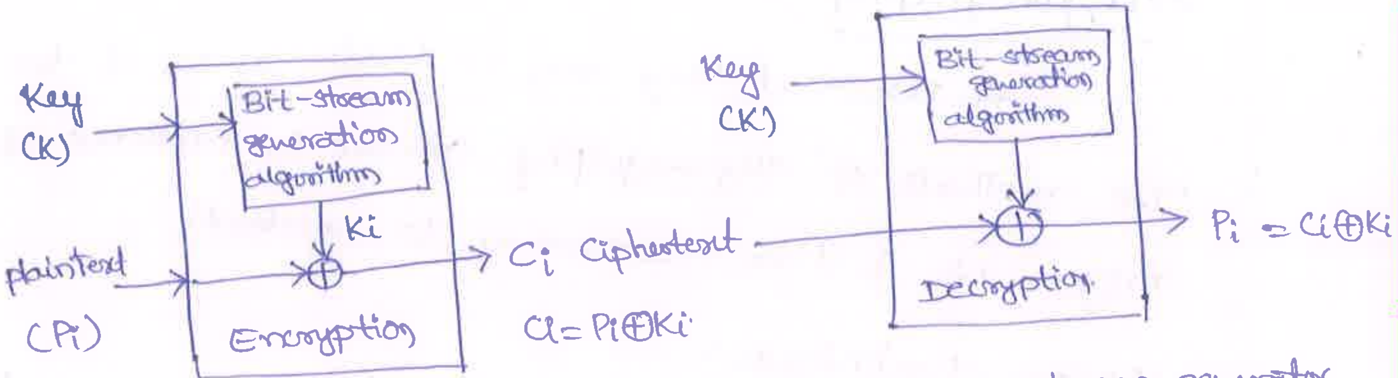
Many symmetric block encryption algorithms in current use are based on a structure referred to as a 'Feistel block cipher'.

* A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. Ex:- streaming of data / video

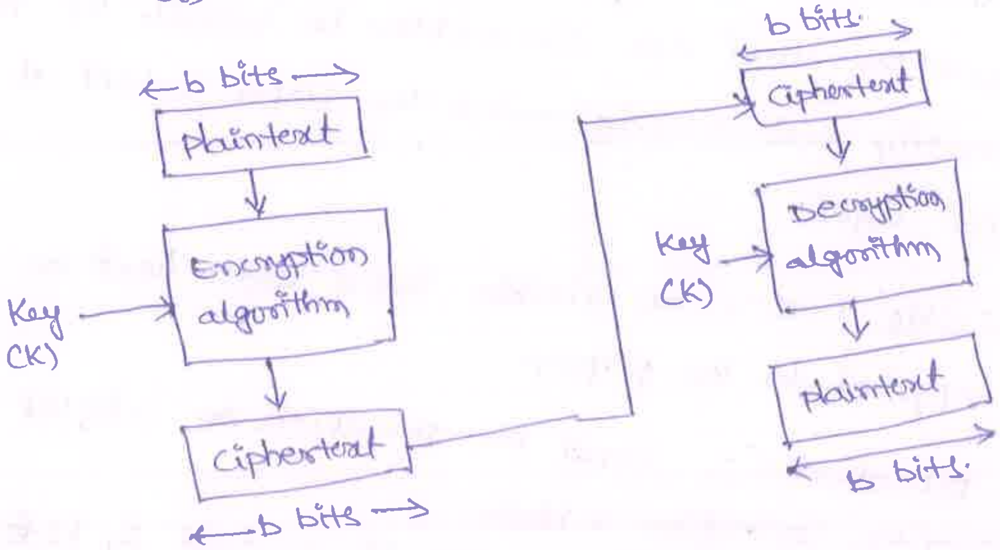
* A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. typically, a block size of 64 or 128 bits is used.

(Information ~~broken~~ broken down to blocks of fixed size)

* size of blocks depends on key size.



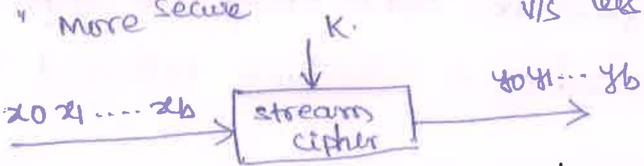
a) stream cipher using algorithmic bit-stream generator



Ex:- DES

b) Block cipher. (Blocks of size:. 40, 56, 64, 80, 128, 168, 192 and 256).

* Block high diffusion v/s stream low diffusion
* Block slow encryption v/s stream fast encryption.
* " high error propagation v/s. low error propagation.
* " More secure v/s less secure



Ex:- One time pad cipher.

confusion:-
* It is a technique of ensuring that a CT gives no clue about PT. It is used in Block & Stream., Achieved by substitution Technique.

Feistel Cipher Structure :-

① Feistel proposed a scheme to produce a block cipher using permutation and substitution alternatively.

permutation:-
A sequence of plaintext elements is replaced by a permutation of that sequence. (change the position of letter or block).

Substitution:- Each plaintext element or group of elements (block) is uniquely replaced by a corresponding ciphertext element or group of elements.

(2) The inputs to the encryption algorithm are a plaintext block of length 2w bits and a key Ki. The plaintext block is divided into two halves, LE_0 and RE_0.

(3) The two halves of the data pass through rounds of processing and Then combine to produce the ciphertext block.

Working:-

1) A substitution is performed on the left half of the data. This is done by applying a round function F to the right half of the data and then taking the EX-OR of the output of that function and the left half of the data.

2) The round function (F) has the same general structure for each round but is parameterized by the round subkey Ki.

3) permutation is performed that consists of the interchange of the two halves of the data. This structure is a particular form of the substitution - permutation n/w (SPN) proposed by Shannon.

The exact realization of Feistel n/w depends on

1) Block size:- Larger block size mean greater security, but speed ↓.
2) Key size:- larger key size means greater security, but may ↓ E/D speed
3) No. of rounds:- A typical size of 16 rounds.
4) Sub key generation algorithm:- Greater complexity in this lead to greater difficulty of cryptanalysis.
5) Ease of analysis
6) Round function F → greater complexity can make analysis harder.
7) Fast s/w encryption/ decryption-

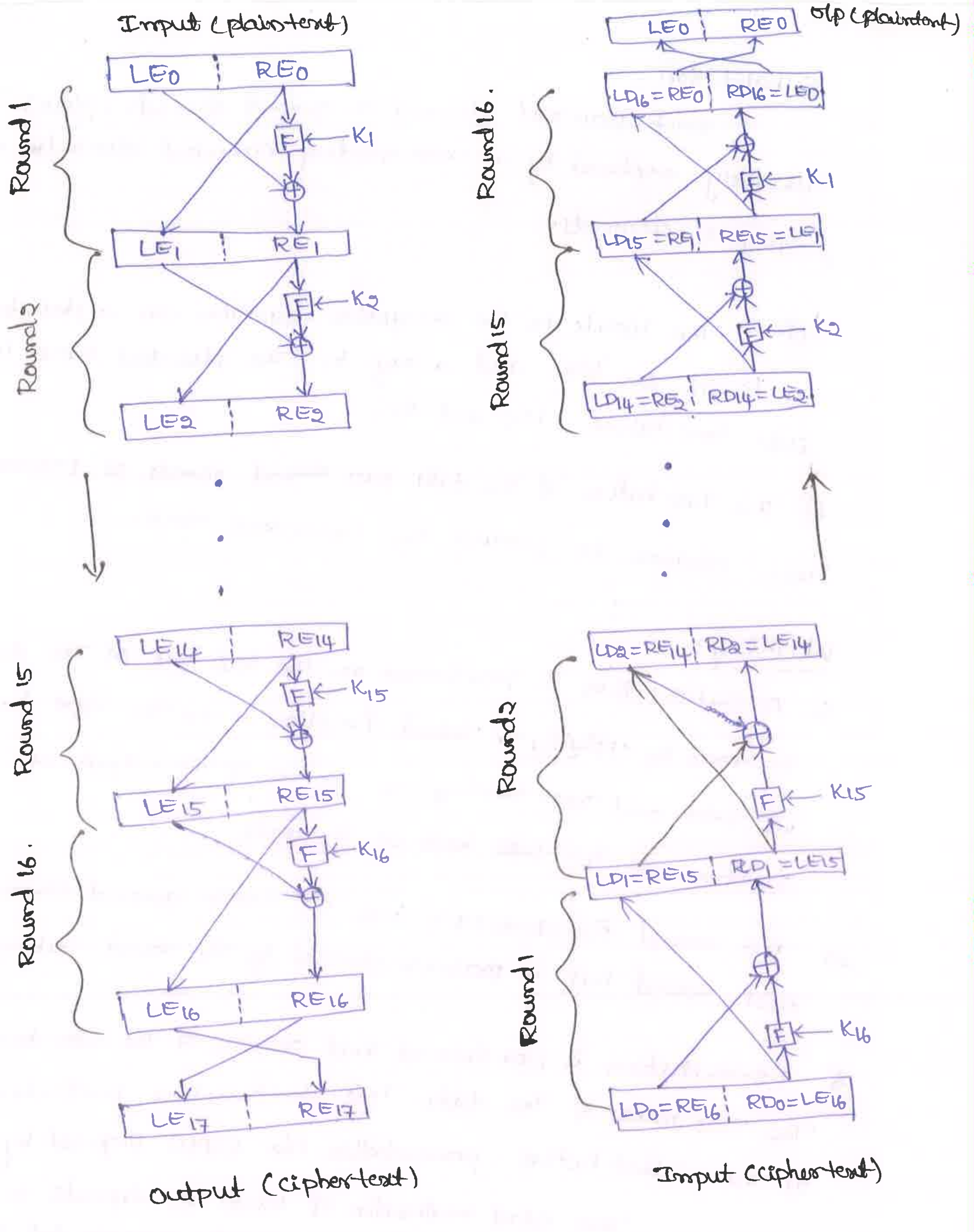


fig :- Feistel encryption and Decryption (16 rounds

Diffusion :- dissipates statistical structure of plaintext over bulk of ciphertext
It is used in block cipher method. It is achieved by permutation

confusion :- makes relationship b/n ciphertext and key as complex as possible

(or) Increases the redundancy of the P.T. by spreading it across rows and columns

Data Encryption standard (DES):-

→ It is a symmetric-key algorithm using block-by-block encryption. (Each block is encrypted individually and they are later changed to ~~format~~ final cipher text)

→ Block size is 64 bits and key size is ~~56~~ bits. (64 bit later converted to 56 bits)
→ No. of sub keys - 16, sub key size - 48 bit.
→ It follows the Feistel cipher structure.

→ The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.

DES Encryption:-

There are two inputs to the encryption function: The plaintext must be 64 bits and the key is 56 bits in length.

The processing of plaintext proceeds in three phases. first

1) The 64 bit plaintext passes through an Initial permutation (IP) that rearranges the bits to produce the permuted input.

2) This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions.

3) Each of these rounds will need keys. Initially we take a 56-bit ~~key~~ cipher key but it is a single key, we pass it on to a Round-key generators, which generates 16 different keys for each single round.

4) These keys are passed on ~~through~~ the rounds as 48-bits. when passing through all these rounds, we reach round 16. By the final key is passed on through the round key generator &

we get a final permutation.

5) In the final permutation the rounds are swapped and we get a final ciphertext.

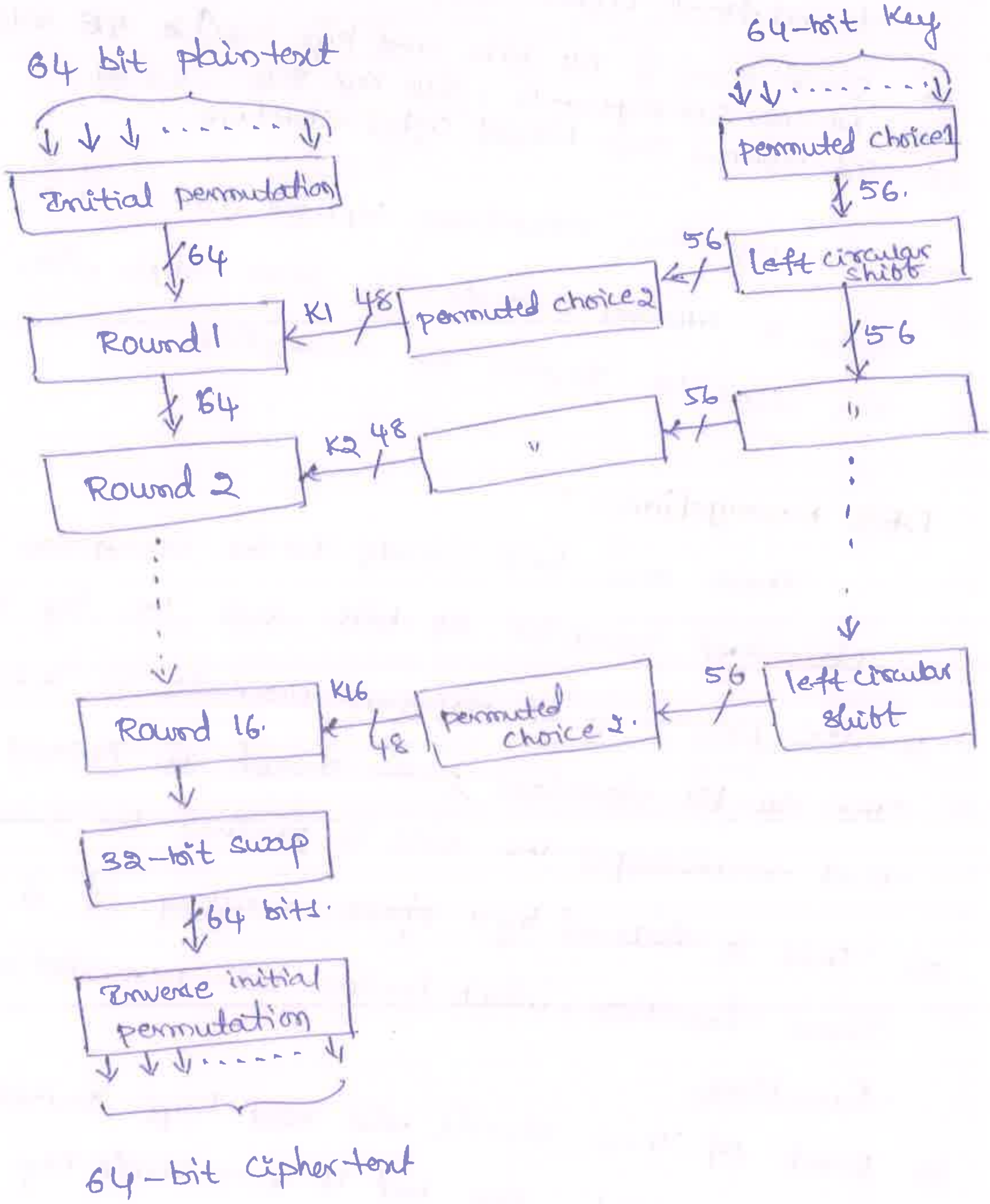


fig:- General Depiction of DES Encryption algorithm

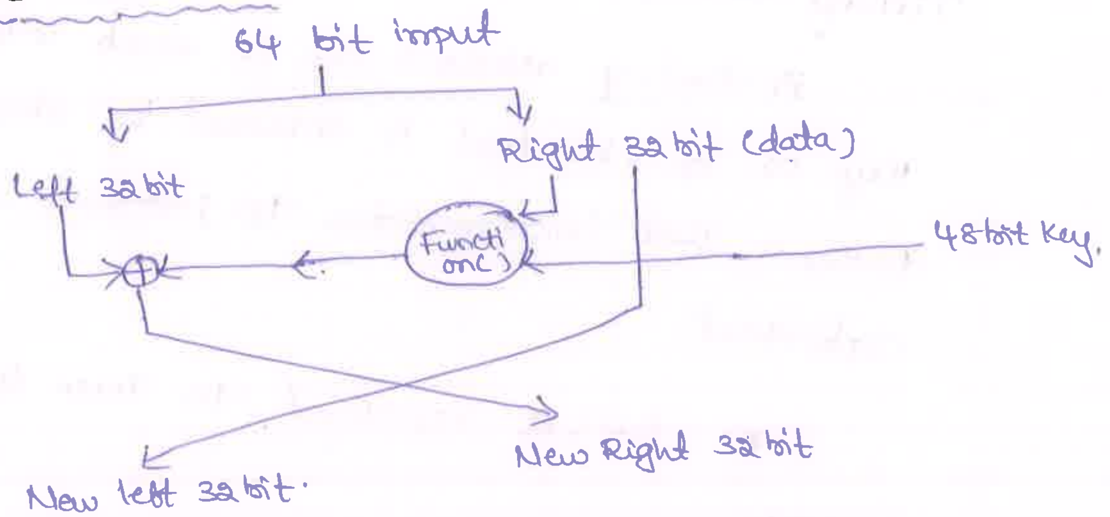
DES Decryption:-

As with any feistel cipher, decryption uses the same algorithm as encryption, except that the application of the sub key is reversed.

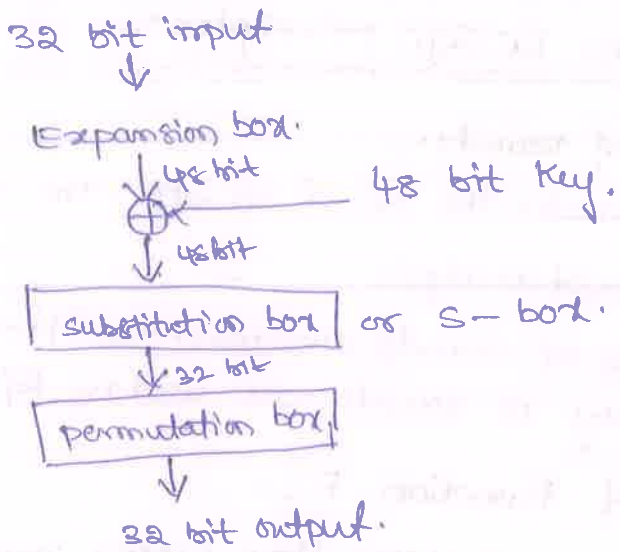
Future of DES:-

1) Replaced by AES in 2002 as the world standard for encryption.
2) 56-bit key size easily broken by new generation computers.
3) withdrawn of support for official purpose in 2005.
4) Triple DES still allowed for important data till 2030.

Ex:- DES - one round.



Function:-



Strength of DES:-

1) The use of 56-bit keys:-
With a keylength of 56 bits, there are $2^{56} = 7 \times 10^{16}$ possible keys. Thus on the face of it, a brute-force attack appears impractical.
→ (Trying all possible keys)

The Nature of DES algorithm:-

1) Another concern is that possibility that cryptanalysis is possible by exploiting the characteristics of The DES algorithm.

2) The focus of concern - Substitution tables, or S-boxes, that are used in each iteration.

Timing attacks:-

A timing attack is one in which information about The key or the plaintext is obtained by observing how long it takes a given implementation to perform decryptions on various ciphertext.

* DES is resistant to these type of timing attacks.

Block Cipher Design principles:-

1) Number of Rounds:-
* The greater the no. of rounds, the more difficult it is to perform cryptanalysis.
* more no. of rounds slowdown the cipher performance.
* Typically 16 rounds are used in E/D.

2) Design of Function F:-
* The function F of The block cipher must be designed such that it must be impossible for any cryptanalysis to unscramble the substitution.
* The criterion that strengthens the function F is it non-linearity.

* more the function F is nonlinear, more it would be difficult to crack it.

* While designing the function F it should be confirmed that it has a good avalanche property, which states that a change in one-bit of input must reflect the change is many bits of output.

3) Key Schedule Algorithm :-

* The key is used to generate one subkey for each round.

* It is suggested that the key schedule should confirm the strict avalanche effect and bit independence criterion.