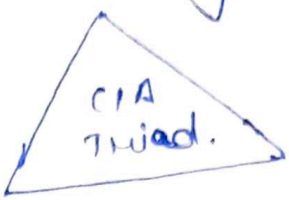
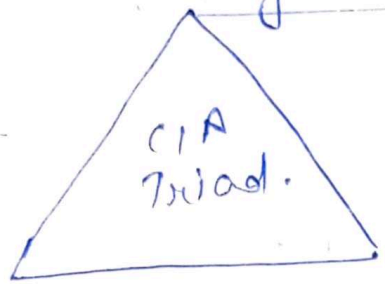
Information Security :-

→ Information :- How data having some meaning.

→ Information that are common are not so important for preserving or securing.

→ To maintain security —





Confidentiality.

↳ cryptography is used to achieved.

↳ Steganography

Availability.

Access control. Notorisation.

Integrity

↳ Hash Code / MAC / HMAC.

MAC → Message ~~Access code~~. Authentication code.

→ Encrypted ~~data~~ form of data — cypher text.

→ Services for security :-

↳ Authentication. → Entity Auth. / Message Auth.

↳ Authorization.

↳ Integrity.

↳ Non repudiation

↳ Access control.

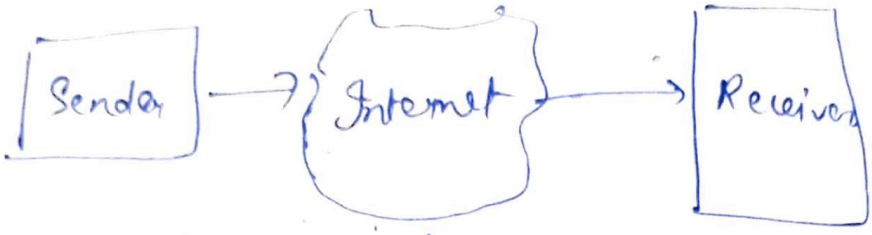
→ Services are given to maintain the CIA triad.

↳ Cryptography & network security — Forouzan.

17/1/23

→ IT industries maintain CIA triad.
↳ additional two steps are maintained.
↳ Authenticity.
↳ Accountability.

*. ↳ confidentiality is required because the internet is more vulnerable area.



↑ vulnerability (threats may be there).

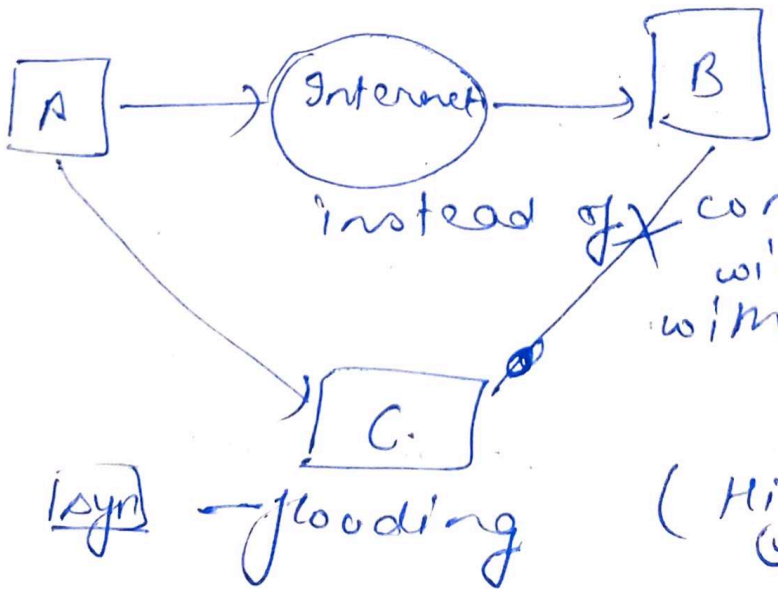
Because the communication is going through public ~~torr~~ channel.

→ Vulnerability is defined by certain threats that may or may not ~~be~~ occur.

→ If threat occurs then it is called attack.
↑ mainly on system & system is compromised.

→ ARP is very important protocol here.

→



instead of communicating with B it do with C.

TCP Syn flooding

session. (Hijacking).

→ ~~even~~ Even if any info. is received by any device, we must maintain confidentiality
↳ this is maintained by technique called encipherment (security mechanism).

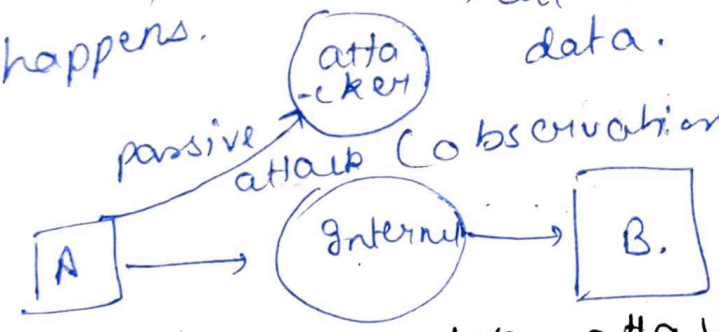
↳ Possible threats in confidentiality
↳ spooning :- capturing the data and misusing it later on ~~at~~ sometime.

Passive
↳ Traffic Analysis - to analyse which type of packet and use this analysis to send fake sync packets to the server.

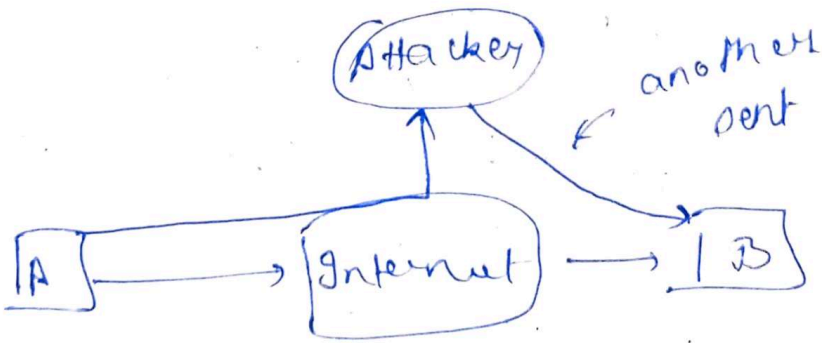
Threats

active
Can be directly converted to attack if happens.

Passive
↳ after a certain time it will convert to a certain attack.
↳ collection of historical data.



passive attack.



Active attack.

Threats / Attacks in Integrity.

(1) → **Modification:-** modification is done in the payload. The attacker changes the MAC address & receives the data changes it & sends to receiver end. (Active attack).

(2) → ~~Mod~~ **Masquading:-** - Impersonation.
Protection: (1) two way authentication (OTP)
(2) Biometric authentication.

(5) **Eavesdroping** - listening your communication.

(3) → **Replay:-**
prevention:- (1) Timestamp.
(2) Nonce.

(4) → **Non Repudiation:-** the devices cannot deny that packets are not sent.
Prevention:- using signature by both devices or append a hash code.

---

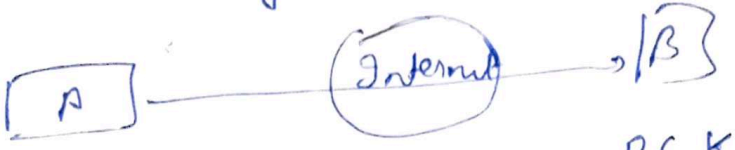
(1) → ARP cache contains table of IP & MAC addresses of devices.

IP	MAC
IP_B	MAC_C ← change in ARP Cache (cache poisoning).

↳ To ~~mai~~ avoid modification the integrity checker must be there in the header of a packet (Techniques used to avoid these threats - hash code / digital signature / MAC.

→ security techniques are used to resist the threats / attacks.

(3) → Timestamp :- adding time at which packet is send by sender & received by the receiver.



↳ PCKT + T1

PCKT + T2.

Should be.

Here — $T1 + \Delta y = T2$

Δy is the net-work delay which is pre computed.

If condition not satisfied then the packet is replay packet.

→ Nonce :- a variable to detect replay packet.

Threats On Availability :-

↳ access of info. is not there due to some issue, is threat to availability.

↳ Prevention :- ① Access Control. (Hw accessability)

② Traffic Padding.
③ Notorisation.
④ Routing Control.

↳ Threat :- Denial of service :- makes the resource unavailable (continue later).

→ Distributed Denial of service.

→ ITU have made security standards for security management.

20/1/25

Threats :-

→ security criterias are based on what threats the network faces.

→ threat is a possibility (may or may not happen).

→ before forming the solutions one should know threat vectors.

→ assets are valuable things.

→ Threat Vectors :- the assets is the target of attackers.

↳ Asset is called target.

Source	Threat	Target

← threat vectors.

list downs the threat possibles.

→ source is from where threat occurs.

→ threat vector provides — vector path.

→ after knowing the threat vectors only then we can provide solution.

→ when threat (or possibility) is applied on system or target is attack. Then the system is called compromised.

① → prioritizing the possible threats once discovered.

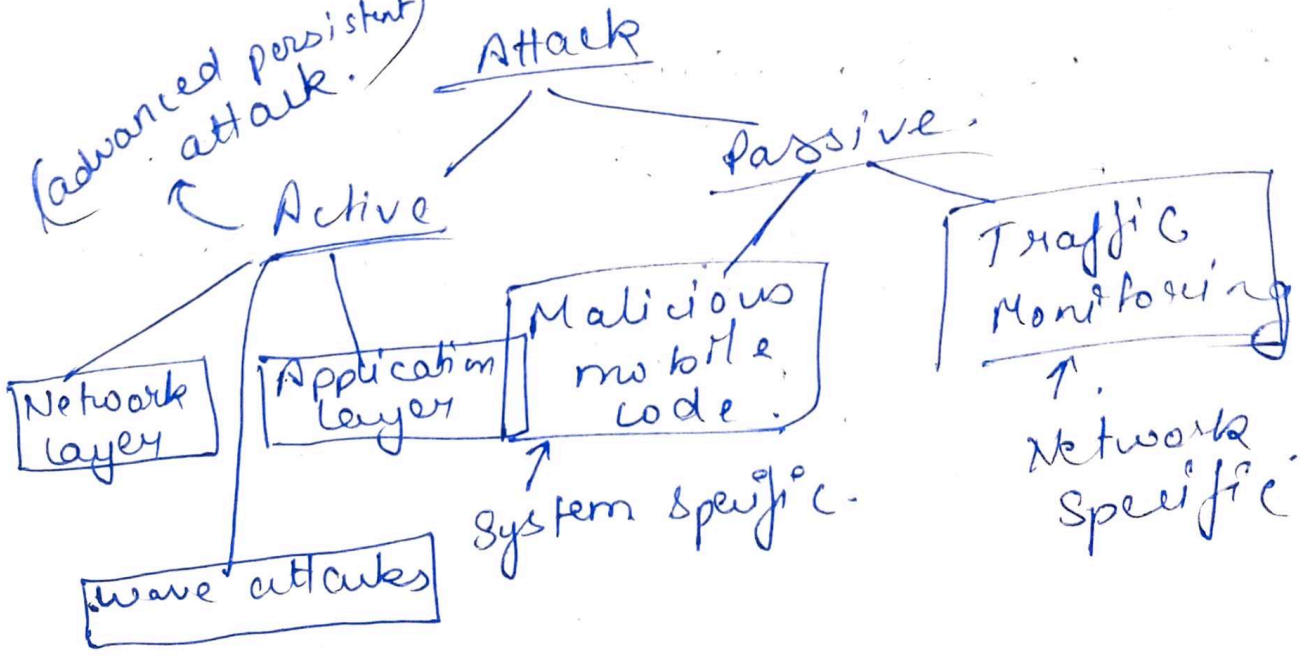
② → Realize what all threats ~~can~~ are more likely to occur.

③ → once attack occurs then restore it (system)
↳ Searching & ↳ Recovery.
↑
search place where changes are there.

④ Identify the attack ~~the~~ type. whether active or passive.

// Malware → logic bomb (eg) — malicious code.
malicious functions are targetted -
↳ delete ↳ replicate ↳ authorization of access.

(advanced persistant attack.)



Malicious Mobile Code

- Malware.
  - Trojan Horses.
  - Worms.
  - Viruses.
  - Adwares.
  - Spywares.
  - Buffer Overflow.

Network layer attacks.

- IP spoofing
- DNS "
- ARP "

→ Active Attacks can be performed when loop holes are known in the system.

Application layer Attacks.

- cyber attacks.

eg – Phishing, Spamming.

↑ connection is established with fake server.

24/1/23.

Threats.

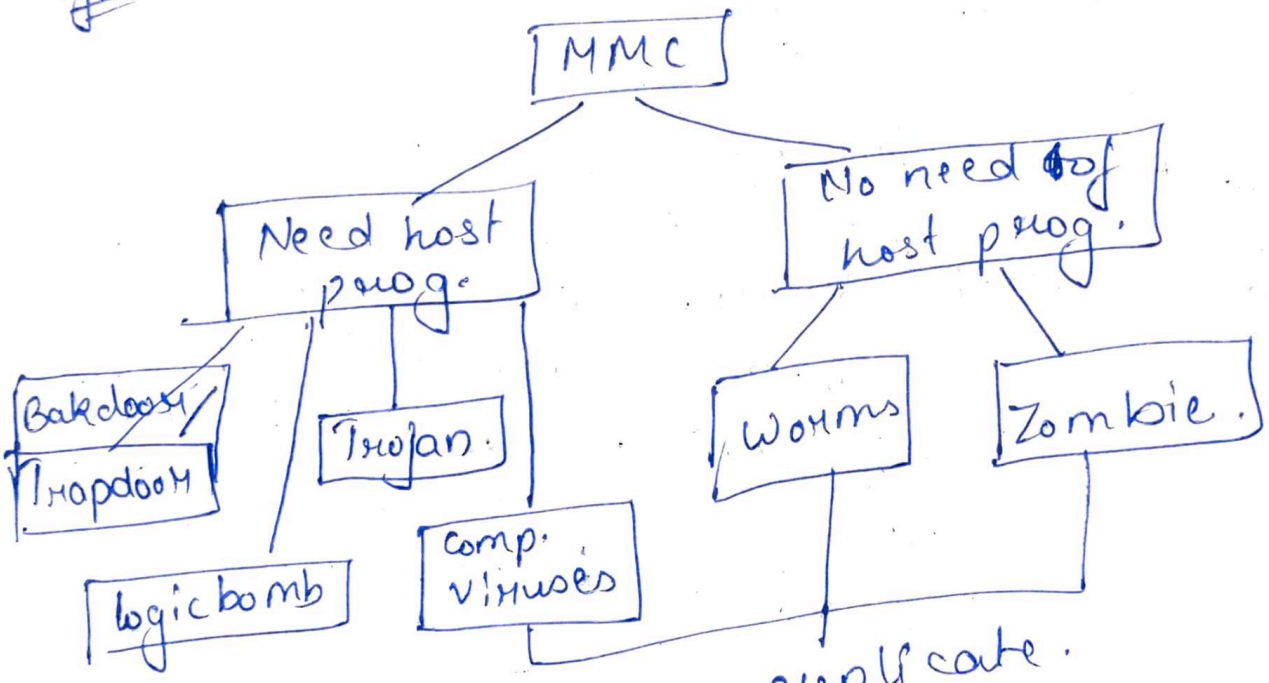
- Threat vectors (Threat sources / targets, paths).
- Types of attacks (Active & Passive).
  - Malicious Mobile Codes.
  - Advanced Persistent threats.
  - Manual attacks.

Malicious Mobile codes :-

- spreads from device to device automatically & are malicious.

Type1 → some need host program to propagate. (mainly in non centralized network).

Type2 → no need of host program.



~~Trapdoor.~~

DDoS — distributed denial of service.

- when multiple clients are unable to get the service from a server to which it is connected.

Three functions in malicious code:-

```
[ infect();
  if trigger() → logic.
  then payload();
```

Life cycle of Viruses:-

① Dormant Phase :- when virus comes inside system

② Propagation Phase.

③ Triggering Phase.

④ Execution Phase.

Types of Viruses.

↳ Boot Sector Virus:- It will infect the booting process by copying itself into the master booting block.
If infected booting becomes slow.

↳ Executable file infector:- It infects files which the operating system (OS) considers to be executable. Targets .exe file.

↳ Overwriting Virus:- It overwrites the target files.

*** ↳ Polymorphic & Metamorphic Virus:-

→ Polymorphic is a hard virus. It comes with encrypted payload.
It is actually a complicated virus that affects data type & functions. It is in an encrypted form.

→ Metamorphic can transform due to the ability to edit and rewrite their own ~~port~~ code.

Spam Bots / Mail Bots — for sending insolicited messages.

31/1/23

CRYPTOGRAPHY

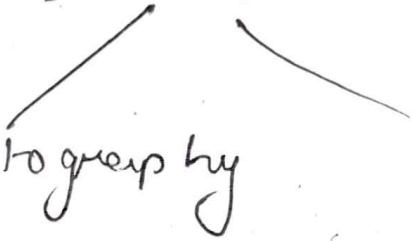
Review:-
↳ Goals - [CIA]
↳ Services -
↳ Techniques -
↳ Threats - Traffic Monitoring] Confidentiality
Spooning
↳ Types of threats
Integrity [= Message Modification.
= Eavesdroping
= Impersonation
= Replay
= Non Repudiation.

Security Techniques.

→ message will be concealed so that message is converted in unreadable form is cryptography.

→ message will be covered by some other information or something else is steganography.

Techniques.



→ (encoding & Decoding) are different from (encryption & Decryption).

→ Computational Time.
→ Brute Force Attack.

Mathematics used in Cryptography.

(1) Integer ~~Mathematics~~ Arithmetics.

Set Integer → $\boxed{Z} = \{..., -2, -1, 0, 1, 2, ...\}$

Binary Operation. $\boxed{(+), (-), (\times)}$
↳ two inputs & single output.

→ Euclidean Algorithm (finding GCD).

Q. $a = 161$ $b = 28$ Find GCD, S & T.

$s = s_1 - q * s_2$ $\quad$ $t = t_1 - q \times t_2$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	(7)	0		(-1)				(6)	

$s = -1$ $\quad$ $t = 6$

GCD = (7)

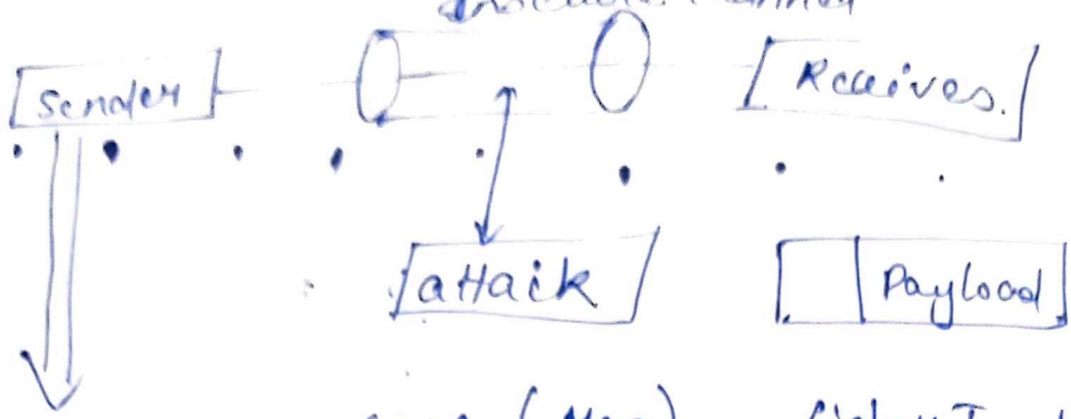
(7) Modular Arithmetic

$a \bmod b$ = remainder when (a) is divided by (b)

$27 \bmod 5 = 2$,

$36 \bmod 12 = 0$,

[CRYPTOGRAPHY]



Plain text = ENC $(Msg)_K$ = Cipher Text.

Msg → (Attack Tonight) (DWWDFN)

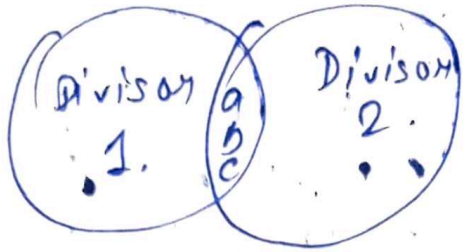
* Brute Force Attack → Do predictions.
* Cryptanalysis :- i) Cipher Text Attack
  - Brute force
  - Statistical.
* Statistical attack → count the occurence of word or alphabets.
  - (ii) Know plain text attack.
  - (iii) choosen cipher text attack.
  - (iv) choosen plain text attack.

* Euclidean Algorithm

Part 1 → gcd(a,0) = a.

Part 2 → gcd(a,b) = gcd(b,r)

GCD → greatest common divisor.



Z_n = { n = no. of sets / No. of element in sets }.

eg $Z_n = \{0, 1, 2, 3, 4\}$

$n = 5$.

Additive property = $a+b = 0 \pmod n$

Multiplicative property = $a \times b = 1 \pmod n$

eg. $a+b = 0 \pmod n$

$a = 2 \quad n = 5$

$2 + b = 0 \pmod 5$.

Extended Euclidean Algorithm.

$$(s \times a) + (t \times b) = \gcd(a, b)$$

s → s_1, s_2 ; t → t_1, t_2.

q	a	b	r	s_1	s_2	s	t_1	t_2	t
2	160	79	2	1	0	1	0	1	-2
39	79	2	1	0	1	-39	1	-2	79
2	2	1	0	1	-39	79	-2	79	-160
	1	0		-39			79		

↑ Eg:- for $a = 160 / b = 79$.

H/w GCD of 2740×1760

GCD of 25×60.

M.I. of 11 in Z_{26}.

$$s = s_1 - q * s_2 \qquad t = t_1 - q * t_2$$

* Set of integers ⟶ set of least residue (Zn).
  - ↳ additive inverse.
  - ↳ Multiplicative "

* Lemma 1 → In set of least residues (Zn) all element holding the additive inverse.

* Lemma 2 → In a set of (Zn) the Element may or may not have their multiplicative inverse.

* Lemma 3 → An element (b) in Zn have a multiplicative inverse if and only if gcd (b, n) = 1.

$$(g \times n) \bmod n + (t \times b) \bmod n \equiv 1 \bmod n$$

** Substitution Method

(1) Monoalphabetic cipher (one to one).
(2) Polyalphabetic cipher (one to many).

→ (1) additive cipher. if key is (k).
encryption eqn ⇒ $p + k = C$.
Decryption " ⇒ $C + k = P$.

② Multiplicative cipher :- if the key is (k)

encryption cipher ⇒ $P \times K = C$.

Decryption " ⇒ $C \times K = P$.

7 4 " " 14

Q. Set of integer → HELLO.

A B C D E F ..... Z

0 1 2 3 4 5 25

Key = 3 additive :-

H → (7+3) mod 26 = 10 → K

E → (4+3) " = 7 → H

L → (11+3) " = 14 → O

L → (11+3) " = 14 → O

O → (14+3) " = 17 → R.

M.I.

H → (7×3) mod 26 = 21 → V

E → (4×3) " = 12 → M

L → (11×3) " = 7 → H

L → (11×3) " = 7 → H

O → (14×3) " = 16 → Q.

encryption.

if we want to decrypt then :-

21×9 mod 26 = H (7)

12×9 " = E (4)

7×9 " = L (11)

7×9 " = L (11)

16×9 " = O (14).

* Affine Cipher.

(additive + multiplicative.)

additive key = k_2

multiplicative key = k_1

$$(p \times k_1) \bmod 26 = T$$

$$(T + k_2) \bmod 26 = C$$

HCH $k_2 = 2$, $k_1 = 3$.

H → $(7 \times 3) + 2 \bmod 26 = 23 \rightarrow X$

E → $(4 \times 3) + 2$ " $= 14 \rightarrow O$

L → $(11 \times 3) + 8$ " $= 9 \rightarrow J$

L → $(11 \times 3) + 2$ " $= 9 \rightarrow J$

O → $(14 \times 3) + 2$ " $= 18 \rightarrow S$

$$(C - k_2) \times k_1^{-1} \bmod 26 = P$$

HW

Q1

Q2.

10/2/23

Q. Plain Text = ab
cipher text = GL.
keys used k_1, k_2

$(P \times k_1) + k_2 \equiv C \pmod{26}$

multiplicative, additive

Z_{26} is set

P	C
a	G
00	06
b	L
01	11

(K_1, K_2).

$00 \times k_1 + k_2 \equiv 6 \pmod{26}$

$01 \times k_1 + k_2 \equiv 11 \pmod{26}$

$\Rightarrow k_2 \equiv 6 \pmod{26}$

$k_1 + k_2 \equiv 11 \pmod{26}$.

$k_1 \equiv 5 \pmod{26}$.

---

if $2k_1 + k_2 = 6$ is there how we will solve!
$k_1 + k_2 = 11$

$$\begin{pmatrix} k_1 \\ k_2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 6 \\ 11 \end{pmatrix} \pmod{26}.$$

Q. H/W. et → wc what will be keys.
et → wF.
affine cipher.

Polyalphabetic cipher.

→ one to many mapping.

① **Playfair** we take a key phrase or word.

↳ the word is converted to matrix whi
→ size of matrix doesn't change.

DIAMOND.

Key matrix.

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

→ no letters are repeated in matrix.

→ I & J are very much used and most frequently occurs so I/J are together in one cell.

→ concept is circular.

THIS IS MY FIRST CLASS TODAY.

(TH) (IS) (IS) (MY) (FI) (RS) (TC) (LA) (SX) (ST) (OD) (AY).

(RL) (AR) (AR) (EM) (BO) (ST) (SE) (KM) (XA) (TU) (ID) (MX)

---

② **Vigenere** – Take positional value.

1 2 9 11 → Key.

PT THIS IS MY FIRST CLASS.

T H I S I S M Y F I R S T. C L A S S

19 7 8 18 8 18 12 24 5 8 17 18

(+) (+) (+) (+) (+) (+) (+) (+) (+) (+) (+) (+)

1 2 9 11 1 2 9 11 1 2 9 11

(+) addition

(×) multiplication.

20 9 17 3 9 20 21 9 6 10 0 3.

mod 26: U J R (29/26) J U V J → CT.

D

H/w

eqn 1

$e \longrightarrow w$

$t \longrightarrow c$.

$e = 04 \rightarrow w = 22$

$t = 19 \longrightarrow c = 02$

$(04 \times K_1 + K_2) = 22 \pmod{26}$

$(19 \times K_1 + K_2) = 02 \pmod{26}$

$$\begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} 19 & 7 \\ 3 & 24 \end{bmatrix} \begin{bmatrix} 22 \\ 7 \end{bmatrix}$$

$$\therefore \begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 16 \\ 10 \end{bmatrix} \quad K_1 = 16 \text{ & } K_2 = 10$$

$\gcd(16, 26) = 2$.

16 doesn't have M.I. in Z_{26}.

eqn (2) $e \longrightarrow w$

$t \longrightarrow f$.

$(04 \times K_1 + K_2) = 22 \pmod{26}$

$(19 \times K_1 + K_2) = 5 \pmod{26}$

$$\begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 5 \end{bmatrix} = \begin{bmatrix} 19 & 7 \\ 3 & 24 \end{bmatrix} \begin{bmatrix} 22 \\ 5 \end{bmatrix}$$

$$= \begin{bmatrix} 453 \\ 185 \end{bmatrix}$$

$$\begin{pmatrix} k_1 \\ k_2 \end{pmatrix} = \begin{bmatrix} 11 \\ 4 \end{bmatrix}$$ So $k_1 = 11$ $k_2 = 4$.

gcd (11, 26) = 1

14/2/23

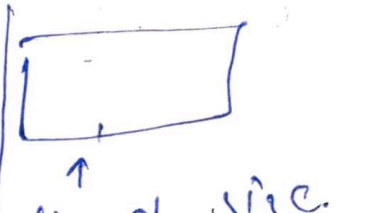
→ Brute force attack will not always give up the desired solution.

Hill Cipher:

→ A cipher produce as a block.

eg representing following stream in block.

This is my question. you have to write correct answer.



TI	H	I	S	I
S	M	Y	Q	U
E	S	T	I	O
N	Y	O	U	M
A	V	E	T	O

5x5.

a block containing information.

→ Plain text & cipher text are represented in blocks.

** we know $C = K \otimes P \pmod n$

operation

P = plain text/message

K = key

c = cipher text.

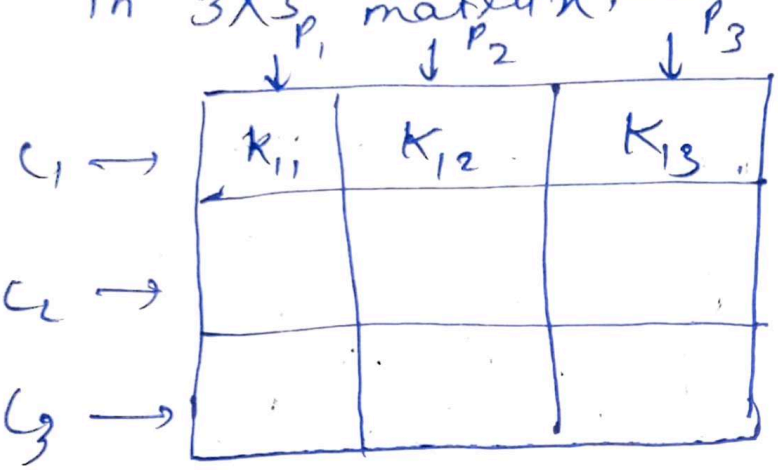
→ each row will be represented in form of ~~$c_1 = kp_1$~~

$$c_1 = p_1 k_{11} + p_2 k_{12} + p_3 k_{13}$$

$$c_2 = p_1 k_{21} + p_2 k_{22} + p_3 k_{23}.$$

$$c_3 = p_1 k_{31} + p_2 k_{32} + p_3 k_{33}$$

in 3×3 matrix,



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

Let's suppose we have key matrix;

$$\Rightarrow \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \times \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \pmod{26}$$

ENC $\Rightarrow C = KP$

DEC $\Rightarrow P = K^{-1} C.$

→ There must be multiplicative inverse of keys only then we can have decryption as —

$$P = K^{-1} C \quad .$$

$$K(K^{-1}) = 1 \pmod{26} \quad \text{condition.}$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

Plain text = PAY MORE MONEY.
15 0 24 taking 3 at a time.

$$\begin{matrix} C_1 \\ C_2 \\ C_3 \end{matrix} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \times \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$$

$$\begin{matrix} C_1 \\ C_2 \\ C_3 \end{matrix} = \begin{pmatrix} 375 \% 26 \\ 819 \% 26 \\ 486 \% 26 \end{pmatrix} = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} \pmod{26}$$

Q. CT → HCRZSSXNSP.
↳ Hill cipher.

Take CT in matrix form.

H C
7 2

$\frac{HC}{CT} \rightarrow \frac{HI}{PT}$

(H C) → C
(H I) → P.

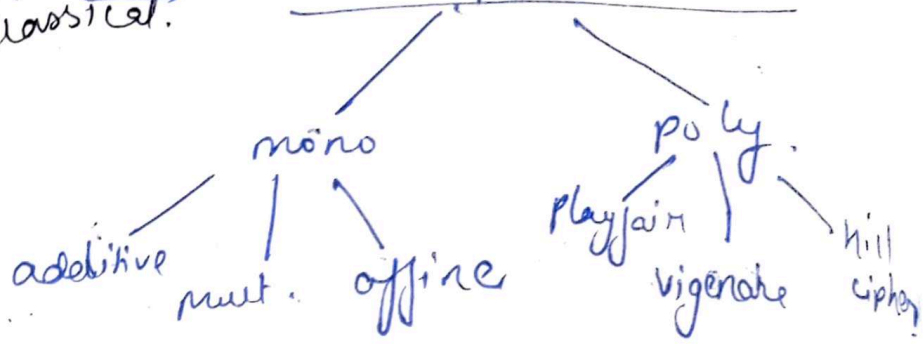
$$\begin{pmatrix} H & I \\ 7 & 8 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 & 2 \end{pmatrix}.$$

$$\begin{pmatrix} 11 & 1 \end{pmatrix} K \bmod 26 = \begin{pmatrix} 17 & 25 \end{pmatrix}.$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 1 \end{pmatrix} K \bmod 26 = \begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix}$$

- Cryptograph
  Traditional/classical cipher:

① Substitution cipher.



② Transposition cipher

② Transposition cipher :-

→ reordering ; change of position.

→ substitution gives change in the structure. Total no. of 0's & 1's in the bit level, ~~there~~ is different.

→ while in transposition, ~~affect~~ the no. of 0's & 1's will not be affected at bit level.

Diffusion & Confusion :-

↓ Hide the relationship b/w the cipher & the plain text. (no role of key).

↓ Hide relationship b/w cipher & the key.

without key

PT → PAY MORE MONEY TODAY.

P A Y M O R E M O N E Y T O D A Y

↳ Broke the text into two rows.

CT — PYOE O E TDAY AMRMNYOA.

→ This is a **keyless cipher**

→ if bandwidth is restrictive then we cannot just send the key and occupy the bandwidth so only the message is sent. Hence the throughput is high.

with a key :- eg (2 1 3 5 4).

↑ 5 different no.s then 5 different columns.

key → (2 1 3 5 4) ↑ DEC.

↓ ENC

Order → (1 2 3 4 5)

For the text, PAY MORE MONEY TODAY

key is 5 columns so column value is fixed only row is changing as per text.

→ row wise PT.

P	A	Y	M	O
R	E	M	O	N
E	Y	T	O	D
A	Y	x	Y	Z

↳ take any other alphabets if blank space is there.

(ENC)

A	P	Y	O	M
E	R	M	N	O
Y	E	T	D	O
Y	A	X	Z	Y

as per key index —

2 column is 1.
1 column " 2
4 " " 5
5 " " 4.

So the encryption is done in this way

column wise → CT → AEYY PREA YMTX ONDZ MOOY.

How do we decryption. —

→ double transposition — do one time transposition & then again do trans-position (with key) on the CT.

→ (3 BOX) , (PBOX / DBOX) .

→ In case of additive cipher,-

Let input = x
output = y.
key = k.

$$p + k = c$$

$$x_1 + k_1 = y_1$$

$$x_2 + k_2 = y_2$$

$$x_3 + k_3 = y_3.$$

This is on bit-wise operation.

↳ 3 bit SBox eqn.

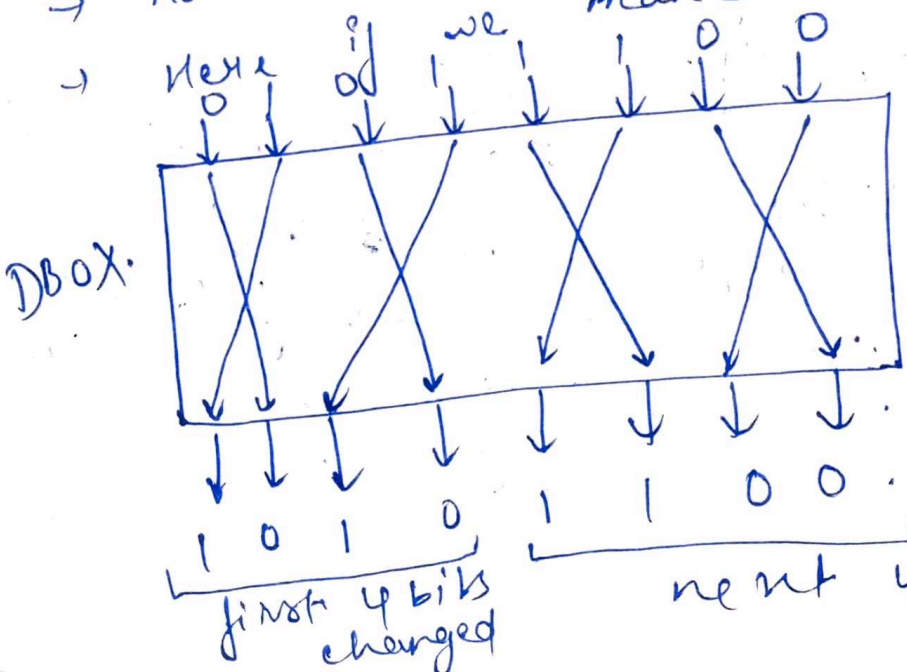
Building Blocks of Modern cipher.

1. Block size
2. Key size
3. Round No.
4. SBOXS / PBOXS
5. OPERATIONS (swap, shift & Inverse).

for doing / maintaining diffusion.

→ no role of key.

→ Here if we make DBox.



This is straight DBox.

→ This DBox can be used as compression and extension.

→ The no. of 0's & 1's remain same.

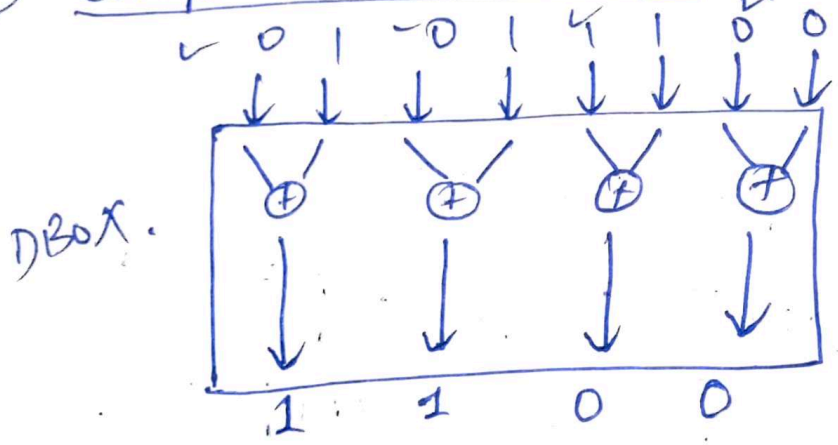
3 Types of DBOXS :-

① Straight DBox.

② Compressed DBox.

③ Extended DBox.

② Compressed DBox. (to compress the bits)



a ⊕ b = c

c ⊕ b = a

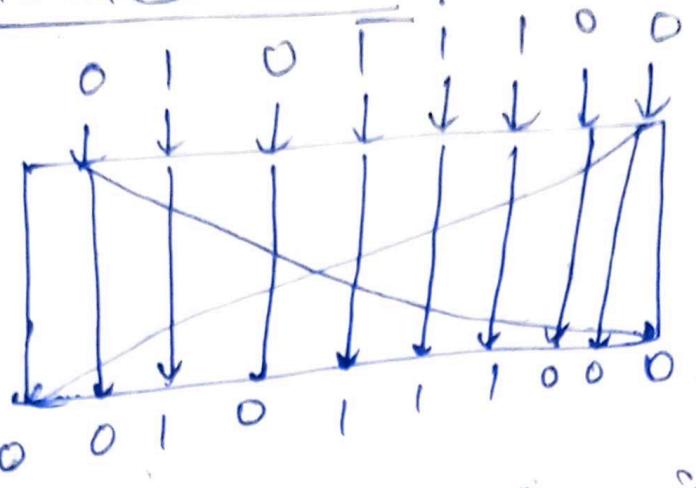
→ take operation in such a way that the decryption can also be done properly.

→ in decryption, the certain bits are known before hand & in form of vector — to do the following.

a ⊕ b = c

c ⊕ a = b.

③ Extended DBOX :- (Increased no. of bits).



(8 bits — 10 bits)

→ extension can be in many ways.

→ another way can be inserting bits

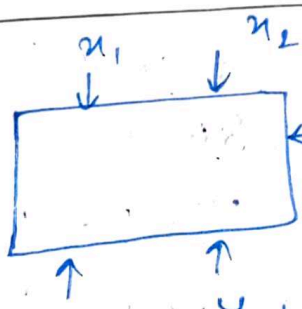
In Hw.

Eg - 0101 1010 1100

entries (taking rest of first 4 bits).

→ This is padding of 4 bits.

SBOX :-



$x_1 \oplus k_1 = y_1$

$x_2 \oplus k_2 = y_2$

Hlw ① Design an affine cipher where the keys depend on the position of the character in the plain text. If the plain text character to be encrypted is in position i.

we can find the key as —

multiplicative — M.I. key is $(i \bmod 12)^{th}$ element in Z_{26}^*.

Additive key is $(i \bmod 26)^{th}$ element in Z_{26}.

Encrypt the message "PAYMORE MONEY".

$(P \times K_1) + K_2$ = CT.

	P	A	Y	M	O	R	E		M	O	N	E	Y.
	0	1	2	3	4	5	6		7	8	9	10	11
K_1	1	3	5	7	9	11	15	17	19	21	23	25	

M.I. $= K_1 \bmod 12 = 0^{th} = 1$

$P = \{(15 \times 1) + 0\} \bmod 26 = 15 \bmod 26 = 15 = P$

$A = \{(0 \times 3) + 1\} \bmod 26 = 1 \bmod 26 = 1 = B.$

$Y = (24 \times 5) + 2 = 122 \bmod 26 = 18 = S.$

$M = (12 \times 7) + 3 = 27 \bmod 26 = 9 = J.$

$O = (14 \times 9) + 4 = 130 \bmod 26 = 0 = A$

$R = (17 \times 11) + 5 = 192 \bmod 26 = 10 = K.$

$E = (4 \times 15) + 6 = 66 \bmod 26 = 14 = O$

$M = (12 \times 17) + 7 = 3[illegible] \bmod 26 = [illegible] D.$

$O = (14 \times 19) + 8 = 14 \bmod 26 = 0.$

$N = (13 \times 21) + 9 = 282 \bmod 26 = 22 = W.$

$E = (4 \times 23) + 10 = 102 \bmod 26 = 24 = Y.$

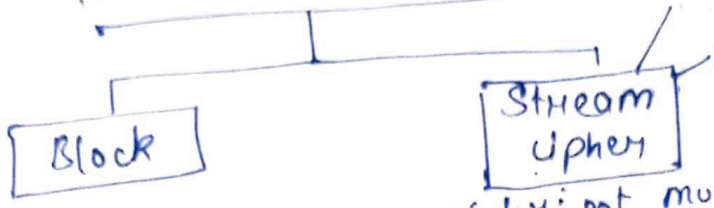
$Y = (24 \times 25) + 11 = 611 \bmod 26 = 13 = N.$

Cipher Text

= PBSJAKODOWYN

17/2/23

→ Modern ciphers.



(RC4) → structures are the building blocks.
LFSR
→ they have certain components.

components

1) Block size – size will be based on processing size.
2) Key.
3) SBox – substitution boxes.
4) DBox – : diffusion boxes.
5) Operations.
6) Round structure (repeat same operation).

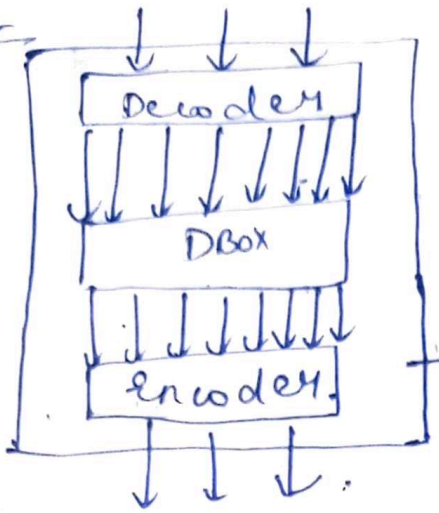
→ if block size (n bit) then it can process n bits.

→ Block ciphers have inbuilt strength of security while stream cipher doesn't.

① Block size:-

② Key – key size is normally equal to or more than the block size.
↳ if key size is small then brute force attack is possible. So size must be high. So keep block size as high as possible.

③ SBox / DBox – mainly contains Idea of substitution & transposition.



→ n bits (input) map to 2^n bits as output

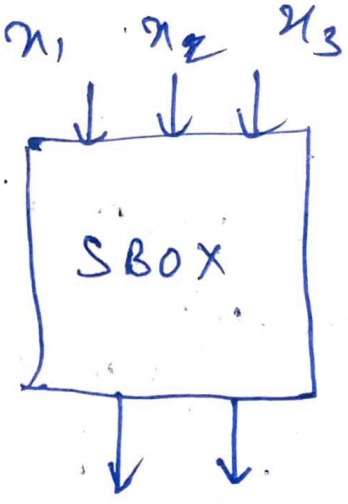
2^n bits (input) → n bits (output)

→ Here — no key is present.

→ In decoder — $(2^n - 1)$ no. of 0's & rest 1.

Product ciphers.

↳ concept of using (key mixers), SBox, and DBox.



SBox

Linear (eg)

$y_1 = x_1 \oplus x_2 \oplus x_3$

$y_2 = x_1 \oplus x_3$.

→ Linear SBox

→ Non Linear SBox.

Non - Linear (eg)

$y_1 = x_1 x_2 \oplus x_2 x_3$

$y_2 = x_1 \cdot x_2 \cdot x_3$

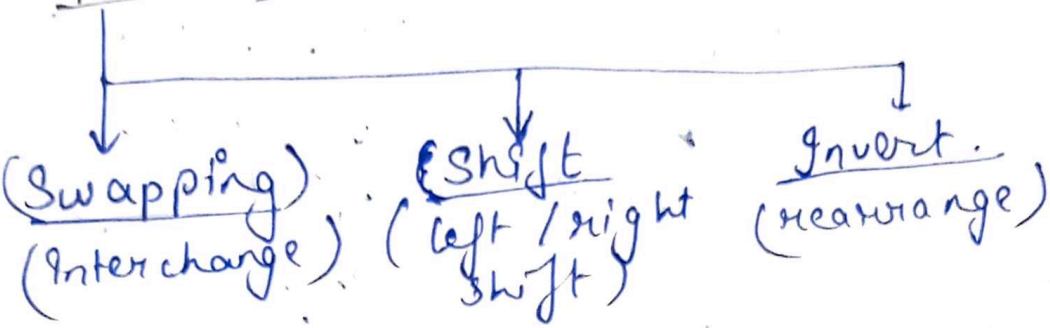
↑ AND operation for multiplication.

⊕ → for addition operation.

→ when bit size is huge then we represent in polynomial time

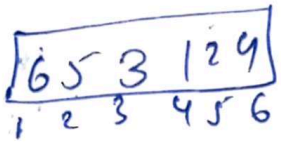
→ Linear SBoxes ~~are~~ are not that strong.

(5) Operations :-

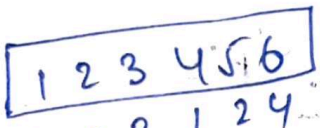


Invert

Step1

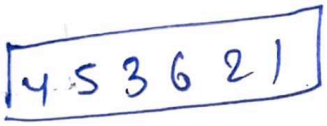


Step2



1 will be 6th position
2 will be 5th posit.
.... So.... on.

Step3



→ when input & output bits are same then that is very weak cipher & we need to repeat the process of cipher so that it is strong. That's why we use round structure.

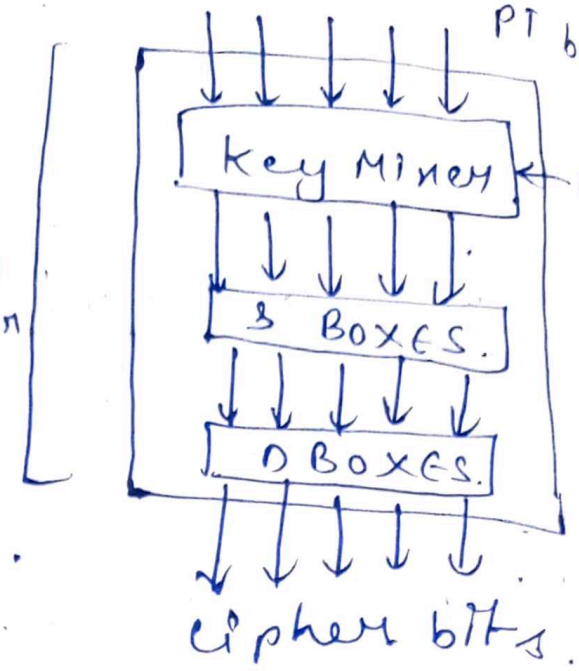
→ Avalanche effect. (repeating round structure)

Product ciphers :-

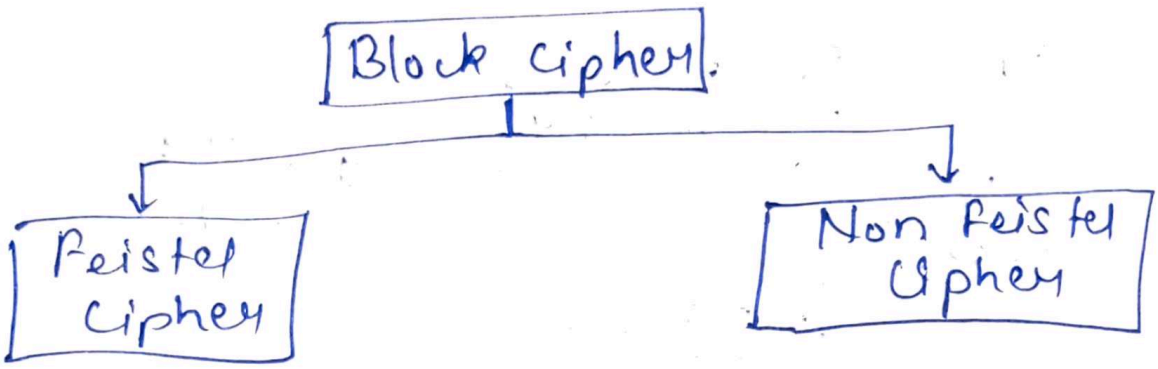
⇒ same no. of bits at input & output.

⇒ key is the round key.

⇒ different operations can be performed.



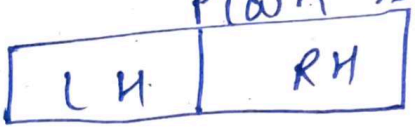
round structure



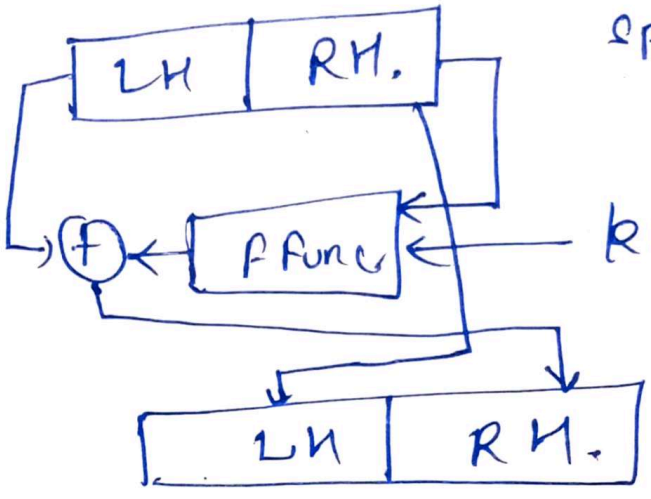
Feistel cipher.

→ break PT into two halves.

Plain Text.



→ function :- will take two input.



Syllabus

DBMS Structures

Set Z_n, Z_n^*

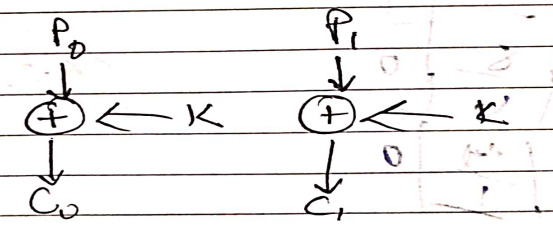
Group of $< Z_n, + >$
$< Z_n, \times >$

Block ciphers

i) BlockSize $-(2^n) - 8$
KeySize $-(2m) - >$ BlockSize.

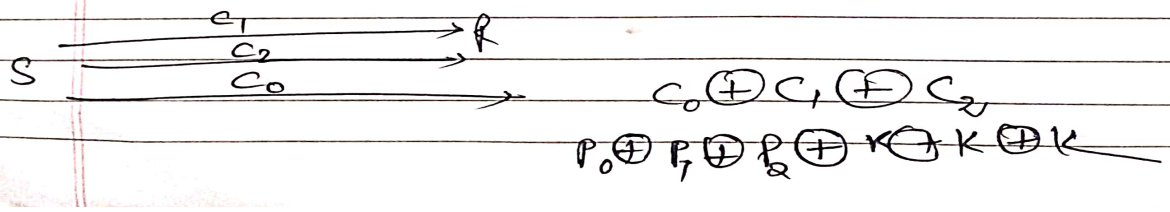
Confusion & Diffision
↓
Hide (CT + K) (C & P)

$C = P \oplus K$ Encryption
$P = C \oplus K$ → Decryption

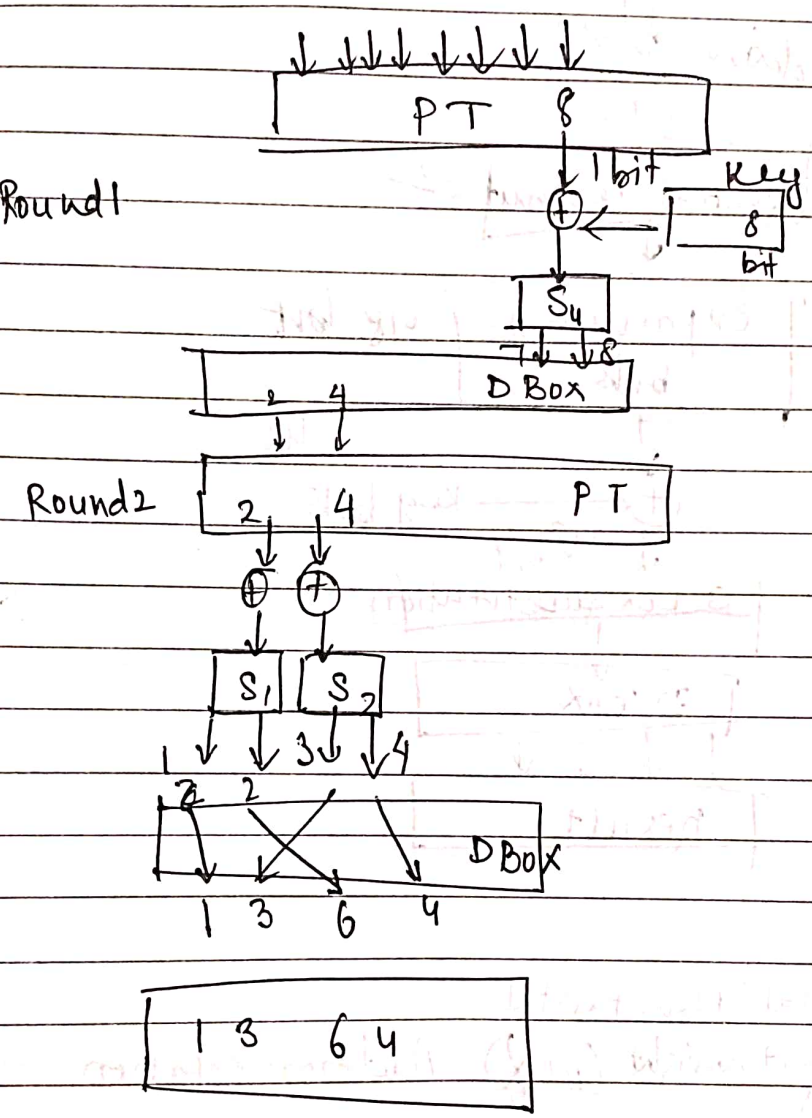


Key is a predefined
Key is for a session

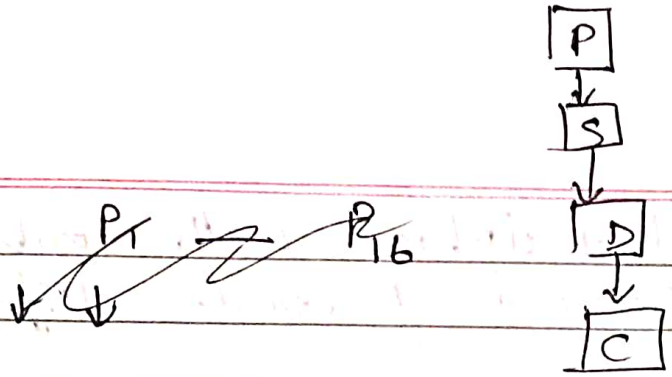
Attacker



How a product cipher with combination of SBox & DBox can guarantee diffusion and confusion.

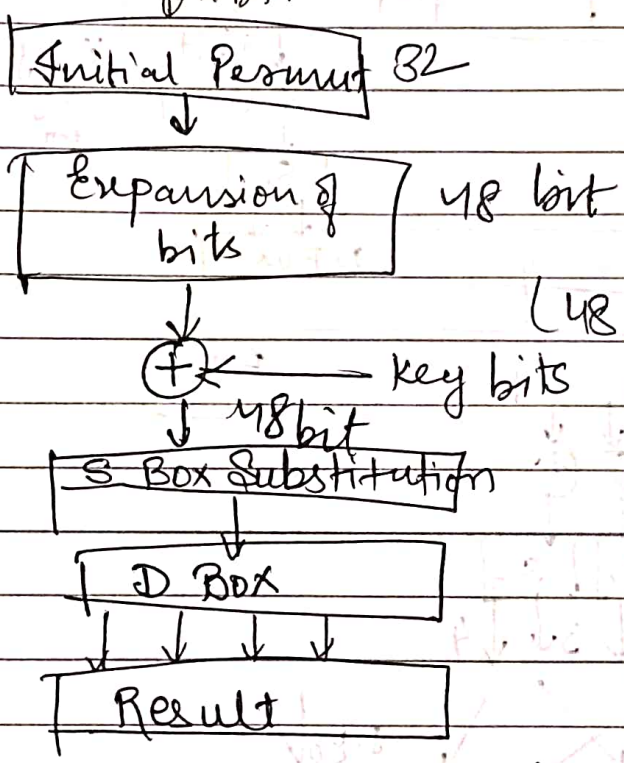


SPN - Substitution Permutation Network.



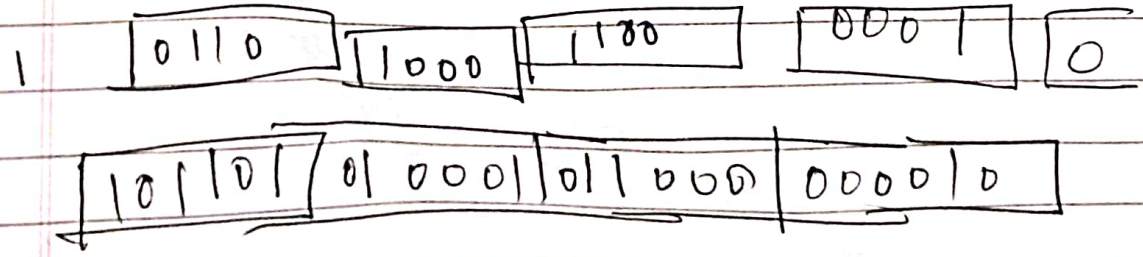
Feistal & Non-feistal structure

Feistal function block



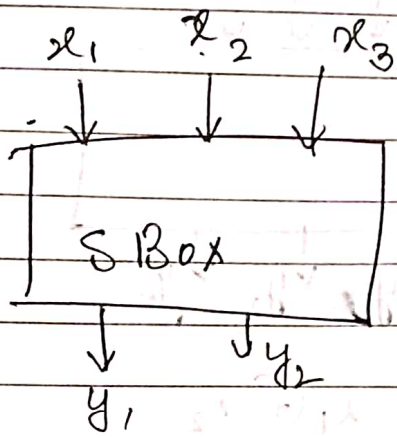
1) SPN
2) Feistal | Non-feistal
3) Lightweight (ARX) Addition Rotation XOR).

Sublock – 8



Key (64 bit) – 56 bit (after removing parity bit)

56 — after doing evering rounds
48 bit



$y_1 = x_1 \oplus x_2 \oplus x_3$

$y_2 = x_1 \oplus x_3$

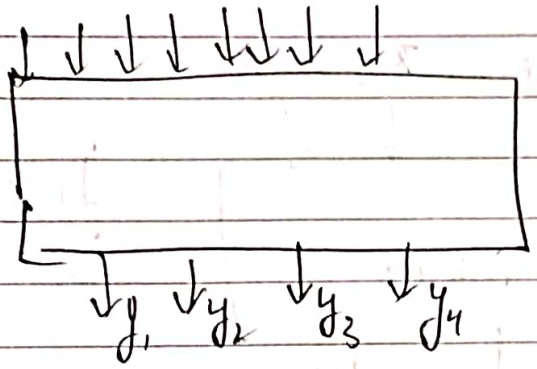
	000	001	010	011	100	101	110	111
y_1	0	1	1	0	1	0	0	1
y_2	0	1	0	1	1	0	1	0

x_1	x_2	x_3	y_1	y_2
0	0	0	0	0
0	0	1	1	1
0	1	0	1	0
0	1	1	0	1
1	0	0	1	1
1	0	1	0	0
1	1	0	0	1
1	1	1	1	0

$y_1 = x_1 x_2 \oplus x_2 \cdot x_3$

$y_2 = x_1 \cdot x_2 \cdot x_3$

Let us construct one feistal function with 16 bit input and key size is 32bit ⊕ & with 4 SBoxes and show the output



$y_1 = x_1 \oplus x_2$

$y_2 = x_3 \oplus x_4$

$y_3 = x_5 \oplus x_6$

$y_4 = x_7 \oplus x_8$.

| A D C F | → Input

| ? | → Output.

Block Cipher
Property
Building Structures
Types of
How feistal cipher/
function designed

Use of Brute force attack to decipher the ~~plain~~ affine cipher where, assume 'ab' is enciphered to 'GL'

XPALASXYFGFUKPXU

Date 07/02/2023

Date 21/02/2022

Blockciphers

1) Blocksize (2^n)
2) Keysize $(2m) \geq$ Blocksize

Bruteforce attack → ciphertext to get the key

3) Blocksize must be in a size of (2^n) ↓ LWBC (Light weight Block Ciphers)

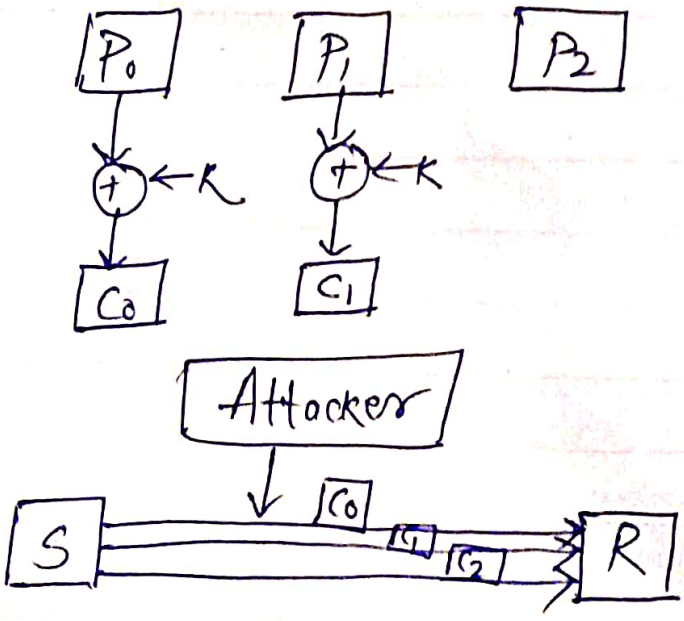
Z_n Z_n^*

→ Group. G1 $\langle Z_n, + \rangle$
$\langle Z_n^*, X \rangle$

* Confusion & Diffusion
Hide (CT+K) (C & P)

$C = P \oplus K$ → Encryption

$P = C + K$ → Decryption



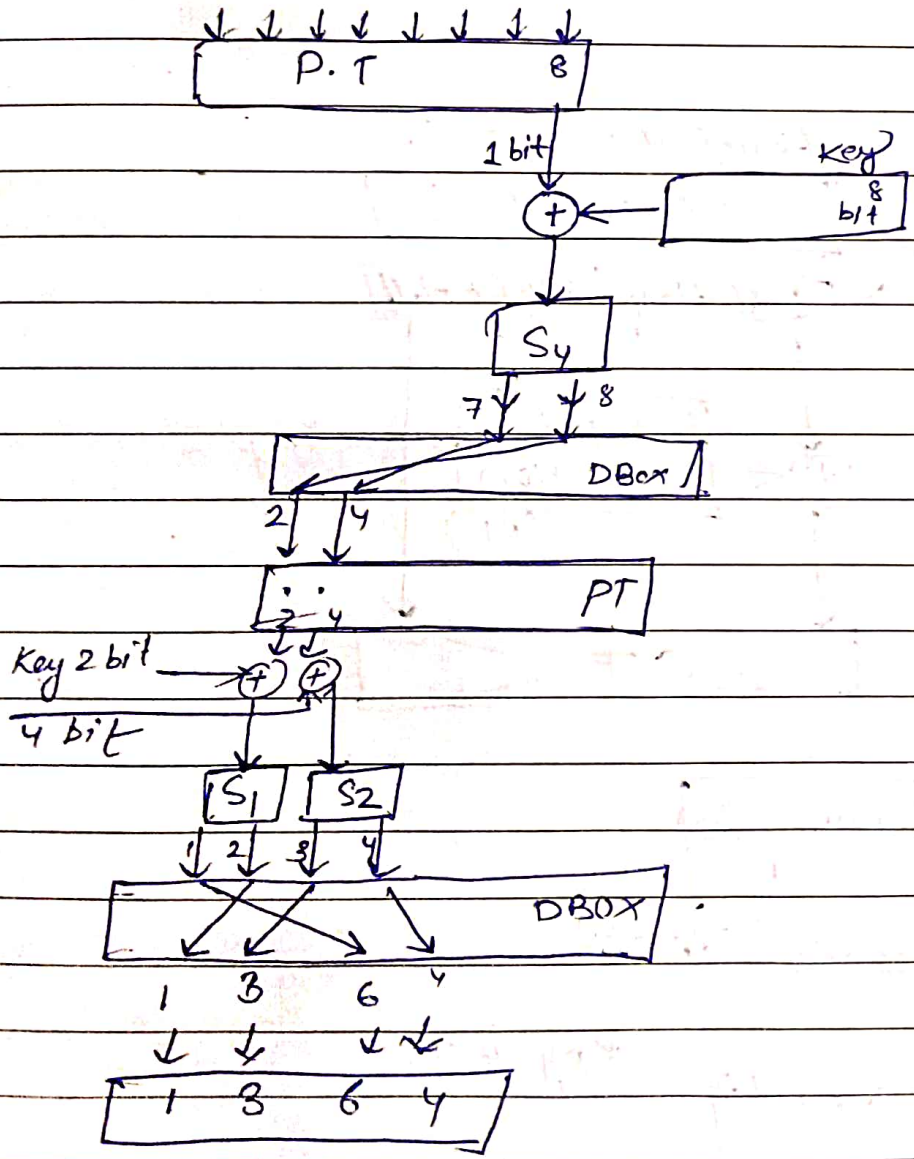
$C_0 = P_0 \oplus K$
$C_1 = P_1 \oplus K$
$C_3 = P_2 \oplus K$

PAGE NO.:
DATE : / /

$C_0 \oplus C_1 \oplus C_2 = P_0 \oplus K \oplus P_1 \oplus K \oplus P_2 \oplus K$

$= P_0 \oplus P_1 \oplus P_2$

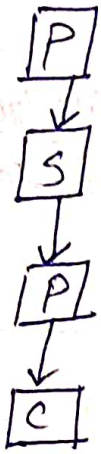
Q How a product cipher with combination of S Box & D Box can guarantee diffusion and confusion.

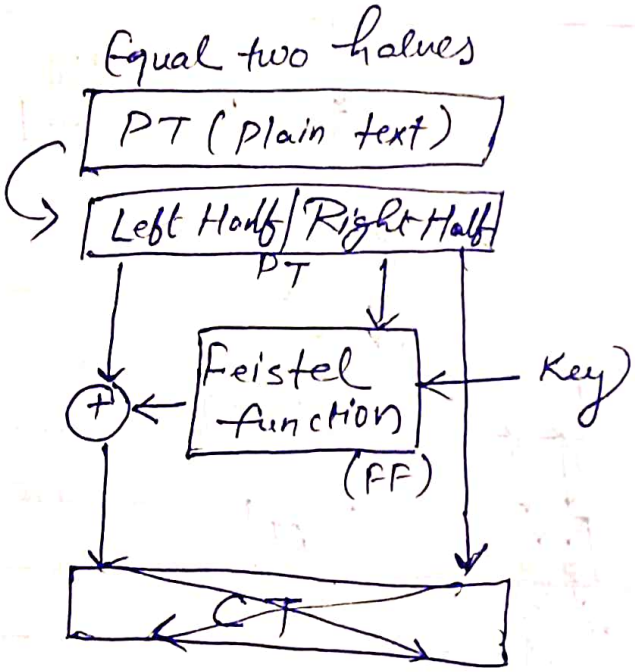


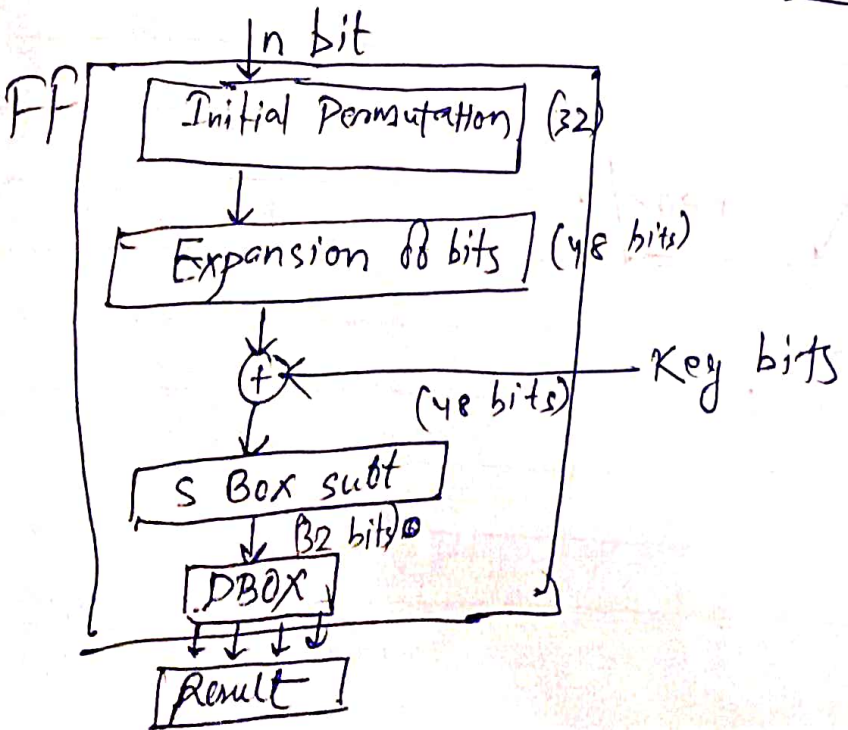
Teacher's Signature

* Feistel & Non Feistel Structure :-

S P N → Substitution Permutation Network





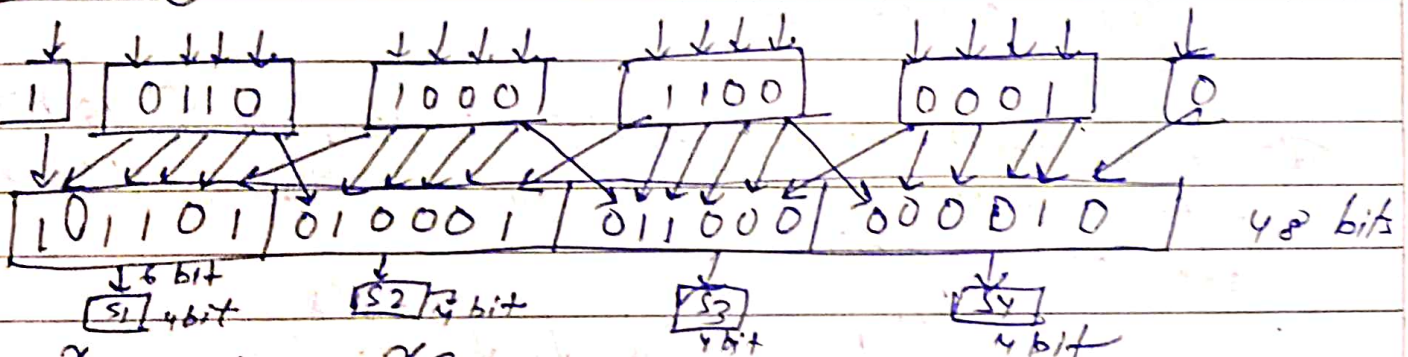


PAGE NO.:
DATE : / /

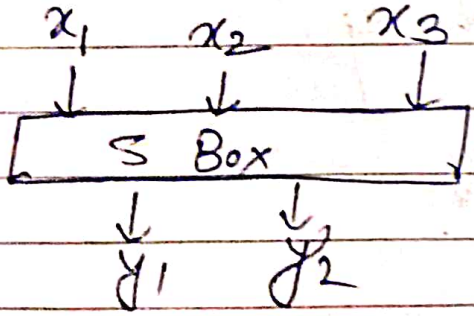
* 1) SPN
2) Feistel / Non-feistel
3) ARX (Addition Rotation XOR)

* (1) Swaping
(2) Spliting
(3) Circular shift
(4) Invert

* Subblock - 8 (4 bit each)



*



$y_1 = x_1 \oplus x_2 \oplus x_3$

$y_2 = x_1 \oplus x_3$

	000	001	010	011	100	101	110	111
y_1	0	1	1	0	1	0	0	1
y_2	0	1	0	1	1	0	1	0

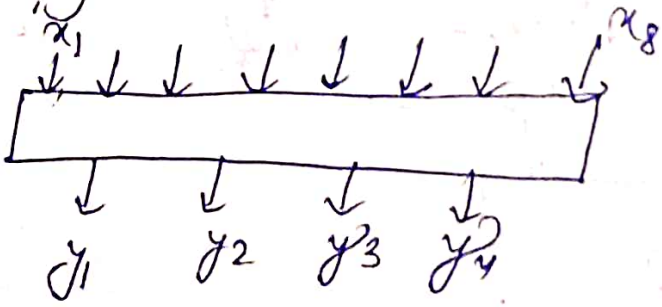
Teacher's Signature

x_1	x_2	x_3	y_1	y_1
0	0	0	0	0
0	0	1	1	1
0	1	0	1	0
0	1	1	0	1
1	0	0	1	1
1	0	1	0	0
1	1	0	0	1
1	1	1	1	0

(*) →

$$y_1 = x_1 x_2 \oplus x_2 \cdot x_3$$
$$y_2 = x_1 \cdot x_2 \cdot x_3$$

(*) Let us construct one feistel function with 16 bit input and key size is 32 bit with 4 SBOX and show the output.



$$y_1 = x_1 \oplus x_2$$
$$y_2 = x_3 \oplus x_4$$
$$y_3 = x_5 \oplus x_6$$
$$y_4 = x_7 \oplus x_8$$

PAGE NO.:
DATE : / /

ADCF → Input

[?] → Output

Q. Use a bruteforce force attack to decipher the affine cipher where assume 'ab' i.e enciphered to 'GL' XPALASXYFGFUKPXU.