Jaipur Engineering College & Research Centre, Jaipur
Department of Computer Science & Engineering

Information Security System
[6CS4-03]
Notes

Prepared By:

Kanishk Jain
Ashish Ameria

Assistant Prof., CSE

VISION AND MISSION OF INSTITUTE

VISION

To become renowned centre of outcome based learning and work towards academic, professional, cultural and social enrichments of the lives of individual and communities"

MISSION

M1. Focus on evaluation of learning outcomes and motivate students to inculcate research aptitude by project based learning.

M2. Identify areas of focus and provide platform to gain knowledge and solutions based on informed perception of Indian, regional and global needs.

M3. Offer opportunities for interaction between academia and industry.

M4. Develop human potential to its fullest extent so that intellectually capable and imaginatively gifted leaders can emerge in a range of professions.

VISION AND MISSION OF DEPARTMENT

VISION

To become renowned Centre of excellence in computer science and engineering and make competent engineers & professionals with high ethical values prepared for lifelong learning.

MISSION

M1: To impart outcome based education for emerging technologies in the field of computer science and engineering.

M2: To provide opportunities for interaction between academia and industry.

M3: To provide platform for lifelong learning by accepting the change in technologies

M4: To develop aptitude of fulfilling social responsibilities.

COURSE OUTCOMES

On completion of the course, students will be able to:

CO1: Identify different security attacks, Mechanism, classical and modern encryption techniques.

CO2: Apply random number generation, AES and S-box theory and Implement public key cryptosystem.

CO3: Evaluate message authentication and digital signatures using hash function and IP security.

CO4: Analyze & Implement Water marking technique and strong password protocol in Information Security System.

PROGRAM OUTCOMES (PO)

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis**: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Educational Objectives (PEO)

1. To provide students with the fundamentals of Engineering Sciences with more emphasis in Computer Science & Engineering by way of analyzing and exploiting Engineering challenge

2. To train students with good scientific and engineering knowledge so as to comprehend, analyze, design, and create novel products and solutions for the real life problems.

3. To inculcate professional and ethical attitude, effective communication skills, teamwork skills, multidisciplinary approach, entrepreneurial thinking and an ability to relate engineering issues with social issues.

4. To provide students with an academic environment aware of excellence, leadership, written ethical codes and guidelines, and the self-motivated life-long learning needed for a successful professional career.

5. To prepare students to excel in Industry and Higher education by Educating Students along with High moral values and Knowledge.

MAPPING CO-PO

Cos/POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	2	2	1	1	1	1	1	1	1	3
CO2	3	3	3	3	2	1	1	1	1	2	1	3
CO3	3	3	3	3	2	1	1	2	1	2	1	3
CO4	3	3	3	3	2	2	2	2	1	2	1	3

Program Specific Outcome's (PSO)

PSO1: Ability to interpret and analyze network specific and cyber security issues, automation in real word environment.

PSO2: Ability to Design and Develop Mobile and Web-based applications under realistic constraints.

Syllabus

SN	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	01
2	**Introduction to security attacks:** services and mechanism, classical encryption techniques- substitution ciphers and transposition ciphers, cryptanalysis, stream and block ciphers.	06
3	**Modern block ciphers**: Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation. Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode.	06
4	**Public Key Cryptosystems with Applications:** Requirements and Cryptanalysis, RSA cryptosystem, Rabin cryptosystem, Elgamal cryptosystem, Elliptic curve cryptosystem.	06
5	**Cryptographic Hash Functions, their applications:** Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA). Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers. Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm.	05
6	**Key management and distribution:** symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure. Remote user authentication with symmetric and asymmetric encryption, Kerberos Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH.	04
	Total	28

LECTURE PLAN

JAIPUR ENGINEERING COLLEGE AND RESEARCH CENTRE			
DEPARTMENT OF COMPUTER SCIENCE ENGINEERING			
LECTURE PLAN			
Subject: Information Security System (6CS4-03)		**Year/Sem: III/ VI**	
No. of Lecture Reqd./(Avl.) : 30 / 30			
Semester Starting:	**Semester Ending:**		
Unit No./ Total Lecture Reqd.	**Topics to be Delivered**	**Lect. Reqd.**	**Lect. No.**
Unit-1 (1)	Objective, Scope , Outcome of the course.	1	1
Unit-2 (6)	Introduction to security attacks	1	2
	services and mechanisms	1	3
	Classical encryption techniques	1	4
	substitution ciphers and transposition ciphers,	1	5
	crypt analysis	1	6
	Stream and block ciphers	1	7
Unit 3- (6)	Modern Block Ciphers: Block ciphers structure	1	8
	Data Encryption Standard(DES), Strength of DES	1	9
	Design principle of block cipher	1	10
	AES with Structure, Key Expansion	1	11
	Multiple Encryption and triple DES	1	12
	Cipher Block Chaining Mode, Cipher feedback mode, Counter mode	1	13
BC-1	**IDEA 64 Bit Encryption & MD5 Message Digest Algorithm**	1	14
Unit 4- (6)	Public Key Cryptosystems: Requirements	1	15
	Public Key Cryptosystems: Analysis	1	16
	RSA Cryptosystem	1	17
	Rabin Cryptosystem	1	18
	Elgamal Cryptosystem	1	19
	Elliptic Curve Cryptosystem	1	20
Unit 5- (5)	Cryptographic Hash Functions, Hash Function based on Cipher Block Chaining	1	21
	Secure Hash Algorithm	1	22
	Message Authentication Code	1	23
	MAC based on Hash Function & Block Cipher	1	24
	Digital Signature, Various Digital Signature Schemes, NIST Digital Signature	1	25
BC-2	**IP Security with Strong Password Protocols**	1	26
Unit 6- (4)	Key Management & Distribution, X.509 Certificates	1	27
	Remote User Authentication	1	28
	Web Security Threats, SSL Architecture	1	29
	Transport Layer Security, HTTPs & SSH	1	30
References:			
1) Stalling Williams: Cryptography and Network Security: Principles and Practices, 4th Edition, Pearson Education			
2) Trappe & Washington, Introduction to Cryptography, 2nd Ed. Pearson.			
3) Kaufman Charlie et.al; Network Security: Private Communication in a Public World, 2nd Ed., PHI/Pearson			

Unit-1st ISS - Information Security Attack

Security Attack :- An attack is any attempt to destroy, or gain unauthorized access.

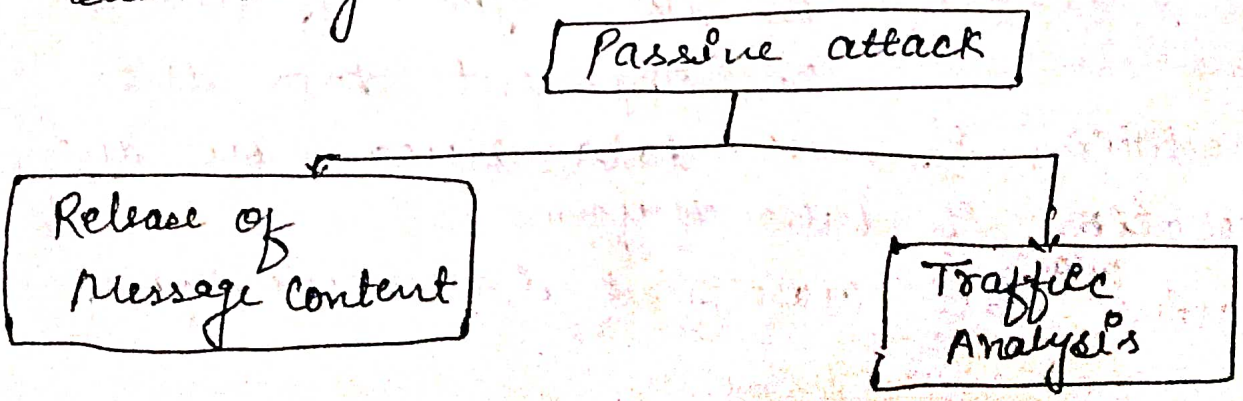
Any action that compromise the security of information owned by an organization is referred to as security attack.

Categorization of attacks is in term of Passive attack & active attack.

1) Passive attack
2) Active Attack

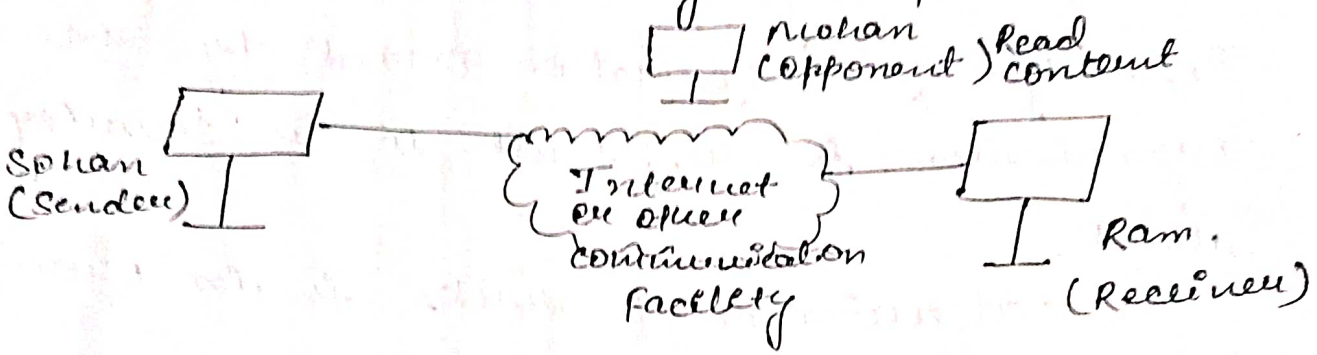
1) **Passive attack :-** Attacks that do not affect the system are called Passive Attack. The term passive attack indicate that the attacker does not attempt to perform any modification to the data.

Classification of Passive attacks into two sub-categories.

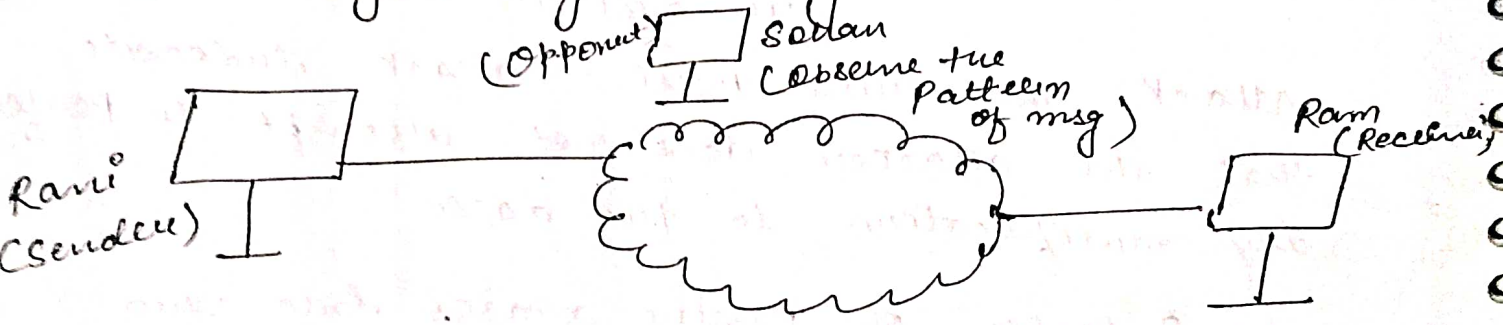


i) Release of Message Contents :- In this opponent try to release or read the contents that is transmitted.

for Example :- A Telephone conversation is recorded or listen by third person.



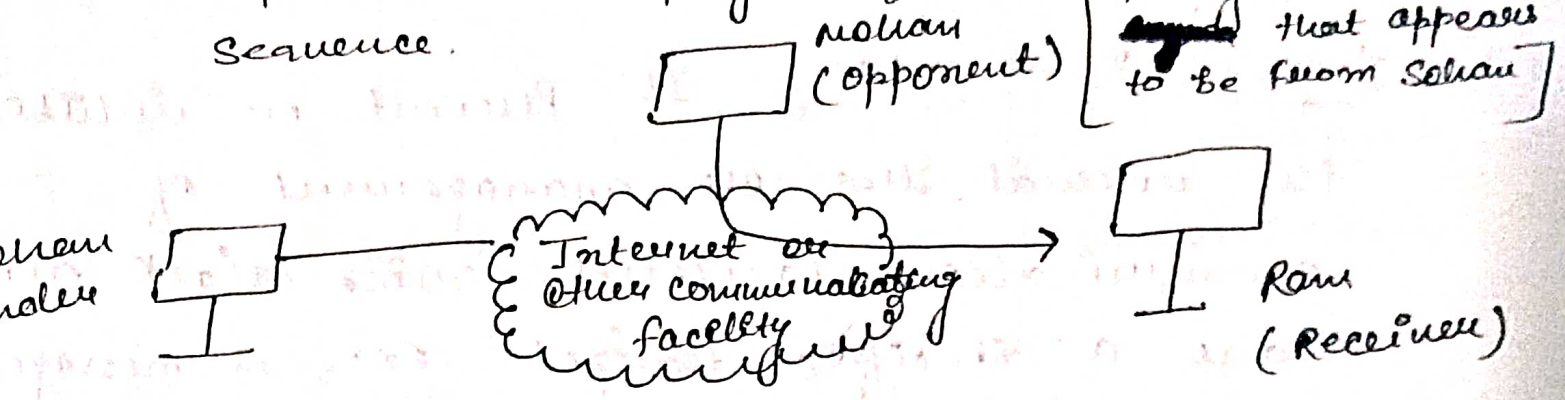
ii) Traffic analysis :- In this the opponent try to analyze and to determine location & identity of communicating host & could observe the frequency and length of message being exchanged.



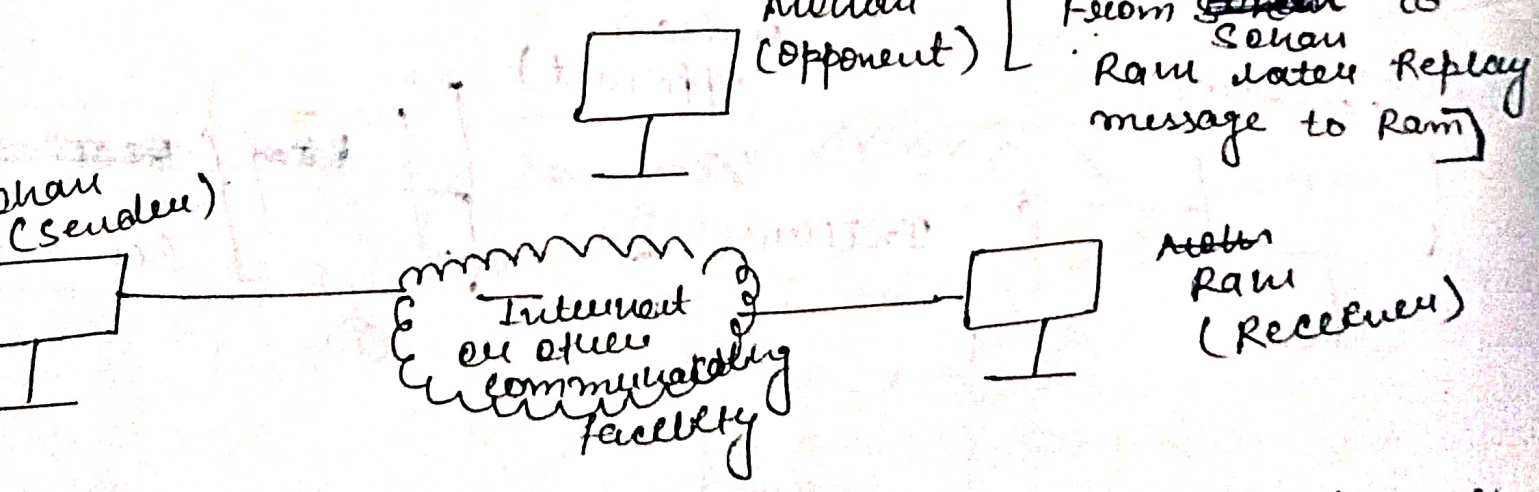
Active Attack :- In this type of attacks the opponent does the modification of the data stream or the creation of false stream.

Active attack are classified in four Types.

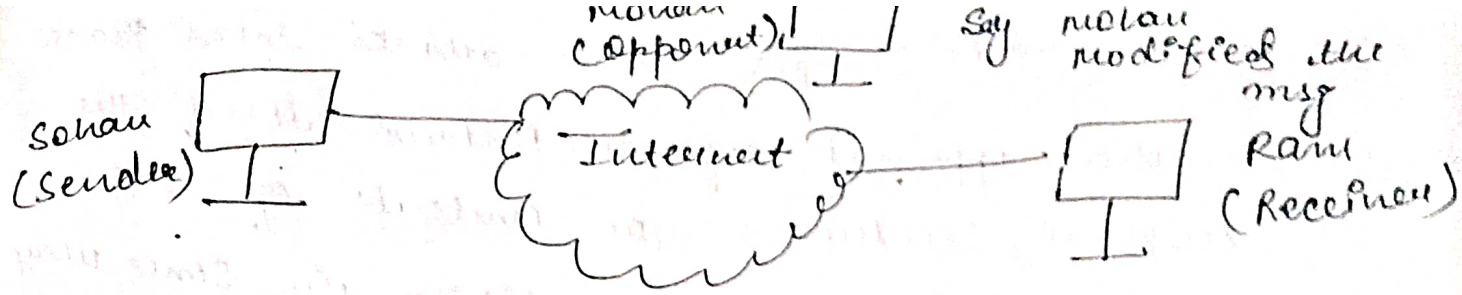
a) **Masquerade** :- This active attacks takes place when opponent try to pretend itself the original sender. & The contents of the original message are modified in some way. for Example. authentication sequence can be captured and replayed after a valid authentication sequence.



b) **Replay** :- It involves the passive capture of a data unit & its subsequent retransmission of captured data to produce an unauthorized effect.

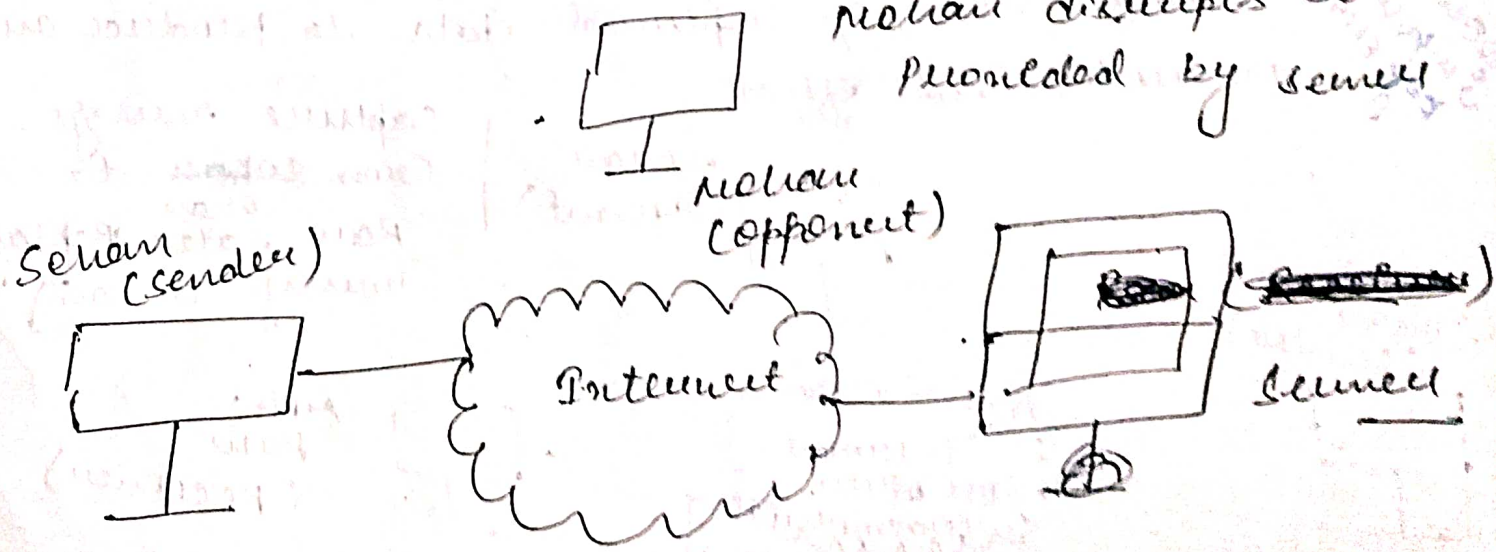


) **Modification** :- It means the some portion of original message is altered, delayed, recorded to produce an unauthorized effect.



Mohan the opponent modifies the message being Transferring b/w Sohan & Ram.

d) Denial of service :- It Prevent or inhibit the normal use or management of communication facilities. This attack may have a specific target Ex:- A message in Suppress in a particular direction as a security audit service.



Security Services :- Security services which ensures sufficient Security of the System or of data being Transferred.

According to X.800 divides these Security Services into five categories.

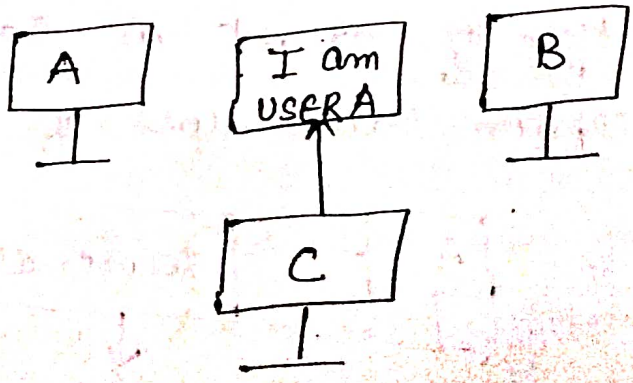
1) **Authentication :-** The authentication process ensure that the origin of electronics message or document is correctly identified.

It provide the two Specific Service :-

(i) **Peer entity authentication :-** use in logical connection to provide confidence in the identity of the entities connected.

(ii) **Data origin authentication :-**

in a connectionless Transfer, provide assured that the source of received data is as claimed.



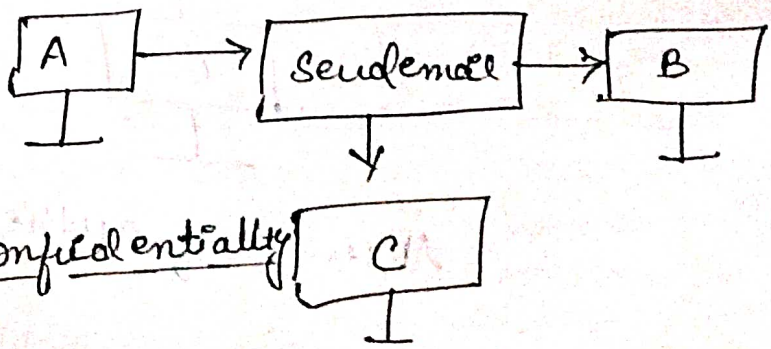
Absence of authentecation

Example :- User C sends an electronic document over the internet to user B & user C has posed himself a user A. & now problem is that how to user B know that msg has come from user C. This type of attack is called fabrication. fabrication is possible in absence of proper authentication mechanisms.

2) Access Control :- The principle of access control determines who should be able to access what.

3) Data confidentiality :- The principle of confidentiality specifies that only the sender & the intended recipient (s) should be able to access the contents of a message. confidentiality gets compromised if an unauthorised person is able to access a msg.

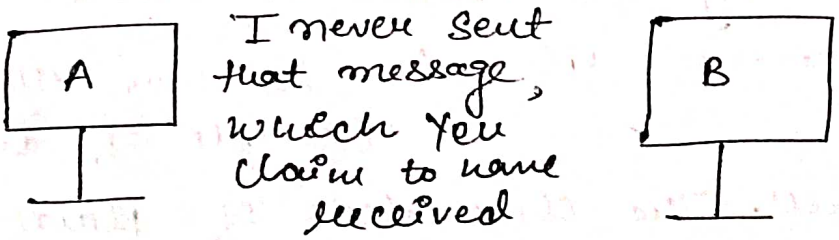
Ex. User A ~~to~~ want to send the msg to user B but another user C gets access to this msg, which is not desired, This defeat the purpose of confidentiality. This type of attack is called as interception. Interception causes loss of message confidentiality



Loss of Confidentiality

4) Data Integrity :- This security service checks the active attacks. It assures that data received are Exactly as sent by an authorized entity. It means that no modification, insertion, deletion, or replay of the message.

5) Non-repudiation :- There are situation where as a user sends a message and later on Refuse that she had send that msg. Non-Repudiation does not allow the sender of a message to refute the claim of not sending that message.



Security Mechanism :- Some of the security mechanism is implemented into the particular protocol layer. Security mechanism process called encipherment.

Security encipherment divided into two parts :-

(i) Reversible Encipherment Mechanism :-

A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted & decrypted.

in this hash algorithm & message authentication codes, which are used in digital signature & message authentication application.

Classical Encryption Techniques :- There are two classic / conventional encryption techniques of cryptography.

1) Substitution Techniques
2) Transposition Techniques.

(i) Substitution Techniques :- A alphanumeric character of the plain text is Replaced by alphanumeric character.

(i) Caesar cipher :- It was the first Example of substitution cipher. The characters of plain text message are replaced by other character, number or symbols. In this techniques each alphabet in a msg is replaced by an alphabet three places down the line.

Ex. LOKESH → ORNHVK

(ii) Modified version of Caesar cipher :-

In this techniques we can not fix the Pattern of Text. in this we use any Same pattern of the text.

c) Mono - Alphabetic Cipher :-

Plain	a	b	c	d	e	f
Cipher	m	n	b	V	C	X

It is similar to Caesar cipher but in this cipher we give any alphabet to this cipher.

d) Homophonic Cipher :-

In this cipher we can Replace a Plain Text in cipher text. It is also alphabetic techniques in this we change Single alphabet in more than one alphabet

for ex. A → D, H, P, R
B → E, I, Q, S etc.

e) Polygram Substitution Cipher :-

In this technique block of alphabet are change in another block of alphabet.

Ex. HELLO - YUQQW but HELL is Totally different cipher text TEUI

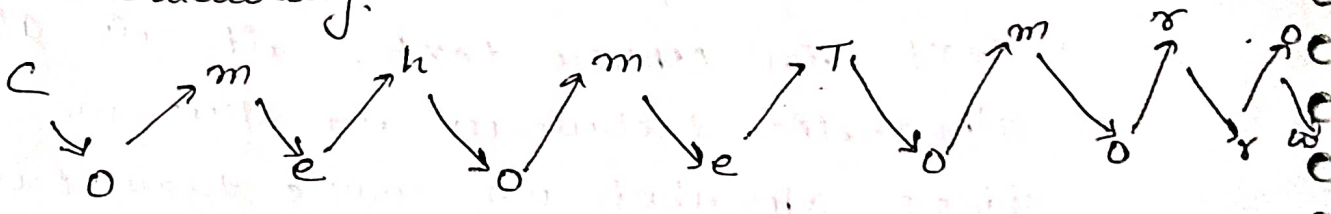
Transposition Techniques :- Transposition Techniques Replace the one alphabet with another alphabet. in this technique we use different combination of alphabets.

(B) Rail Fence Technique :-

→ In this plain Text write down in Sequence of diagonal.

→ & than read the plain text in new step (i)

→ now by row read & write it Sequentially.



Cmhmtmroo e o e oorw in cipher text.

Simple Columnar Transposition Techniques

(i) Basic Techniques :-

→ In this we write the plain text row by row.

→ Read the message column by column & it is not in the order of 1, 2, 3 or 3, 2, 1 etc.

Original plain text message :- Come home Tomorrow

1) Let us consider with 6 columns.
To write the plain text.

Col 1	Col 2	Col 3	Col 4	Col 5	Col 6
c	o	m	e	h	o
m	e	t	o	m	o
w	w	o	w		

2) Let u decide the order of columns as some random order 4, 6, 1, 2, 5, 3

3) & than cipher text is eowoocmwoehmmto

Simple columnar transposition technique with multiple Round

1) write a plain text row by row in a rectangle of pre-define size.

2) net fix the order of column is 123 or 3,2,1 for the cipher text.

3) Repeat the (i) step as many time desired.

c o m e h o m
m e t o m o
w w o w

eowoocmwoehmmto

1	2	3	4	5	6
e	o	w	o	o	c
m	w	o	e	w	h
m	m	t	o		

oeochemmomwowc

c) Vernam Cipher :- This technology is also called One time pad.

The length of input cipher text is equal to the length of plain text.

1)

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

Plain Text	H	O	W	A	R	E	Y	O	U
	T	14	22	0	17	4	24	14	20
	13	2	1	19	25	16	0	17	22
One time Pad	N	C	B	T	Z	Q	A	R	X

"discard after a single use & secure at small text"

Initial Total	20	16	23	19	42	20	24	31	43

Subtract 26, if result > 25	20	16	23	19	16	20	24	5	17
	U	Q	X	T	Q	U	Y	F	R

Cryptanalysis :- The process of analyze the plain text or key is known as Cryptanalysis.

1) Attempt to break a single msg

2) Recognize the pattern of encrypted msg, to be able to break

Subsequent ones by applying decryption algo

Stream & Block Cipher :- The Generation of the cipher text from plain text can be classified in 2 ways.

1) Stream Cipher
2) Block Cipher

1) **Stream Cipher** :- The plain text encrypted one bit at a time.

→ original msg in plain text is 'lokesh' in ASCII. & Now we convert in binary values. Suppose it is 01011100.
& key is applied is 10010101 in binary

→ we assume that we are applying (X-OR) logic for encryption.

Ex. plain text 01011100
key 10010101
11001000

Same bit - 0
Diff - 1

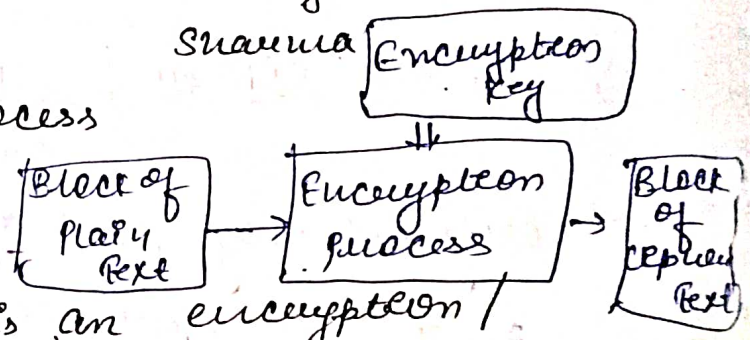
2) **Block Cipher** :- A block of bit is encrypted at one go.
in this plain text "lokesh_kumar_sharma"
& the block cipher lokesh will be encrypted first followed by kumar & finally sharma.

plain text	Lokesh	- Kumar -	Shanna
	Encrypt	Encrypt	encrypt
cipher text	+^(#)@	!)*+%#	+@()#$

Block cipher Encryption process

+^(#)@	!)*+%#	+@()#$
Decrypt	Decrypt	Decrypt
Lokesh	- Kumar -	Shanna

Block cipher decryption process



Block Cipher Techniques :-

A block cipher is an encryption / decryption scheme in which a block of plaintext is treated & used to produce a cipher text of equal length.

Shannon's Theory of Confusion and Diffusion

The concept of diffusion & confusion are introduced by claude Shannon.

1) **Confusion :-** This is also known as Substitution. Cipher text result when the letters in the plaintext

$X = (x_0, x_1, x_2 \cdots x_{n-1}) \rightarrow (y_0, y_1, y_2 \cdots y_{n-1})$

Confusion is technique in which no clue of cipher text.

Diffusion :- This is also known as Transposition when the position of letters in the plaintext of letter in the plaintext $X = (X_0, X_1, \cdots X_{n-1})$ are rearranged $(X_0, X_1, \cdots X_{n-1}) \rightarrow (X_{x_0}, X_{x_1}, \cdots X_{xn-1})$. Diffusion increase the redundancy of the plaintext by spreading it across row & columns.

Feistel Cipher structure :- Most of the block ciphers used this cipher structure. The input to the encryption algorithm is a plaintext block of 2B bits length and key K.

The plain text block is divided into 2 parts of B bits each as L_0 & R_0. These 2 parts of data are processed through n rounds.

After n rounds of processing the two output block of data are combined to produced the cipher text.

All rounds has the same structure.

The performance of the feistel cipher structure depends on the following task.

1) **Number of Rounds :-** The no. of rounds, higher the security we use 16 rounds.

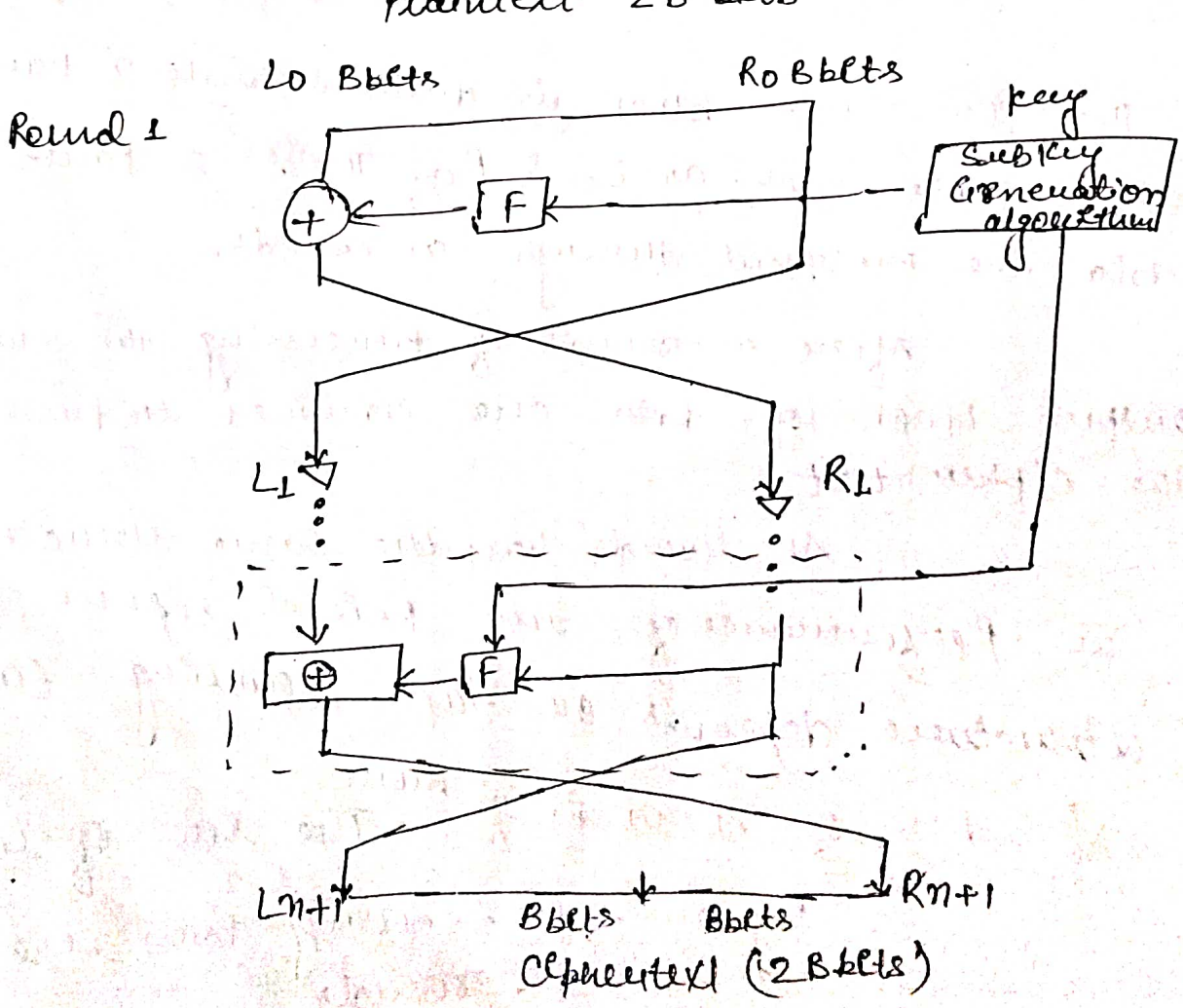
Feistel cipher is not a specific scheme of block cipher. It is design model from which many different block ciphers are derived.

Block Size :- Longer block size increase security. But it reduce the computational speed of encryption / decryption. Generally a block of 64 bits is used.

3) **Key Size** :- Larger the key size reduced the encryption / decryption speed but it provides the greater security.

1) **Sub-key Generation Algorithm** :- Greater complexity in this algorithm lead to greater difficulty to cryptanalysis.

Round function :- greater Resistence to the function.

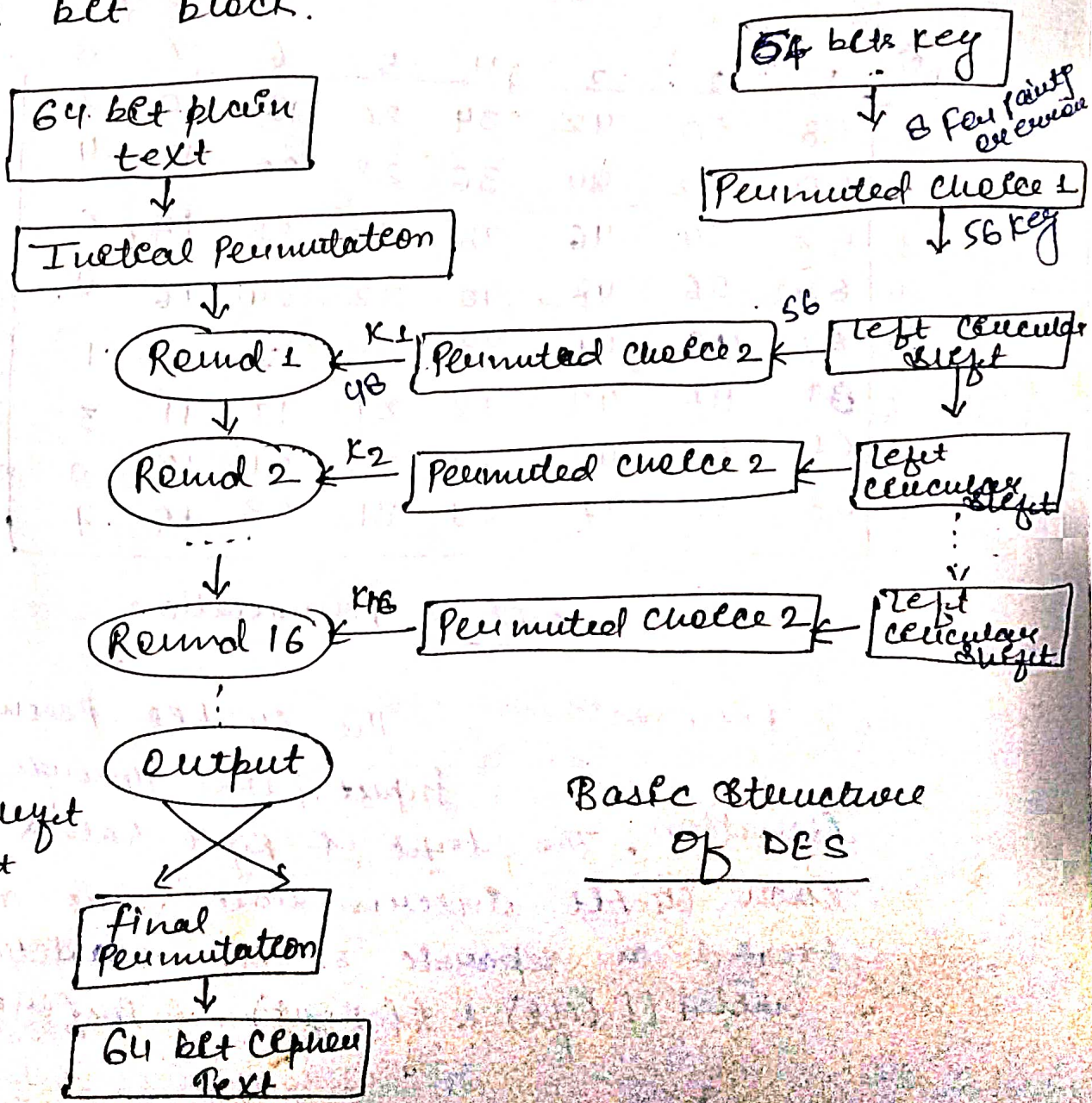


Data Encryption Standard (DES):

DES is very well known block cipher encryption algorithm that published in 1977 by the National bureau of Standards for use in commercial.

In DES we use the plain text block of 64 bits in length and key is of 56 bits in length.

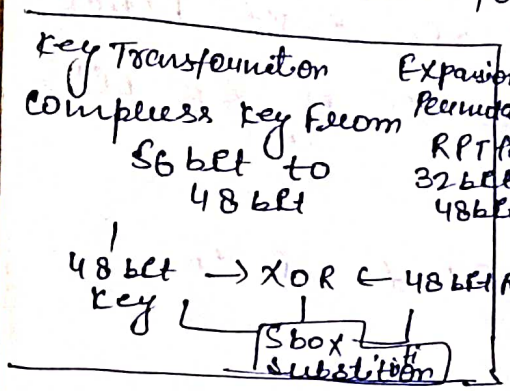
longer text is divided into 64 bit block.



Basic Structure of DES

Initial Permutation :-

This phase Rearrange the 64 bit plaintext to produce the permuted output. This is enhance the DES security



Bit position in the plain text block

To be overwritten with the contents of this bit position

1 = 58
2 = 50
3 = 42
⋮
64 = 7

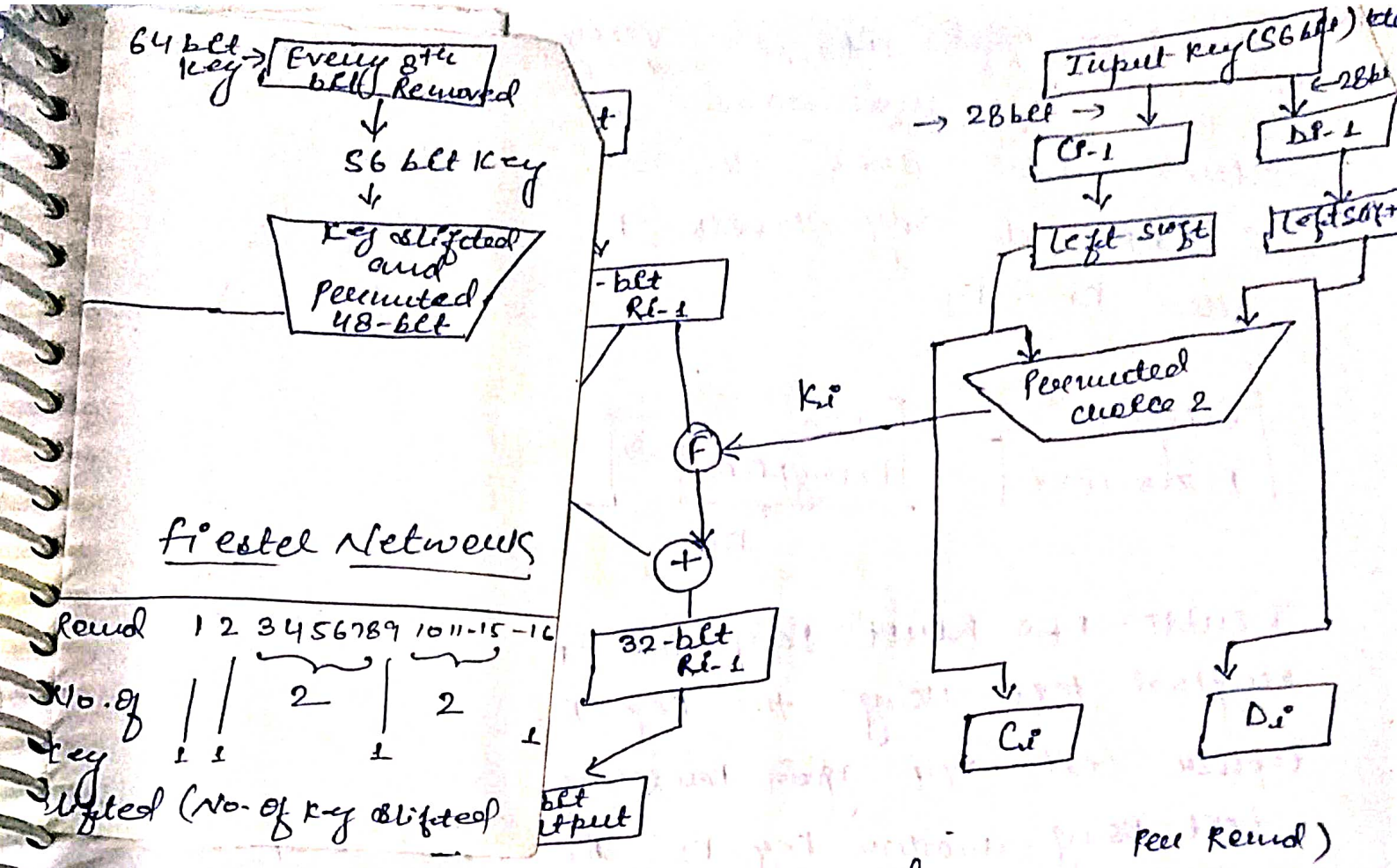
Select

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

Initial permutation

Round Foundation :-

The 64-bit permuted input passes through 16-iteration. The left & Right halves of each 64-bit intermediate value are treated as separate 32-bit quantities. Labled (L (left) & R (Right). & Perform ⊕ XOR.



A DES Round

The Strength of DES :-

The strength of DES are divided into 2 areas :-

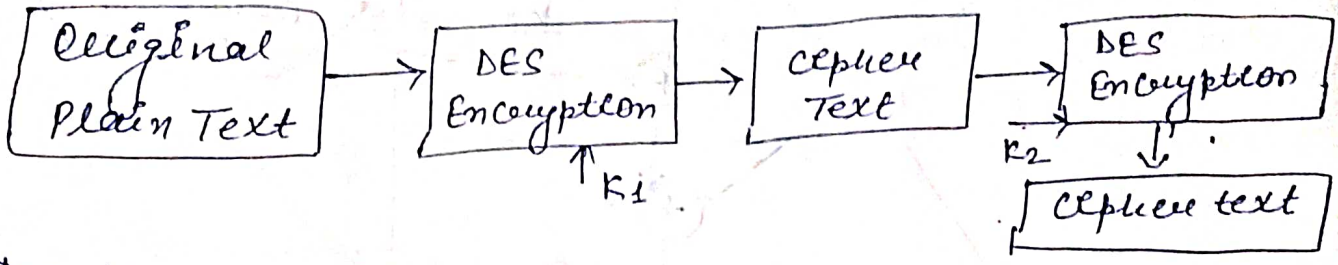
1) Key size
2) Nature of the algorithm

a) **Key size :-** We use key size of 56-bit that can generate 2^56 different possible keys.

b) **The Nature of the DES Algorithm :-**

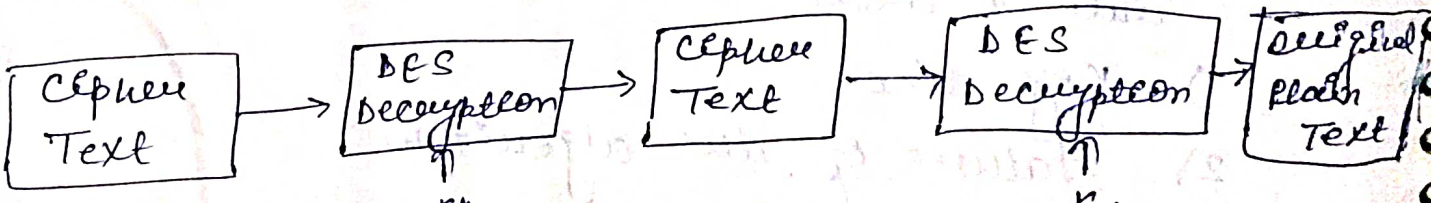
Nature of DES algorithm is more secure, Reliable, & flexible.

Double DES :- It is very simple to understand double DES. The double DES does the same thing that is DES do only once. Double use 2 keys, called K_1 & K_2.



Double DES first performs DES on the original text using the key K_1 to get the cipher text. It again performs on the cipher text using another key K_2. The final output is the cipher text (Encrypted Text)

The Double DES decryption is the reverse process of encryption.

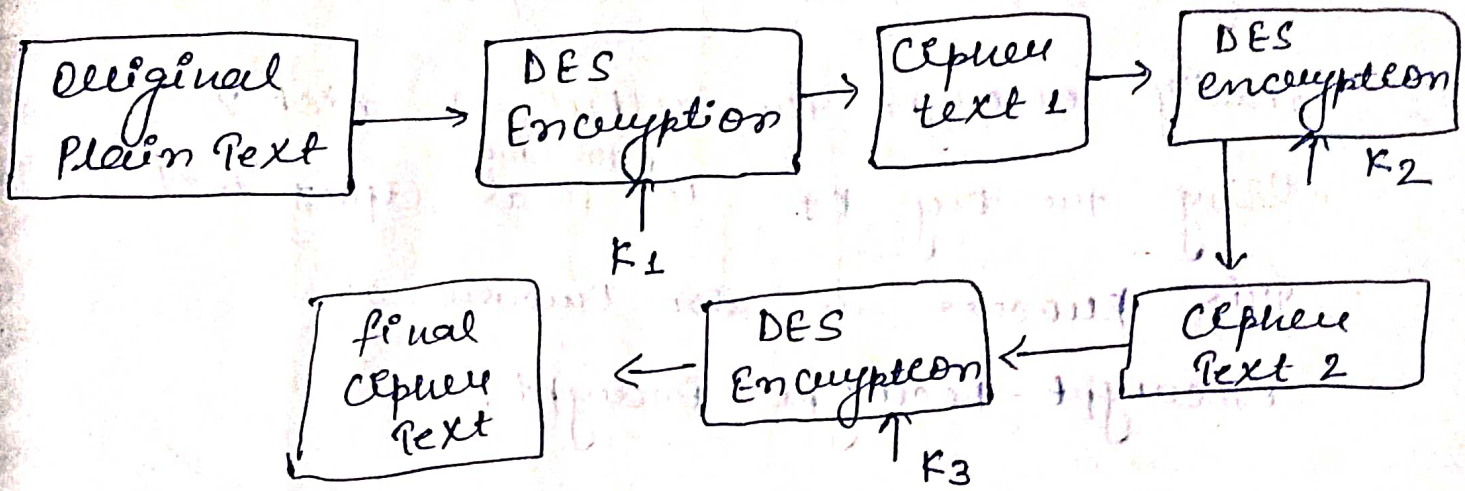


Double DES Decryption

Triple DES :- In this DES we use 3 keys. The plain text first encrypted with key K_1, then encrypted with 2nd key K_2, & finally with the key K_3.

Where K_1, K_2, K_3 are different to each other

for the decryption cipher text first decrypt using key K_3, then K_2 & finally with key K_1 & obtain the plain text.



Triple DES with Three keys

Triple DES with Two keys :-

Triple DES is highly secure but practically implementation is a difficult. Because it requires $56 \times 3 = 168$ bit for key, is difficult.

So we overcome this problem Triple DES with 2 key.