31/7/19

INFORMATION SECURITY
ACCS- 16505

It is the process of protecting information availability, data integrity and privacy.

Primary goals of IS:-

Confidentiality
Integrity
Availability (CIA)

Data types:-
Public
Private / Internal
confidential
Secret

Elements of IS

Physical elements:- guard, camera, restricted R-zone, access rights.

System elements

Process elements

Security Types.

- Physical
- Personal
- Operations
- Communications
- Network
- Information

1/8/19

The OSI Security Architecture

To assess effectively a security needs of an organisation and to evaluate and choose various security products and policies, the manager responsible for computer and network security needs some systematic way of defining the requirements for security and characterising the approaches for satisfying these requirements.

ITU-T (International telecommunication union - telecommunication standardisation sector)

ITU-T recommendation X.800 security architecture for OSI define such a systematic approach. The OSI security architecture is useful to ~~an~~ manager

It is useful to manager as a way of organising the task of providing security. Further more because this architecture was developed as an International standard, computer and communications vendored have developed security features for their products and services.

X.800

attacks | services | mechanism

Attacks

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

Security Mechanism

A process i.e., designed to detect, prevent or recover from a security attack.

Security Service

A processing or communication service that enhances the security of data processing system and the information transfers of an organization.

5 marks *

Categories of Security Attacks :→

- Passive Attack (no data modification)
- Active Attack (data modification)

Attack :- Gaining the access of data by unauthorized user.
→ Accessing the data
destroying
Modifying

PASSIVE ATTACK :

A passive attack attempts to learn or make use of information from the system but doesn't affect your system resources.

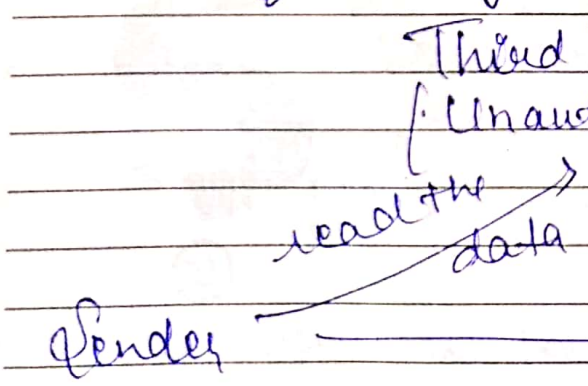
ACTIVE ATTACK

An active attack attempts to alter system resources or affect their operation.

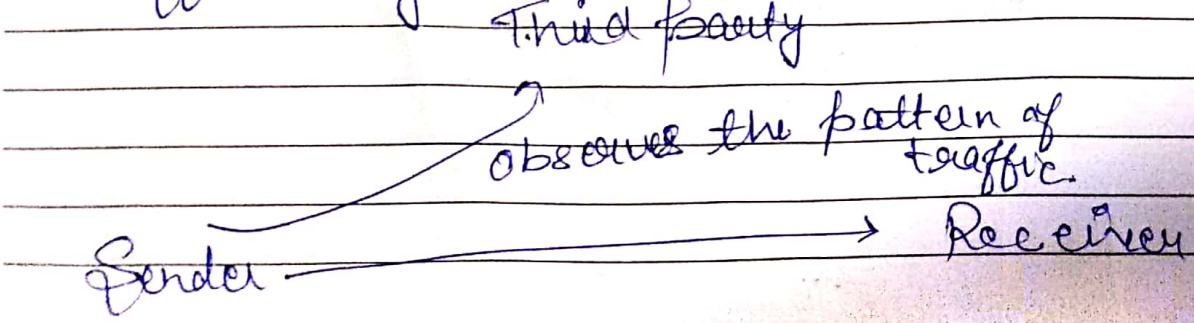
PASSIVE ATTACKS

- Release of message content
- Traffic Analysis.

Release of message content :

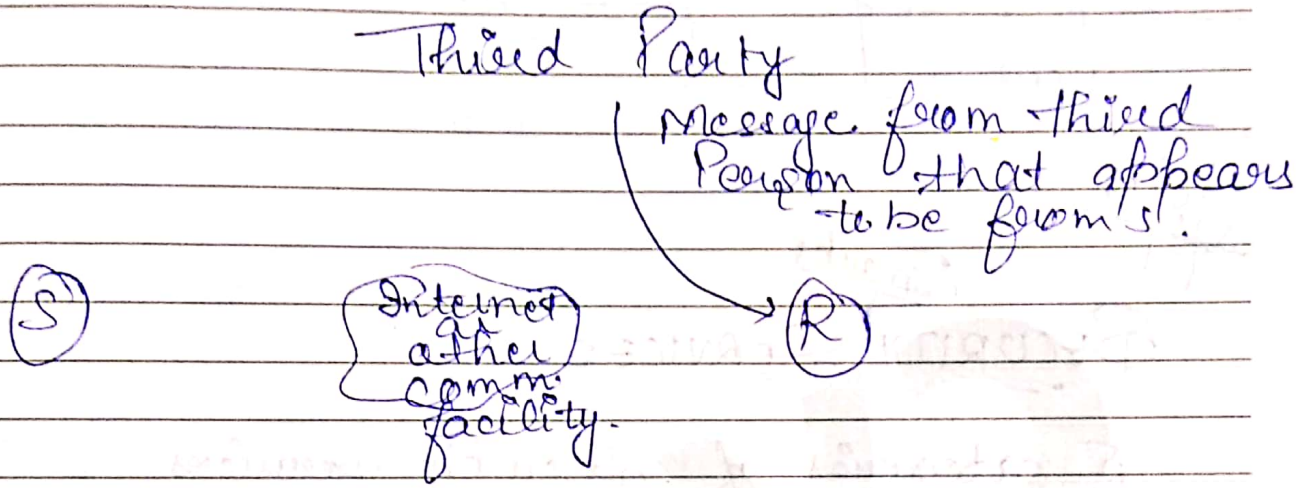


Traffic Analysis :

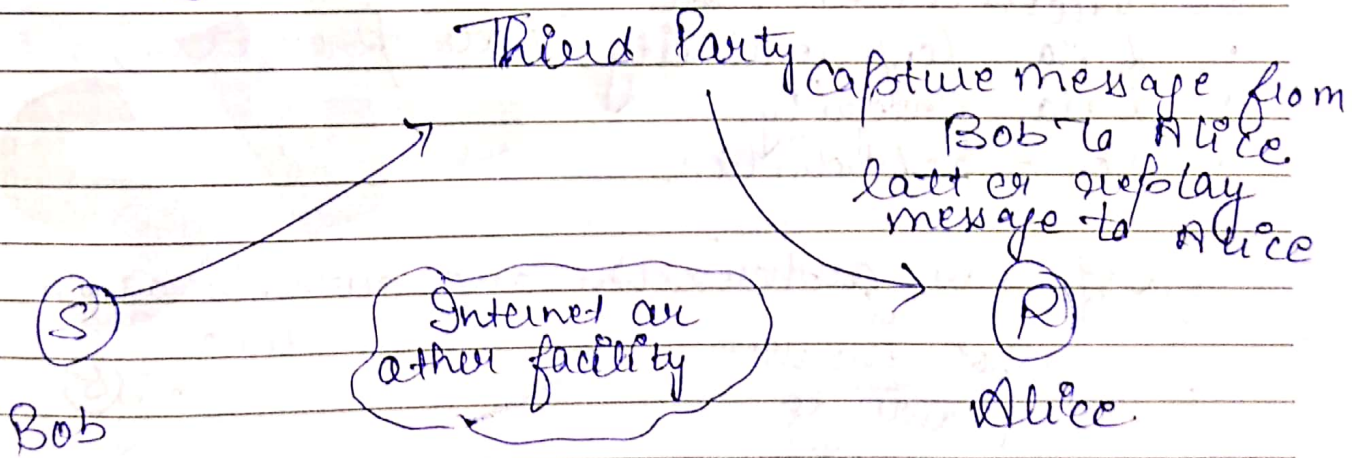


ACTIVE ATTACK

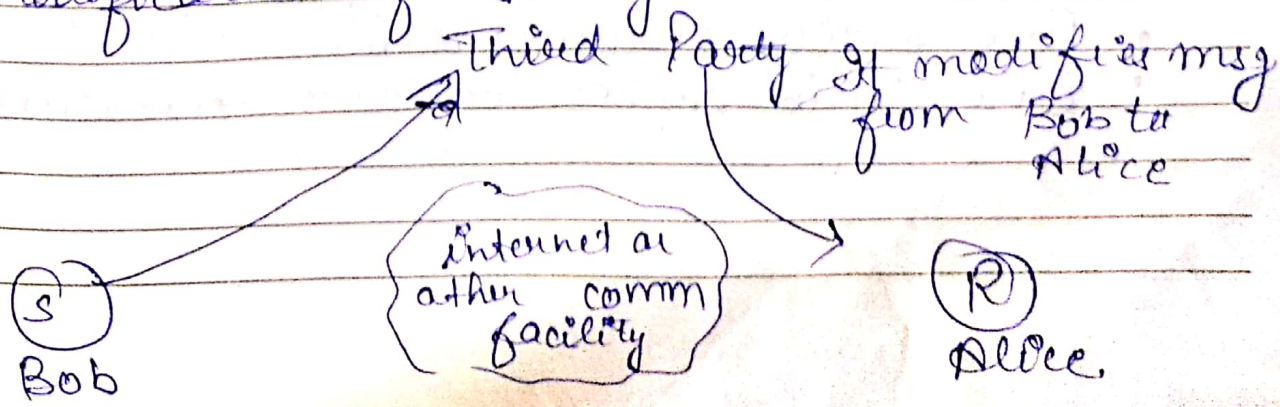
- Masquerade attack



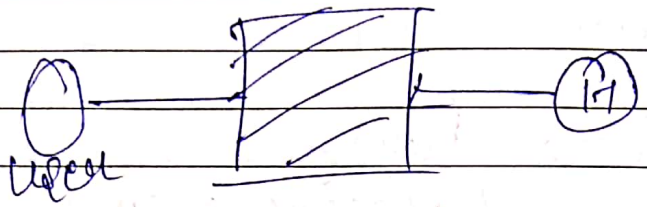
- Replay attack



- Modification of messages



DOS attack



8/8/19

5 marks

SECURITY SERVICES

5 categories of security services

- Authentication
- Access Control (authorization)
- Data Confidentiality (Data protection)
- Data Integrity
- Non - Repudiation

Diff b/w authorization and authentication

what the user wants to do?	who is doing.

AUTHENTICATION

- Peer entity Authentication → connection oriented
- Data Origin Authentication → connectionless

ACCESS CONTROL

- who can access a resource.
- condition under which access occurs.
- operation that may be performed an resource.

DATA CONFIDENTIALITY :-

- Connection confidentiality.
- Connectionless Confidentiality
- Selective - Field Confidentiality
- Traffic Flow Confidentiality.

DATA INTEGRITY

- Connection integrity with recovery
- Connection integrity without recovery.
- Selective - field Connection Integrity.
- Connectionless integrity.
- Selective - field connectionless integrity.

Non - Repudiation

- Non repudiation, Origin
- Non repudiation, Destination.

5 marks

SECURITY MECHANISM

Specific security mechanisms
- encipherment
- digital signatures
- access controls
- data integrity
- authentication exchange
- traffic padding
- routing control
- notarization

Pervasive security mechanisms
- trusted functionality
- security labels
- event detection
- security audit trails
- security recovery

7/8/19

Pervasive Security

Trusted functionality
Security labels
Event detection
Security audit trail
Security recovery.

Model for Network Security

Model for Network access security.

Encryption Methods

- (Conventional, Symmetric)
- Public Key

Symmetric Encryption

→ conventional / private-key / single-key

plain text → original message

cipher text → coded message.

Cipher → algorithm for transforming plain text to cipher text.

Key :- info used in cipher known only to sender / receiver.

Encipher → encryption

decipher → decrypt.

cryptography :- study of encryption principles

Cryptanalysis :- study of method for decrypting cipher cipher text without key

Cryptology → cryptography + cryptoanalysis.

Conventional Encryption.

5 components:

- plain text
- Encryption algorithm.
- Secret key
- Cipher text
- Decryption algorithm.

Classification of Cryptographic Systems:

(i) Type of operation used for encryption:
- Substitution
- Transposition
- Product.

(ii) The number of keys used.
- Hash function: no key.
- Symmetric
- Asymmetric

(iii) The way in which the plain text

Processed :->
- Block Cipher
- Stream cipher.

Attacks on encryp method.

Classical Symmetric Cipher
- Substitution Ciphers.
- Transposition ciphers.

Substitution ciphers.
- Monoalphabetic (Ceaser cipher)/Shift Cipher.
- Polyalphabetic.
(Playfair and Vigenere Cipher)

MONOALPHABETIC

0 1 2 3 ... 24 25 26
A B C D ... X Y Z

Cipher	0	1	2	3	4	5	6	7	8		24	25	26
Plain	A	B	C	D	E	F	G	H	I	...	X	Y	Z
Cipher	d	e	f								a	b	c

$C = E(K, P) = (P + K) \bmod 26$
$= E(3, 0) = 3 \bmod 26$
$C = 3$

TUTORIAL → ~~WWW~~
→ wxworldo

Decryption $P = D(C, K) = (C-3) \bmod 26$

	0	1	2	3	4	5	6	7
Cipher	a	b	c	d	e	f	g	h
Plain	X	Y	Z	A	B	C	D	E

23	24	25
x	y	z
U	V	W

$P = D(K, C) = (C-3) \bmod 26$

$= D(3, 0) = -3$ → last three char

8 8 19

Ceaser Cypher

(Brute Force attacks are very common)

- Simple Substitution Technique

- Polyalphabetic:-

① Playfair cypher. Key = Tutorial

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

PT:- Hide money

Monoalphabetic cypher is a substitution cypher in which for a given key, the cypher alphabet for each plain alphabet is fixed throughout the encryption process.

If A is encrypted as d, for any no. of occurence in that plain text A will get encrypted to d all the time.

These cyphers are highly susceptable to cryptanalysis. In ceaser cypher the key set consist of 25 keys as a result bruteforce attacks are quite common. So in order to enhance the security of encryption simple substitution cypher is invented.

Poly alphabetic cipher is

It is a substitution cipher in which cipher alphabet for plain alphabet maybe different at different places during the encryption process is

PLAYFAIR → It was invented by Charles Wheatstone in 1854. In this scheme, pair of letters are encrypted, instead of

single letter as in the case of simple substitution cipher.

In playfair cipher initially a key table is created. A key table is 5×5 grid of alphabets that acts as a key for encrypting the plain text. Each of the 25 alphabets must be unique and 1 letter of the alphabet usually 'j' is omitted from the table as we need only 25 alphabets instead of 26. If plain text contains j then it is replaced with i.

→ Sender and receiver will decide

Let key = tutorial

Step 1: The plain text is split into pairs of two letters if there is an odd no add x at the end

PT: Hide money

Hi de mo ne yx

qc ef nu

Step 2: Rule 1: If both the letters are in the same column, take the letter below each one going back to the top if at the bottom.

qc

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

Rule 2 :- If both the letters are in same row take the letter to the right of each one going back to the left if at the farthest right.

q c e f

Rule 3 :- If neither of the preceding two rules are true, form a rectangle with two letters and take the letters on the horizontal opp corner of the letter

Hi de mo ne yz
qc ef nu mf ve

14 | 8 | 19

VIGENERE CIPHER :-

Key = point

Msg to = attack from south east

P → 16, O → 15, I → 9, N → 14, T → 20

PT	a	t	t	a	c	k	f	r	o	m	s	o	u	th	h	e	a	s	t
key	16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	25	9	14
CT	Q	I	C	P	W	A	U	A											
	Q	I	C	O	W	A	U	A	K	G	I	D	D	H	B	U	P	B	H
key	16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14
PT	a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t

The process of vigenere cipher

Step 1:- The sender and the receiver decide on a key say "point" numeric representation of this key is 16 15 9 14 20.

Step 2:- The sender wants to encrypt the message say "attack from south east". He will arrange the plain text and numeric key as follows.

PT

Key

Step 3:- Now he shifts each plain text alphabet by the no. written below it to create cipher text as shown below.

CT

Step 4:- Here each plain text character has been shifted by a different amount and the amount is determine by the key. The key must be less than or equal to the size of message.

Step 5:- For decryption the receiver uses the same key and shifts received cipher text in reverse order to obtain the plain text.

CT
Key
PT

VERNAM (One-time Pad)

Eg :→ PT = hello
key = XMCKL

Encryption :→

PT :	h	e	l	l	o
PTvalue :	8	5	12	12	15
One-time pad text :	X	M	C	K	L
one-time pad value :	24	13	3	11	12
Sum of PT+Key	32	18	15	23	27
after modulo subtraction :	6	18	15	23	1
CT	F	R	O	W	A

Decryption

CT	F	R	O	W	A
Value	6	8	15	23	1
One-time text Key	X	M	C	K	L
Pad value	24	13	3	11	12
Sub	-18	5	12	12	-11
mod26	8	5	12	12	15
	h	e	l	l	o

- Vernem cypher was developed by Gilbert Vernem in year 1917 in AT & T labs.
- Implemented by using one time pad (key)
- Key is discarded after one use.
- Length of input cipher text is equal to the length of original plain text.

Algorithm.

1. Write each plain text alphabet as no. i.e., a = 1, b = 2 . . . . z = 26 and so on
2. process will continue for one time pad.
3) Add plain text alphabet no. to one time pad no.
4) If sum is greater than equal to 26 subtract 26 from it.
5) Convert each no. of sum of alphabet.

Modulo:- The process of keeping a computed no. within a specified range is called modulo thus range 1 to 26 is called modulo 26.

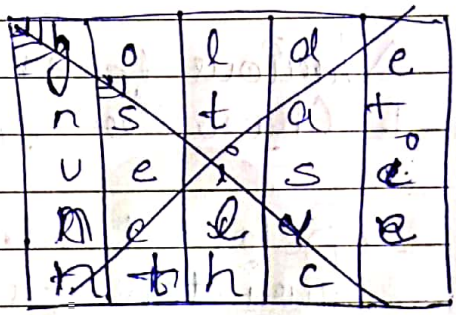
26/8/19

Transposition Cipher

Plain text : "golden statue is in eleventh cave"

Random Key is "five"

g	o	l	d	e
n	s	t	a	t
u	e	i	s	i
n	e	l	e	v
e	n	t	h	c
a	v	e		



Cipher text gnune aosecnvlti...

Stagnography

Steganos → Greek (to cover)
(covered/Hidden)

It is a technique of ~~fino~~ hiding secret data within an ordinary, non secret, file or message in order to avoid detection, the secret data is then extracted at its destination.

A plain text message may be hidden in one of

two ways. The methods of steganography conceals the existence of the message whereas the methods of cryptography renders the message unintelligable to outsiders by various transformation of the text.

Various techniques used is
1. Character marking :→

Selected letters of printed or type written text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

2) Invisible Ink :
A no. of substances can be used for writing but leave no visible traces until heat or some chemical is applied to a paper

3) Pin Punchers :→ Small pin punctures on selected letters are ordinarily not visible unless a paper is held up in front of light.

4) Typewriter correction ribbon

Used b/w lines tied with a black ribbon, the result of typing with correction make are visible only under a strong light.

Transposition Cipher

- Rearrange the order of Plain text bits.
- No Replacement / Substitution

1. Rail Fence
2. Row Transposition.

⇒ RAIL FENCE

PT → TEXT BOOK PAGE THREE
Key → 3 (no. of rows)

T	_	_	_	B	_	_	_	P	_	_	_	T	_	_	_	E
_	E	_	T	_	O	_	K	_	A	_	E	_	H	_	E	_
_	_	X	_	_	_	O	_	_	_	G	_	_	_	R	_	_

Cipher text → TBPTEETOKAGHEXOGR

Jumbling of characters is done is Rail fence cipher to get the cipher text it is used for short length messages and easily ~~cha~~ crackable.

Firstly, we will decide the value of key. Suppose value is 3 we will make 3 row and then count the no. of alphabets present in the original message and make that much amount of column.

Key :- WELCOME ACET Key = 4

For this case we will make 4 rows 11 columns.

ROW TRANSPOSITION

PT :- WELCOME TO MY SESSION
Key :- Unique no. (no repeat)

3	2	4	5	1
W	E	L	C	O
M	E	T	O	M
Y	S	E	S	S
I	O	N	X	Y

X Y → dummy character

Cipher Text : OMSYEESOWMYT
LTENCOSX

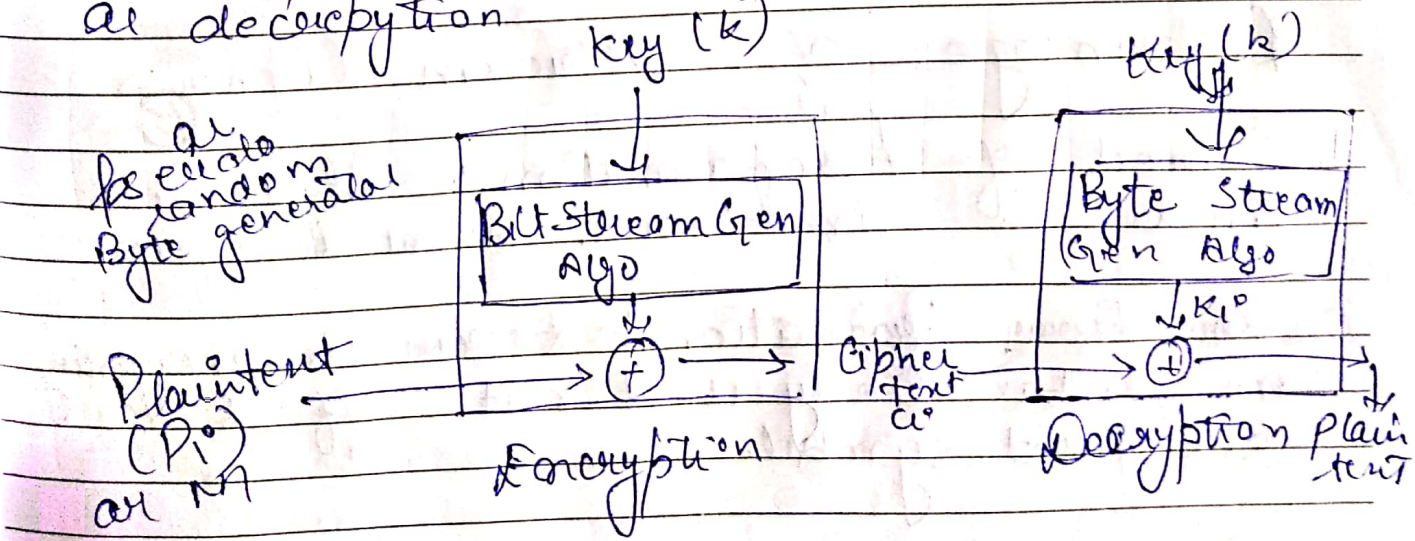
Symmetric Key Cipher

- Stream Cipher
- Block Cipher

- Single Key b/w S & R
- Both algo are inverse to each other

Stream Cipher :->

1. Generalization of one time pad
2. Stream cipher initialized with short key
3. Key is stretched into long key stream
4. Have a Pseudo Random property.
5. Key stream is used like one time pad.
6. XOR operation is perform for encryption as decryption



$$
\begin{array}{rl}
 & 1\,0\,1\,1\,0\,1\,1\,0 \quad - M \\
\oplus & 0\,1\,0\,1\,0\,1\,0\,1 \quad - K \\
\hline
 & 1\,1\,1\,0\,0\,0\,1\,1 \quad - \text{Cipher Text} \\
\oplus & 0\,1\,0\,1\,0\,1\,0\,1 \quad - K \\
\hline
 & 1\,0\,1\,1\,0\,1\,1\,0 \quad - \text{Plain text.}
\end{array}
$$

Let E be an encipherment algorithm let $E_K(b)$ ~~the~~ be the encipherment of message (b) with Key K.

Let message $m = b_1 b_2 \ldots$ where each b_i is of fixed length and $K = K_1 K_2 \ldots$

A Stream cipher is a cipher for which

$$E_K(m) = E_{K_1}(b_1)\, E_{K_2}(b_2) \ldots$$

Advantages of Stream Cipher is

1. Speed of transformation :- Algo are linear in time and constant in space.
2. Low Error Propagation :- Error in encrypting one symbol likely will not affect subsequent symbol.

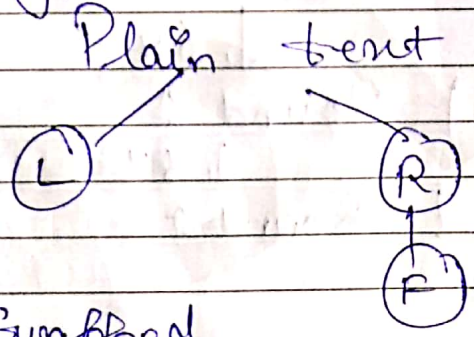
Disadvantage

1. Low Diffusion
2. Susceptibility to insertion/ modification

~~29/8/19~~

4/9/19

Data Encryption Standard



Swapped

↓

Cipher text

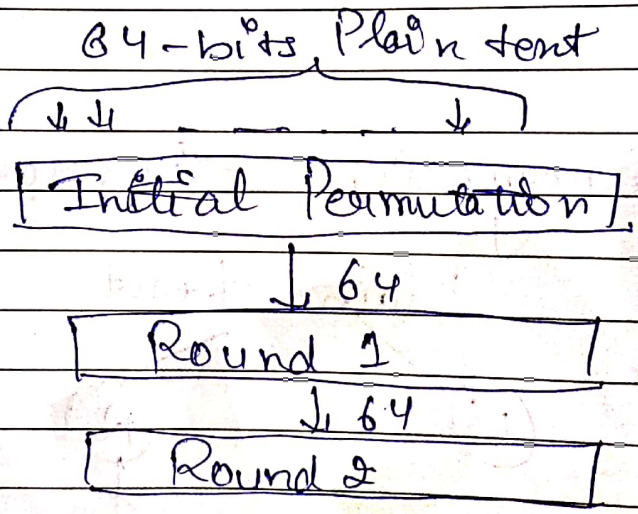
History : 1971, IBM developed LUCIFER block of 64 bits, 128 bit key.

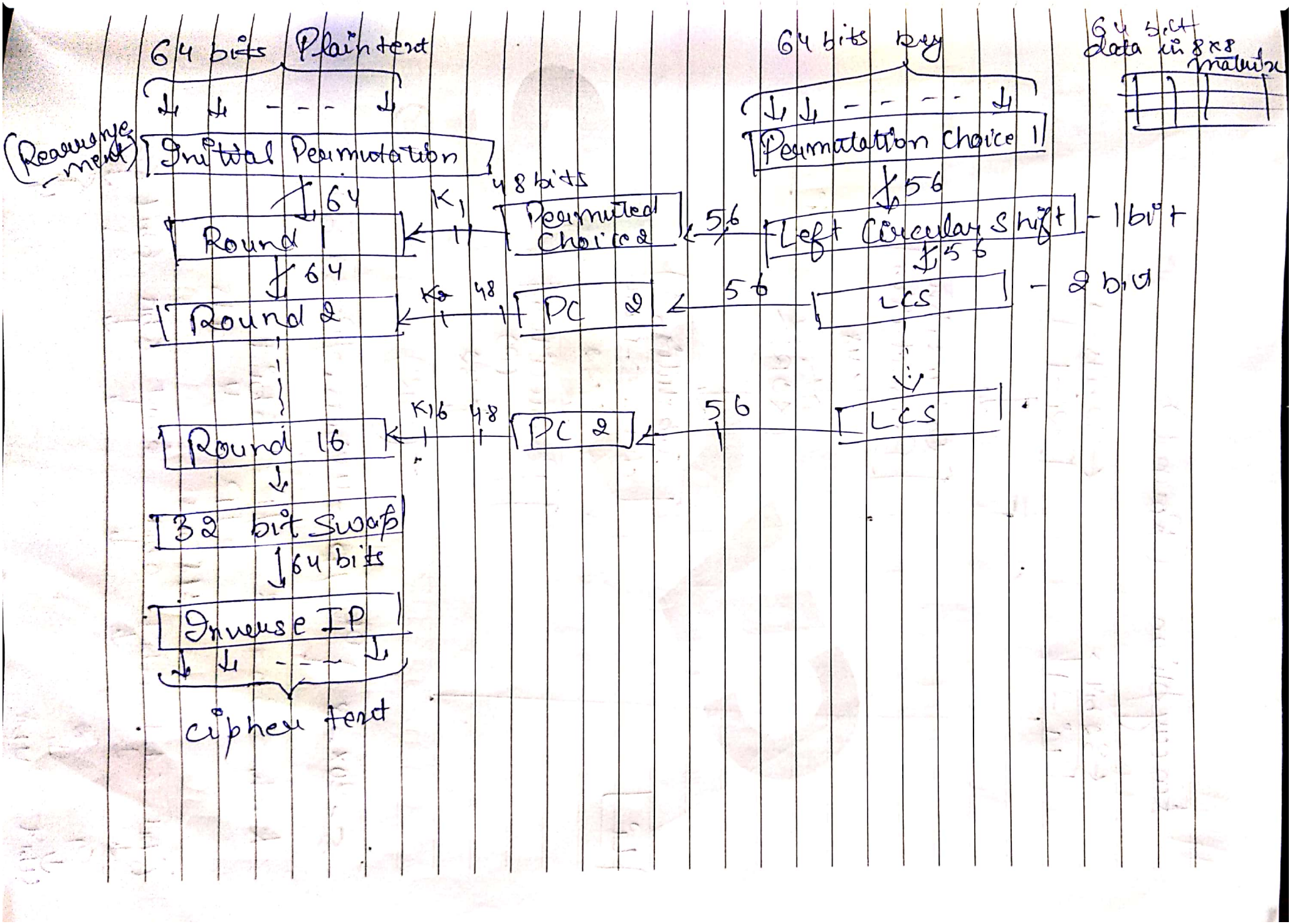
Walter Techman, redefined LUCIFER & reduced key to 56 bit

1977, results of Tuckman's project as DES

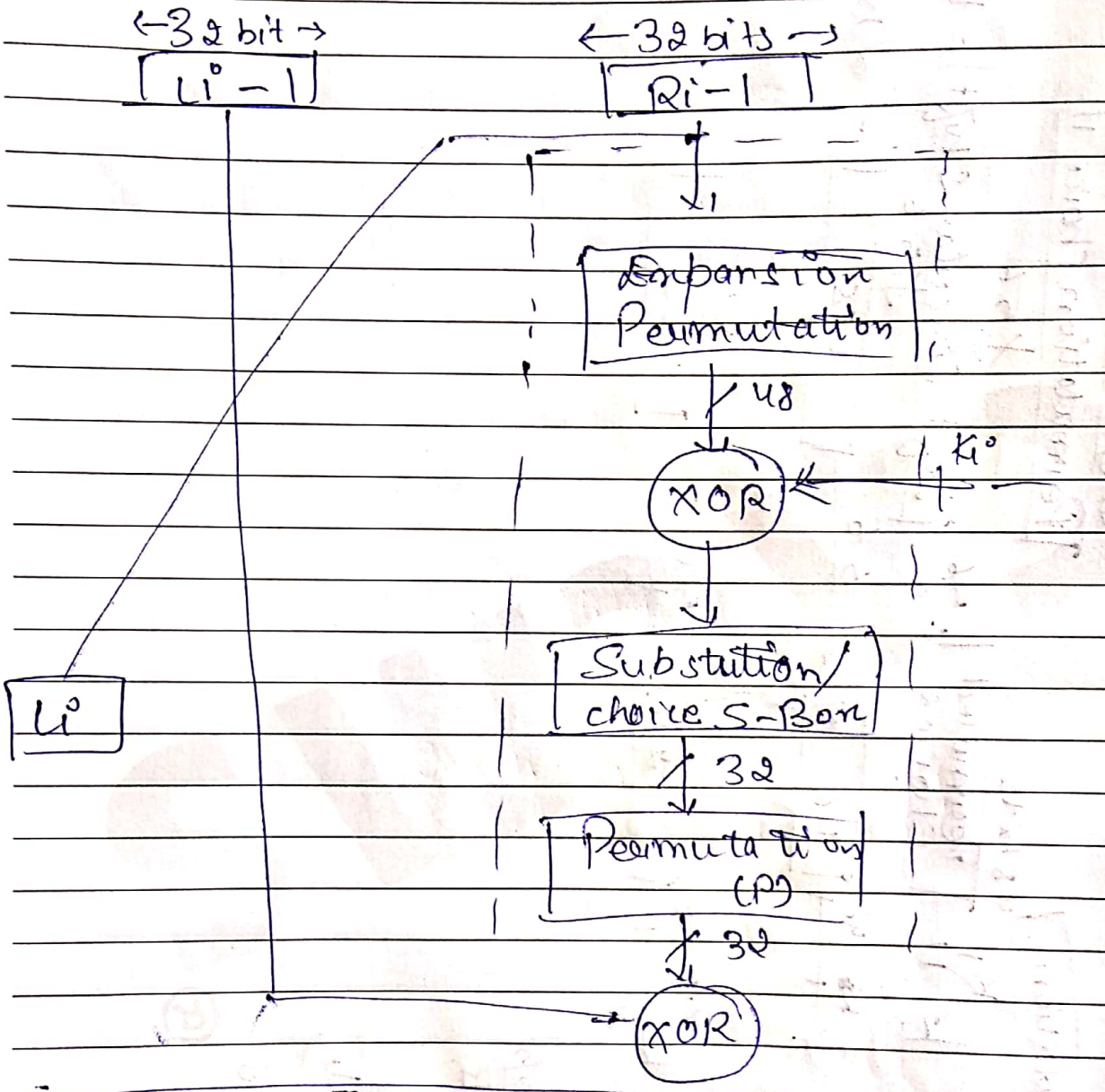
- Block Size : 64 bits (PT)
- No. of rounds : 16
- Key size : 64 bits.
- No. of subkeys : 16 rounds (16 subkeys)

Subkey size : 48 bits
Cipher text : 64 bits





Encryption (Round)



S-Box-8 [DES I/P = 48 bits, O/P = 32 bits]

Each SBox & I/P = 6 bit
O/P = 4 bits

48 bits

6 bit | 6 bit | 6 bit | 6 bit | 6 bit | 6 bit | 6 bit | 6 bit

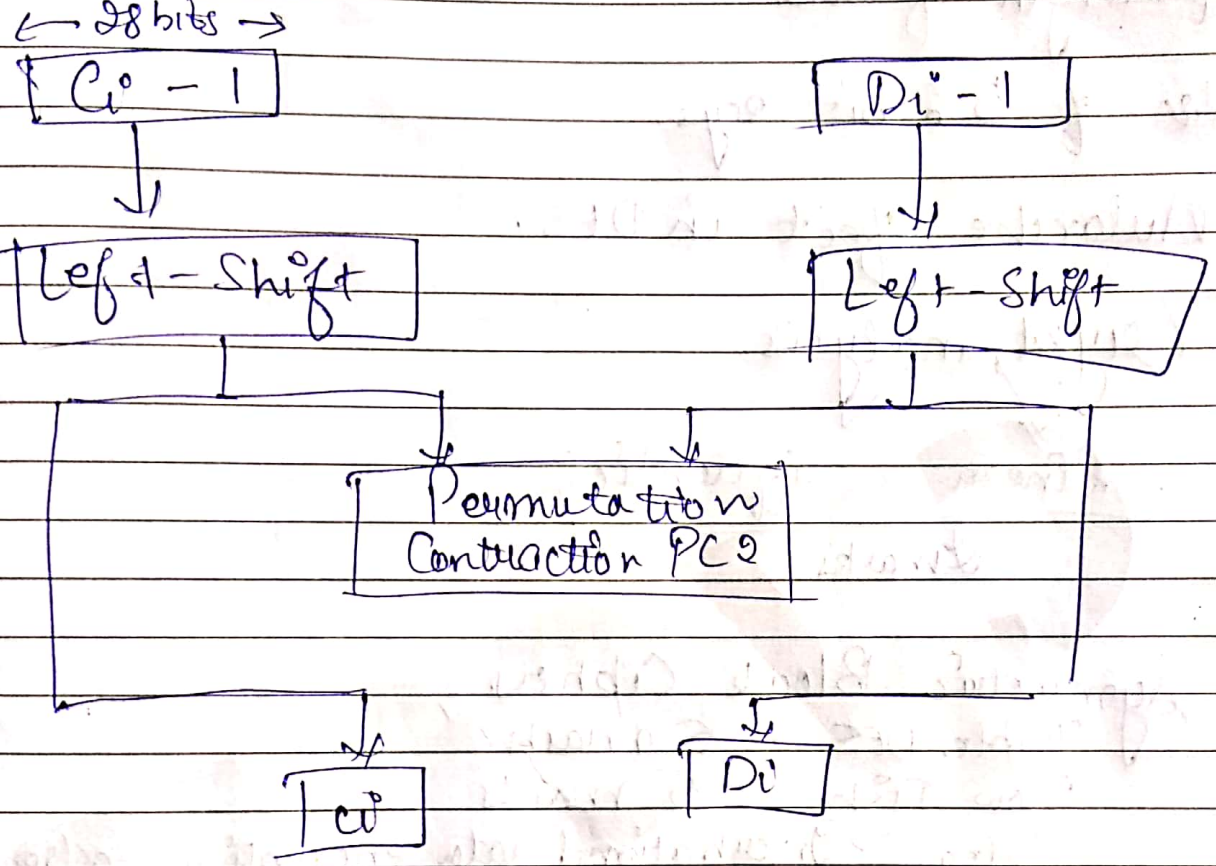
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

S_1 S_2 - - - - S_8

↓ ↓ ↓

4 bit 4 bit - - - - 4 bit

Key Generation



Eg : F
1 0 0 1 1 0

F + L → Row → 2 → (4)

0 0 1 1 → Column → 4 bits → (16)

	0	1	2	3 4	...	16
0						
1						
2						
3						

8 → 1600

9/9/19

Strength of DES

Use of 56 bit keys.

Avalanche effect in DES.

Cryptanalysis.

Linear differential

8 marks

Symmetric Block Ciphers.

Triple DES - 5 marks

Blow Fish - 5 marks

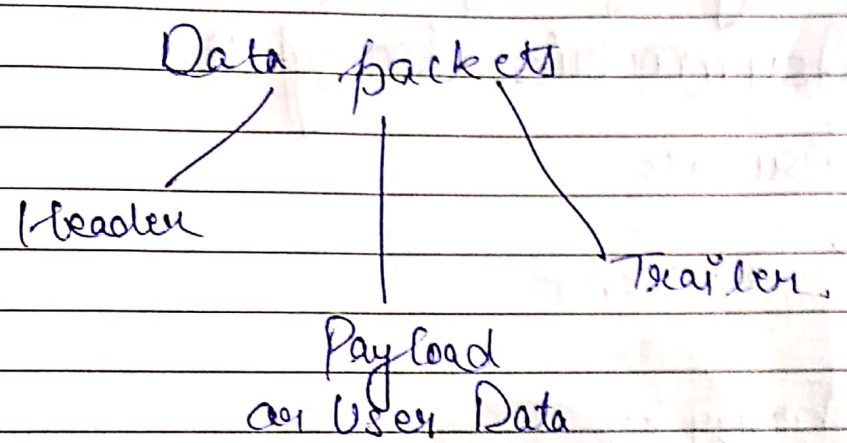
Idea -> International data encryption algo.

RC5 -> Rivest Cipher / Ron's Code

Triple DES

11/9/19 Confidentiality using Symmetric Encryption.

How to distribute the secret key.



end-to-end encryption

link encrypt → 1 & layer
end to end → 3...

Traffic Analysis.

covert channel

⇒ Link Encryption
- Traffic Padding

→ End to end encryption
- Pad out data units to uniform length
- Null messages

Key Distribution

12/9/19

Public Key Cryptography / Asymmetric Encryption

Keys → Private
→ Public

Number Theory :-

1. Prime No :- An integer $p > 1$ is a prime no. iff its only divisor are ± 1.

Any integer $a \geq 1$ can be factored in a unique way

$$a = P_1^{a_1} \times P_2^{a_2} \times \cdots P_t^{a_t}$$

where $P_1 < P_2 < \cdots P_t$ are prime nos and where each a_i is a positive integer

Eg → $91 = 7 \times 13$

$$3600 = 2^4 \times 3^2 \times 5^2$$

2. Relatively prime no. :=

8, 15

8 → 1, 2, 4, 8

15 → 1, 3, 5, 15

} no common divisor rather than 1.

gcd (8, 15) = 1

$a = \prod_{p \in P} p^{a_p}$ where each $a_p \geq 0$.

25

GCD :→ $300 = 2^2 \times 3^1 \times 5^2$

$18 = 2^1 \times 3^2 \times 5^0$

↳ $2^1 \times 3^1 \times 5^0 \Rightarrow 6$

Theorem

This theorem is used in public key and private key testing.

if p is prime &

a is the integer not divisible p

i.e., (gcd(a, p) = 1)

then $a^{p-1} \equiv 1 \pmod{p}$ or $\frac{a^p}{a} \equiv 1 \pmod{p}$

~~$a^{p-1} \pmod{p} =$~~

$a^p = a \pmod{p}$