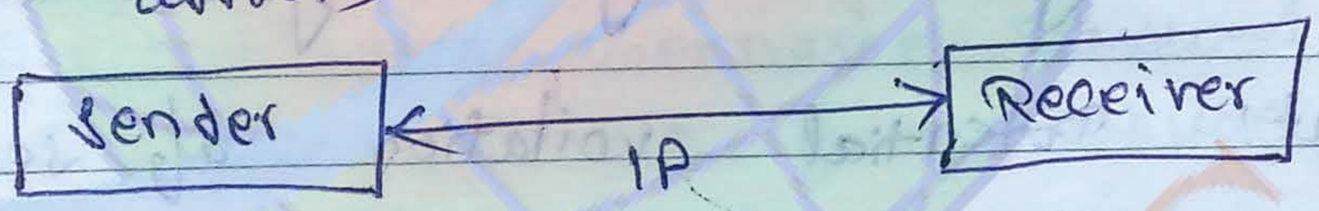
Network Security

Date : / /
Page No :

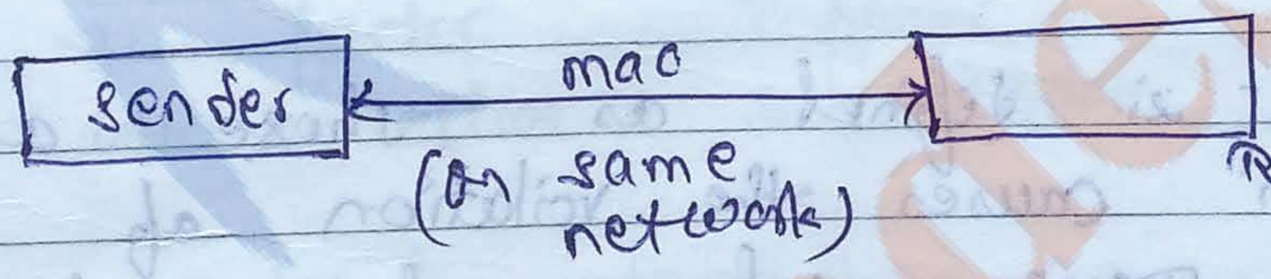
IPV4 - 32 bit
ip config
getmac
Datalink layer - mac address
TCP/IP
Provides segmentation → Packets
error control
Provides IP, Routing function

IP address - IPV4 32 bits - IPV4 - 128 bit

mac address - It is in hexadecimal, 48 bit
port address 16 bit - TCP Protocol address
(Process address)



(on different network)



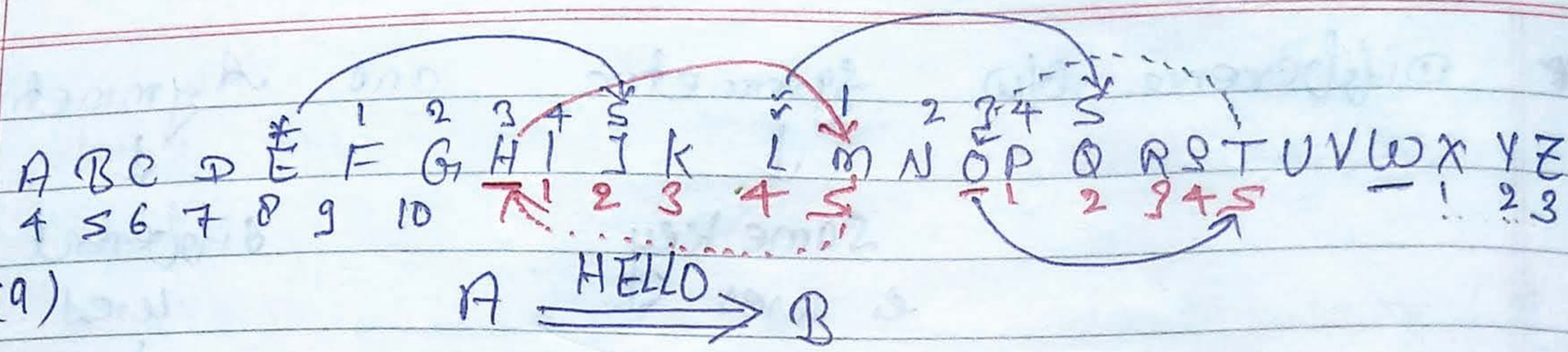
(On same network)

Port address - 0 to 65535
↳
to Promote multitasking.

IPv4 - Public and Private IP

max no. of Combinations 2^{32}
Same IP's for multitasking
class A, class B, class C, class D, class E
reserved

Date : / /
Page No :



(a) A ⟹ B

P = HELLO ← plain text

C = MJQQT

encryption ($\xrightarrow{enc}$)
$k = \downarrow 5$
decryption ($\xleftarrow{decr}$)
$k = -5$

(b) P = WISDOM
C = GSCNYW
k = 10

- monoalphabetic ciphers

P = Room

C = OLLJ

monoalphabetic

k = -3 (encryption)
k = 3 (decryption)

"Caeser cipher" because key = 3 is given by Joulous Caeser

* Polyalphabetic ciphers-

P = Room

-3 -4

k = -3
k = -4

C = OLKI

Date : / /
Page No :

* P = Hello my dear

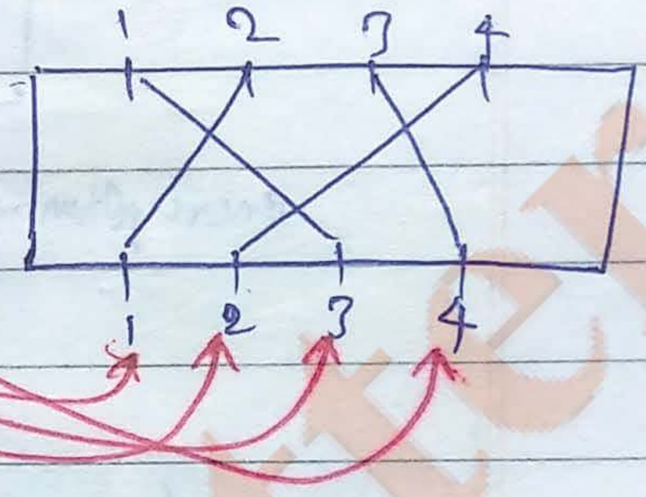
↳ firstly we have to remove spaces

= Hellomy dearz → dummy
k=2 k=5 k=7 k=7 k=11

* Transposition

P = ~~Hello~~ HELL

C = ~~Eolo~~ ELHL K =



* Bitwise ciphers :

(1) XOR ciphers

→ ~~Length~~ of plaintext and key should be same

Plaintext ⊛ key = encryption
= ciphertext

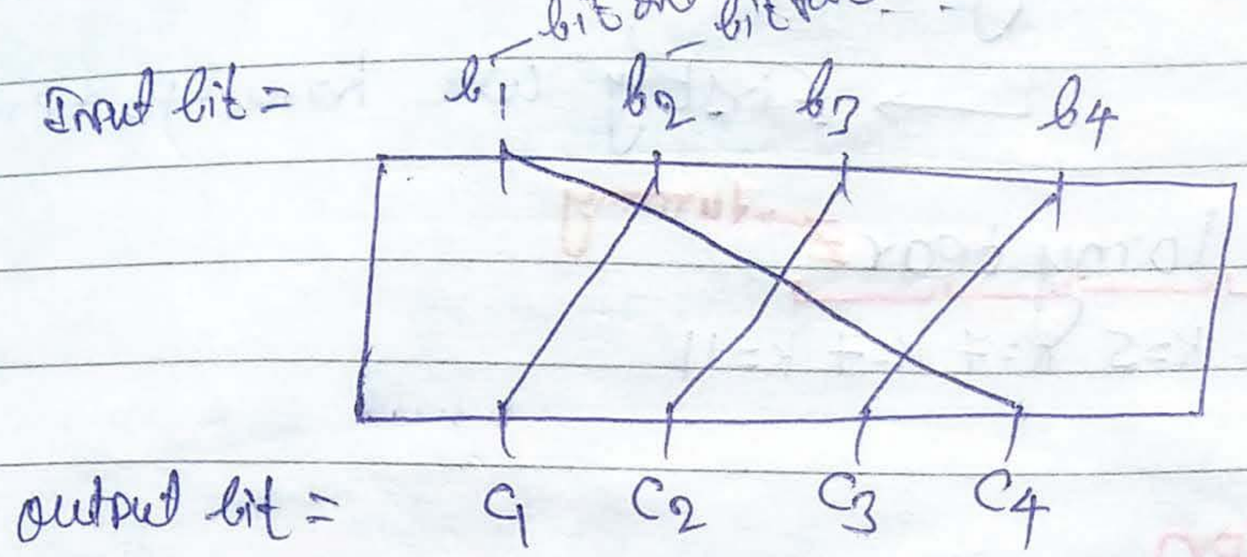
P-plaintext
C-Cipher
Key = one

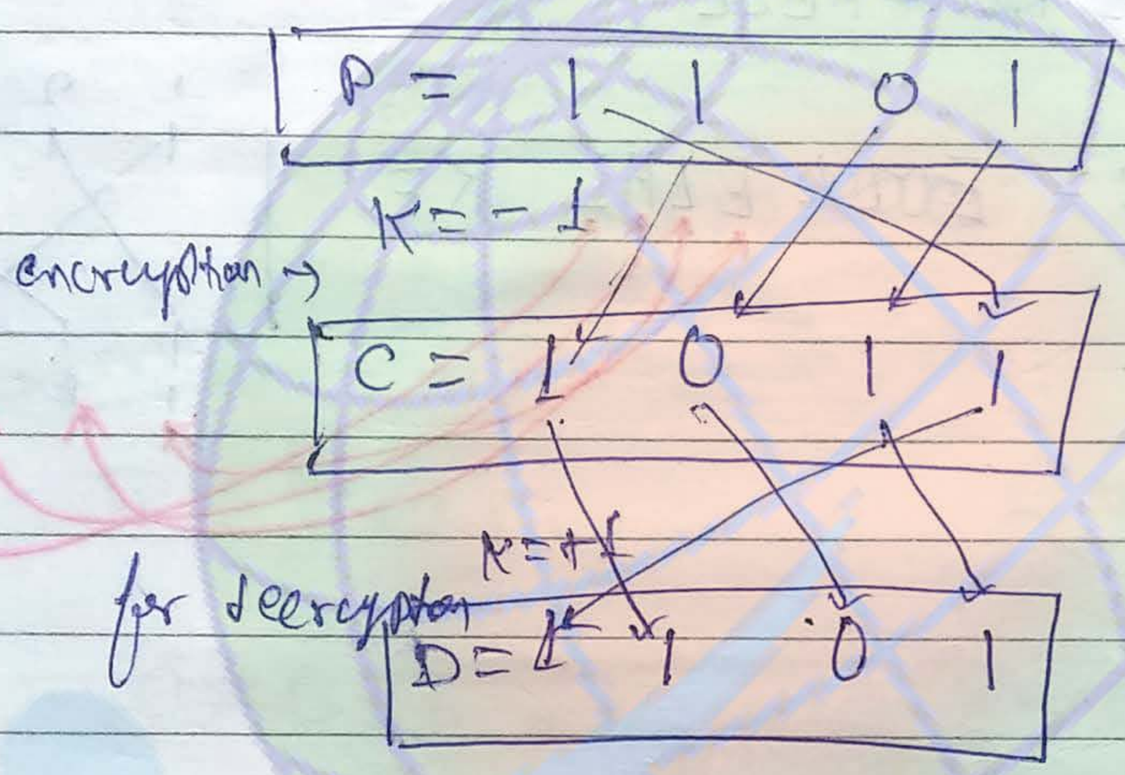
ciphertext ⊛ key = plaintext

P = 1101001
K = 1001100
C = P ⊛ K
C = PK + P̄K
10 + 01 = 0
C = 0100101 ← encryption

Decryption
D = C XOR K
C = 0100101
K = 1001100
P = 1101001

(2) ~~Caesar~~ Rotation ciphers: -





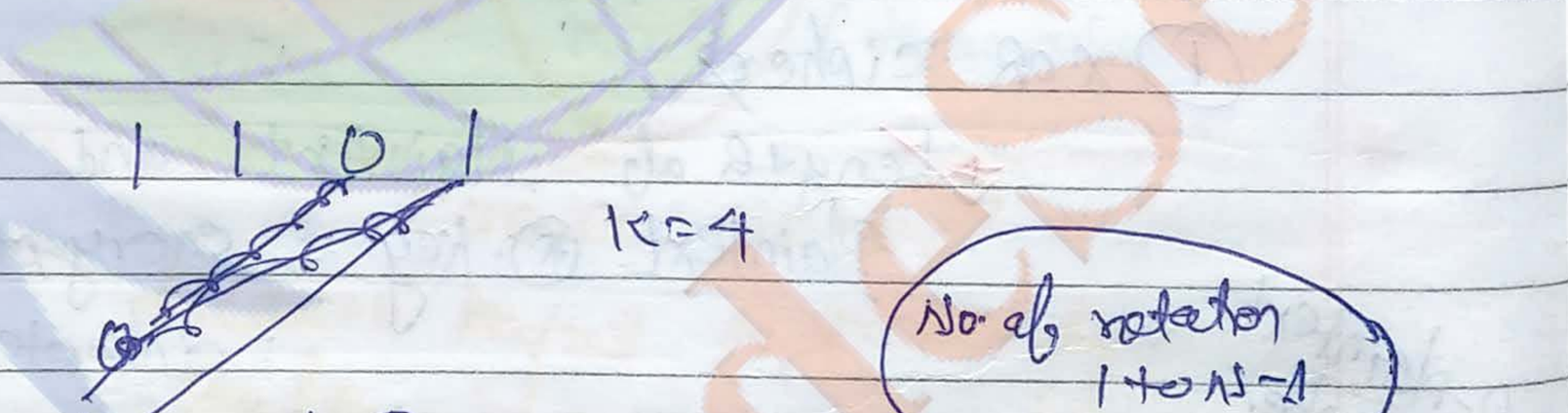
* P = 1 1 0 1

K = 3 K = 4

1 1 1 0

No. of rotation
1 to N-1

(3) S-box cipher



nversion is based
n some mathematical
function or
table."

" M and N have may same number of bits or not"

SARAA

Date: / /
Page No:

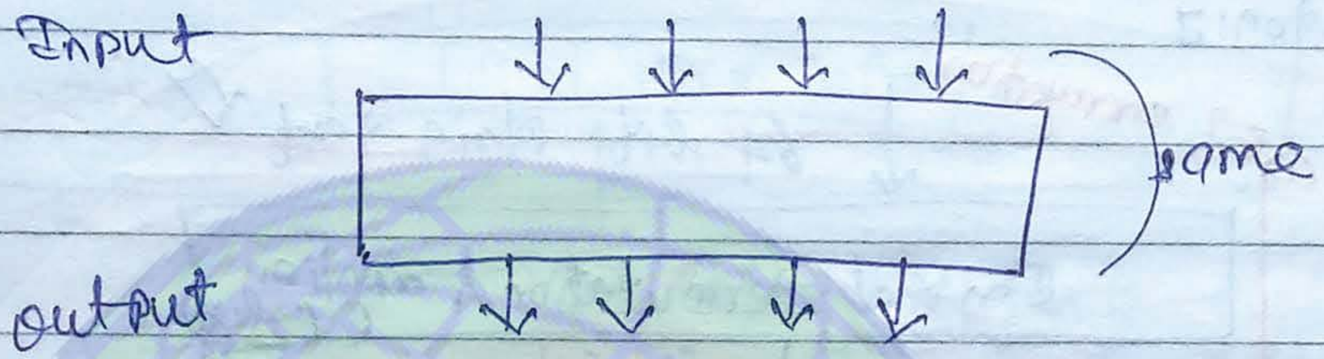
(4) P-box (Position change) cipher

Permutation box cipher

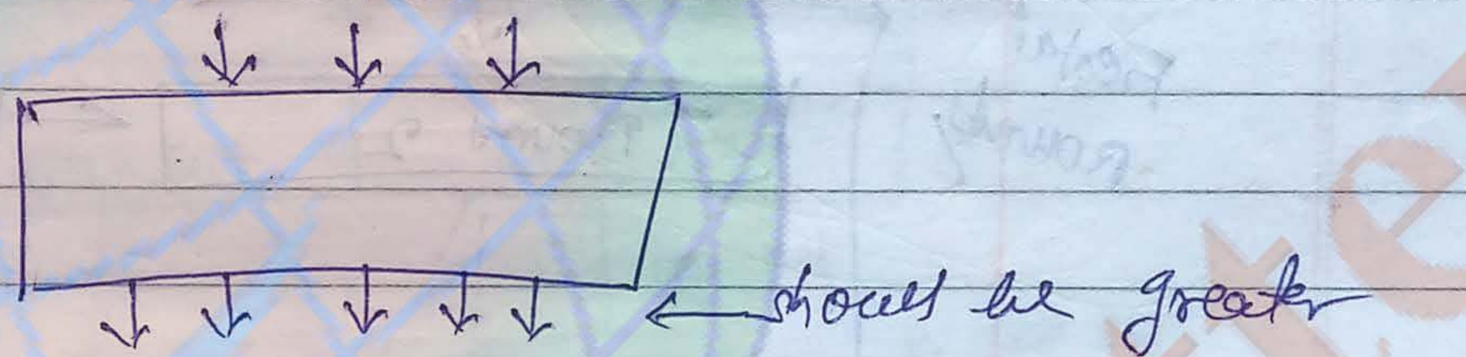
Three types of Permutation

(1) straight P-box

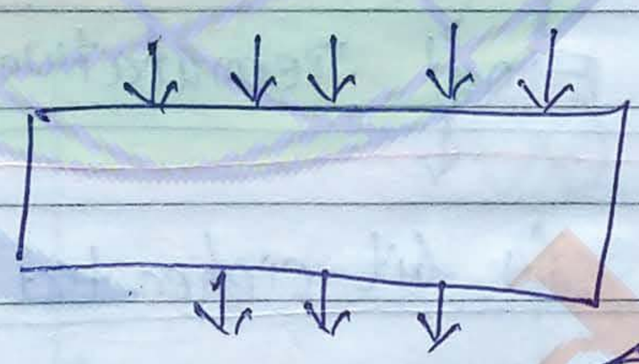
"Number of input and output should be same."



(11) expantion P-box



(111) Compression P-box:-



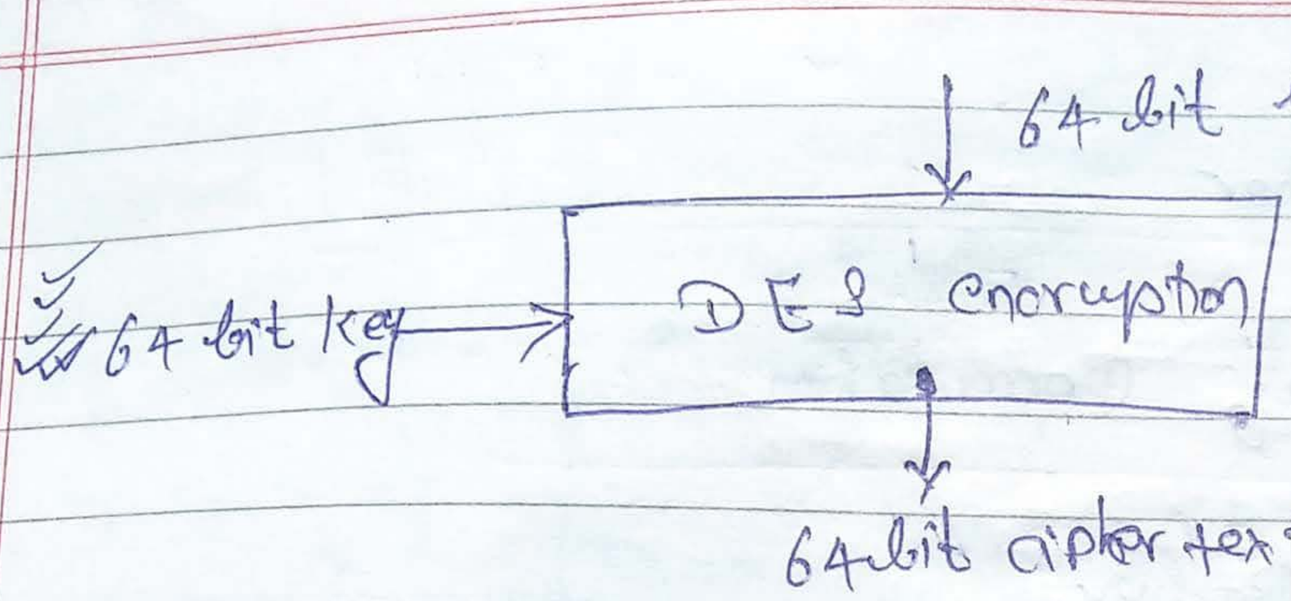
(•) Block Ciphers

↳ make a block by combination of bit's.

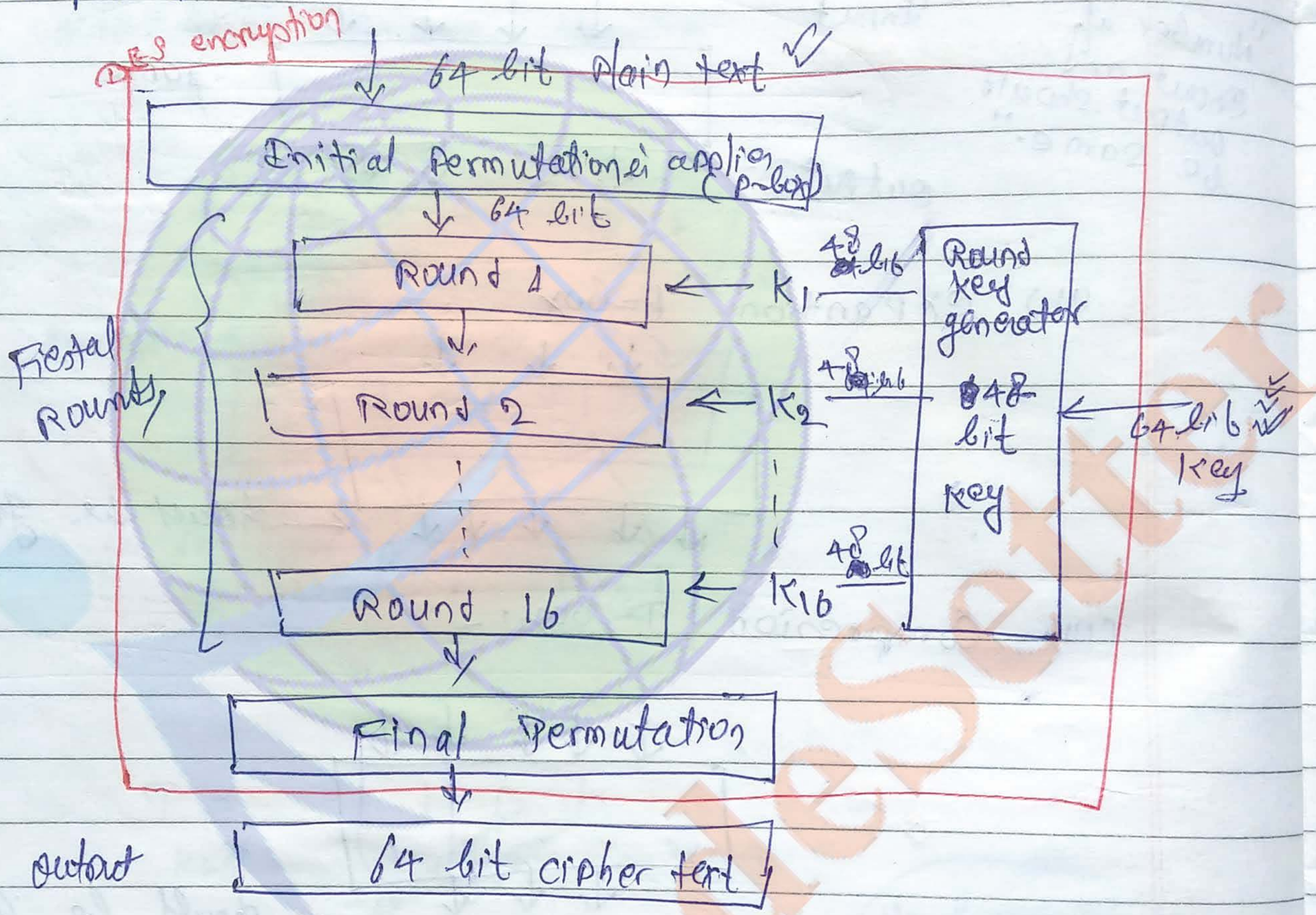
(1) Data encryption standard
(11) Advance encryption standard.

(1) Data encryption Standard
↳ developed by IBM
↳ takes input as a blok of 64 bits.

Date : / /
Page No :

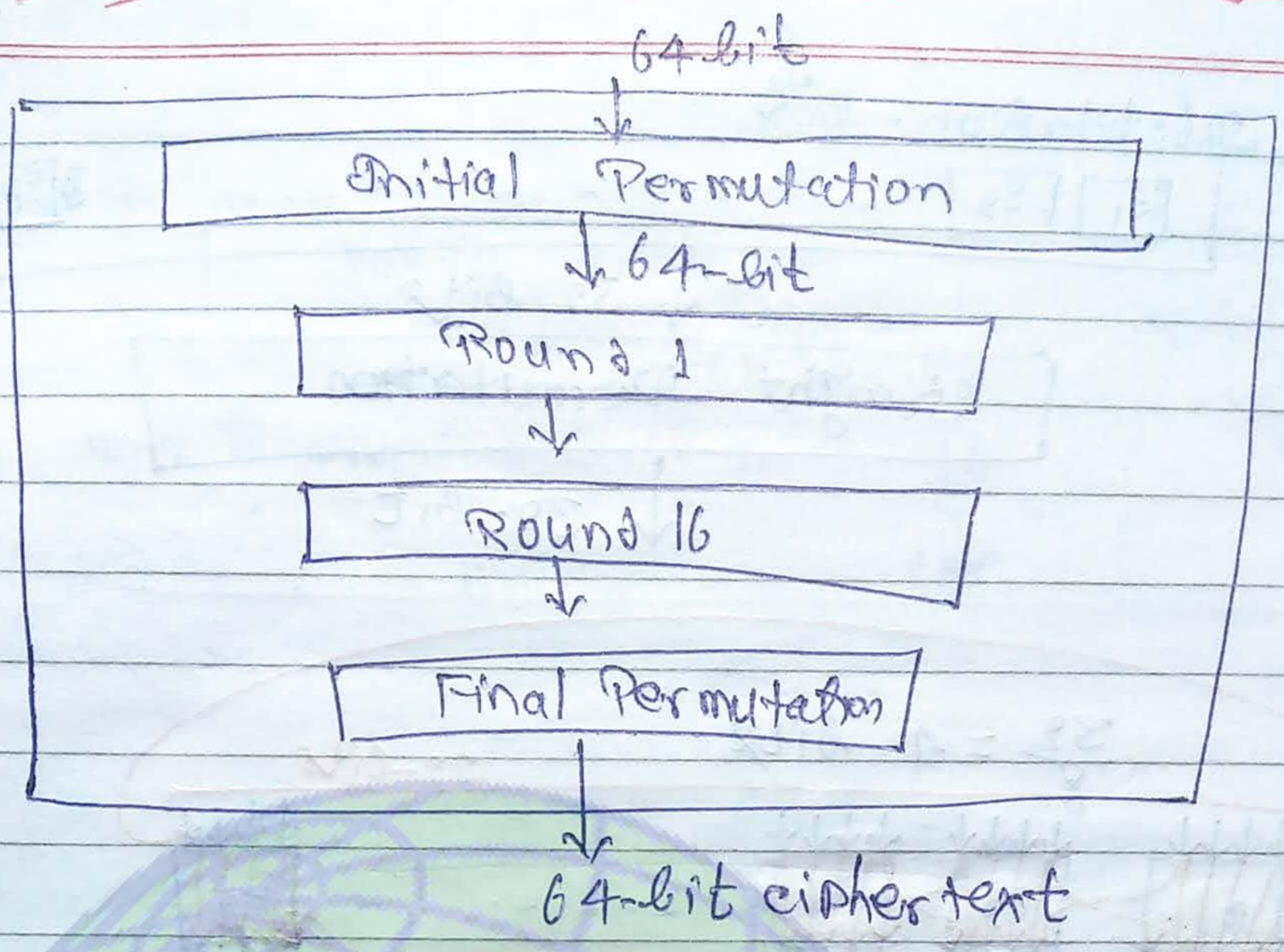


encryption:

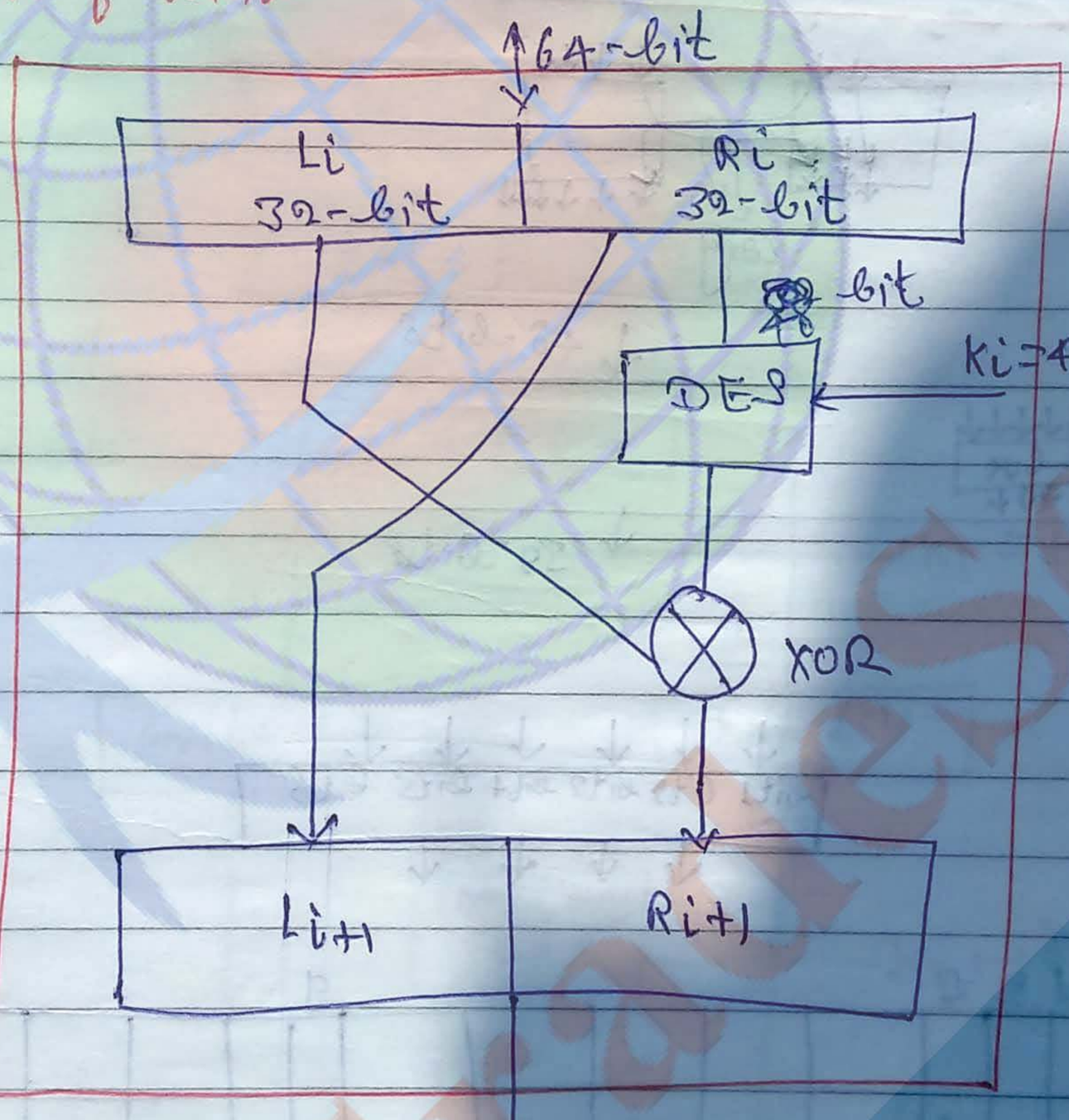


* DES - Data encryption standard

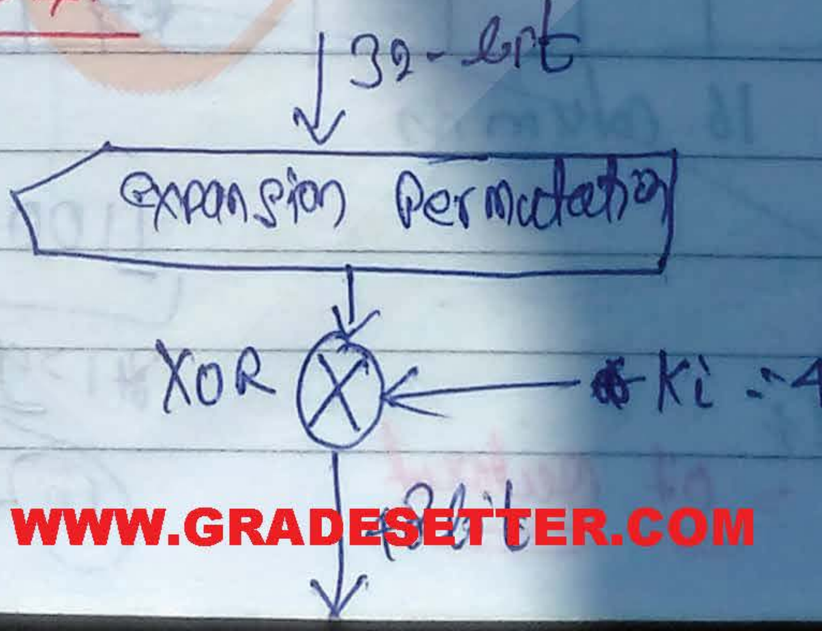
Date: / /
Page No:

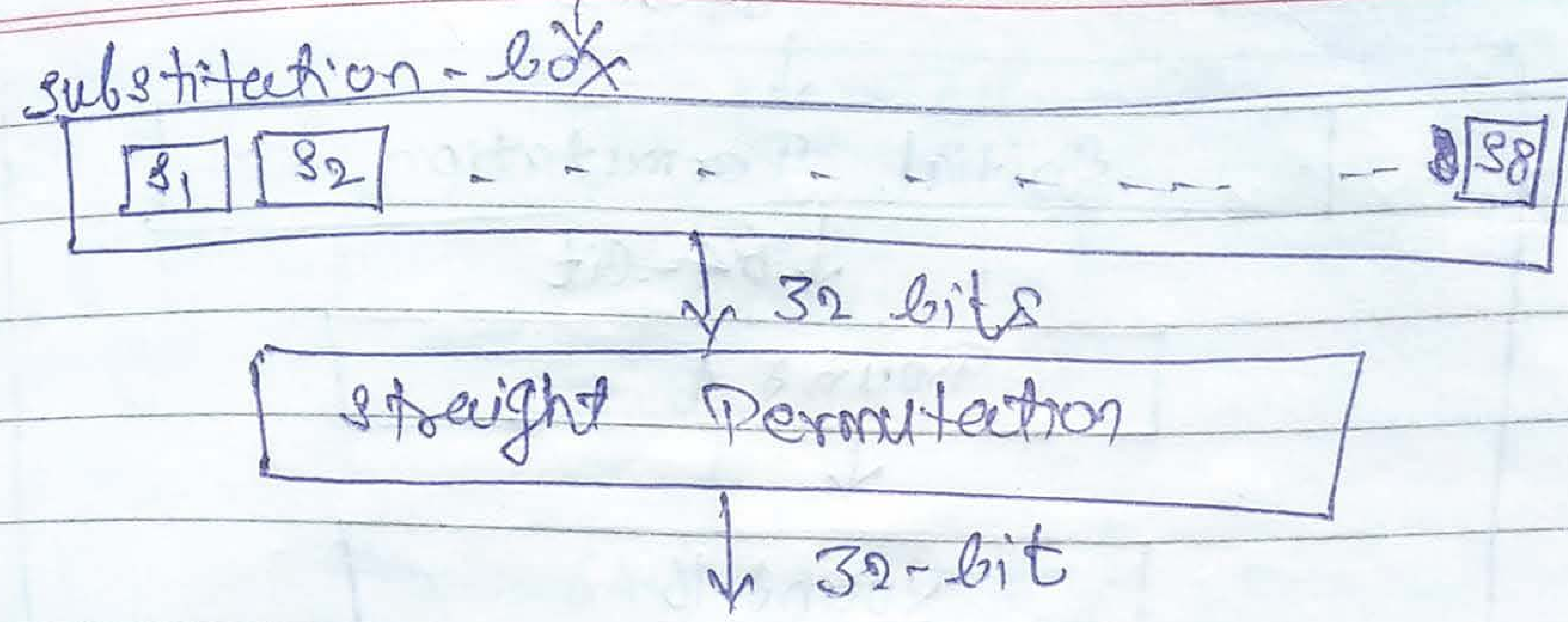


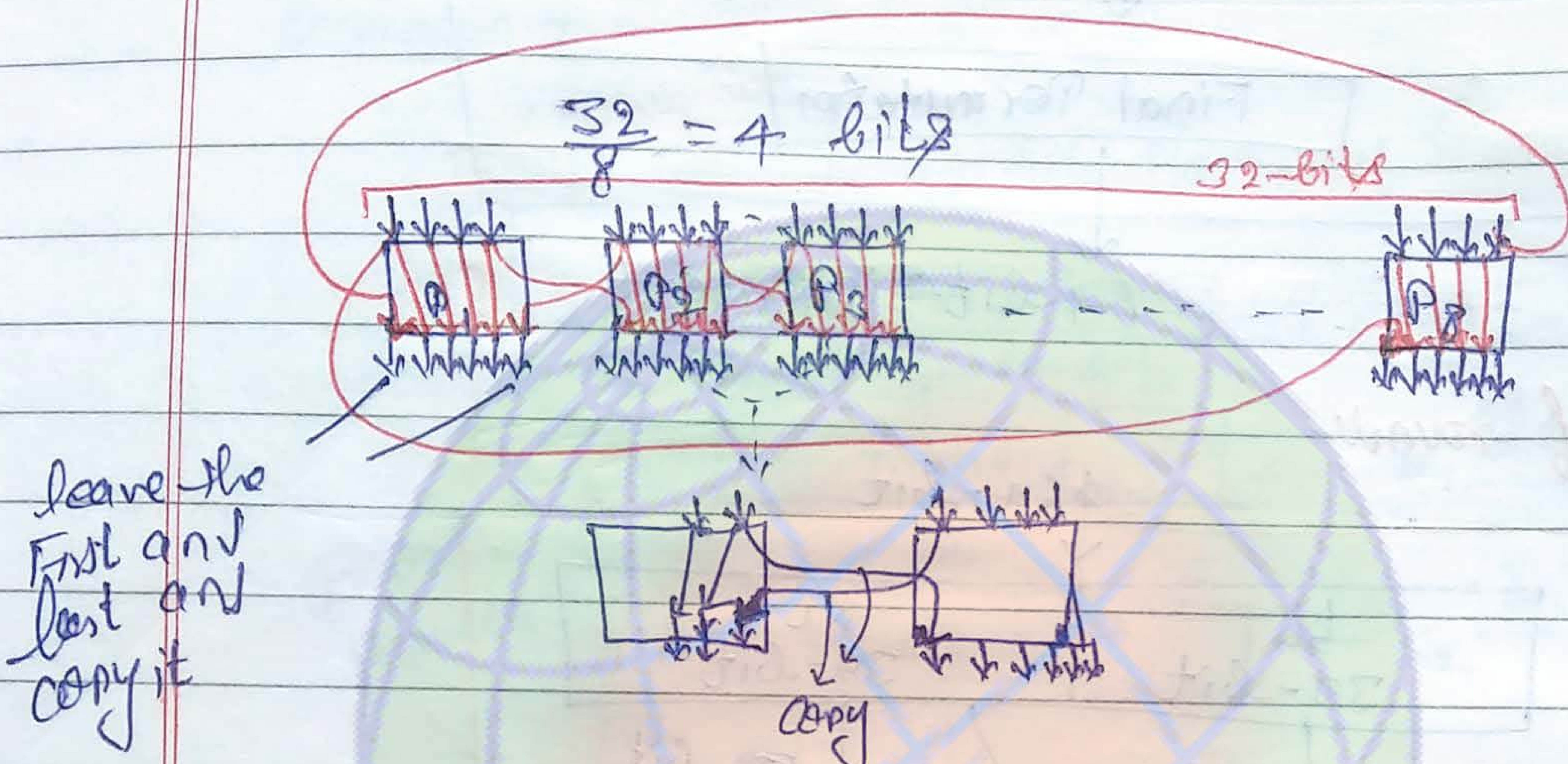
* Structure of round:-

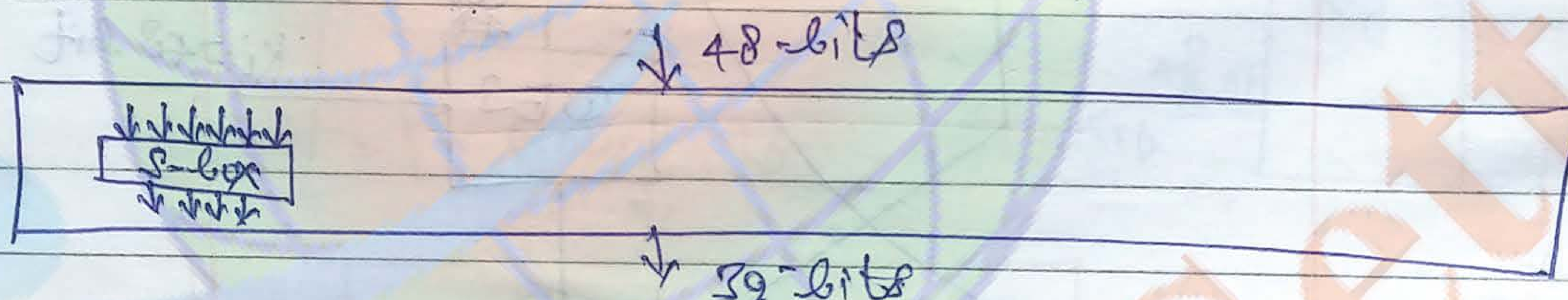


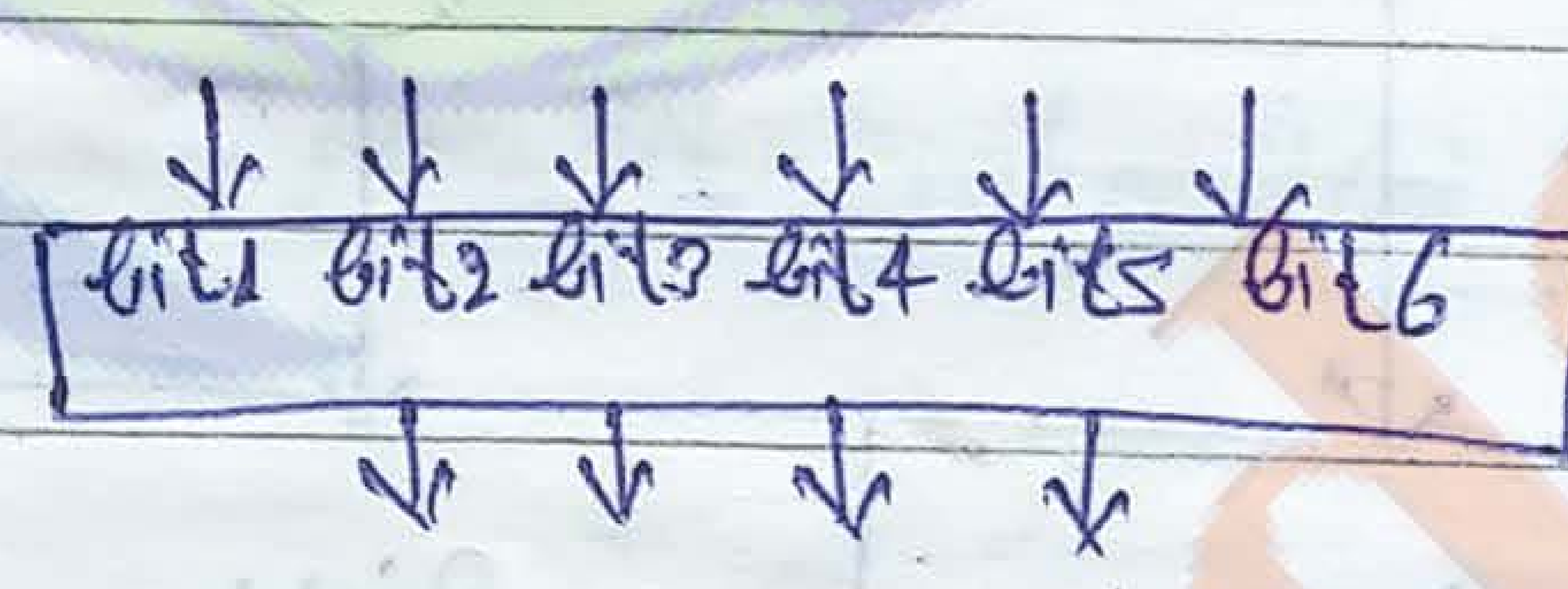
* DES Function:-

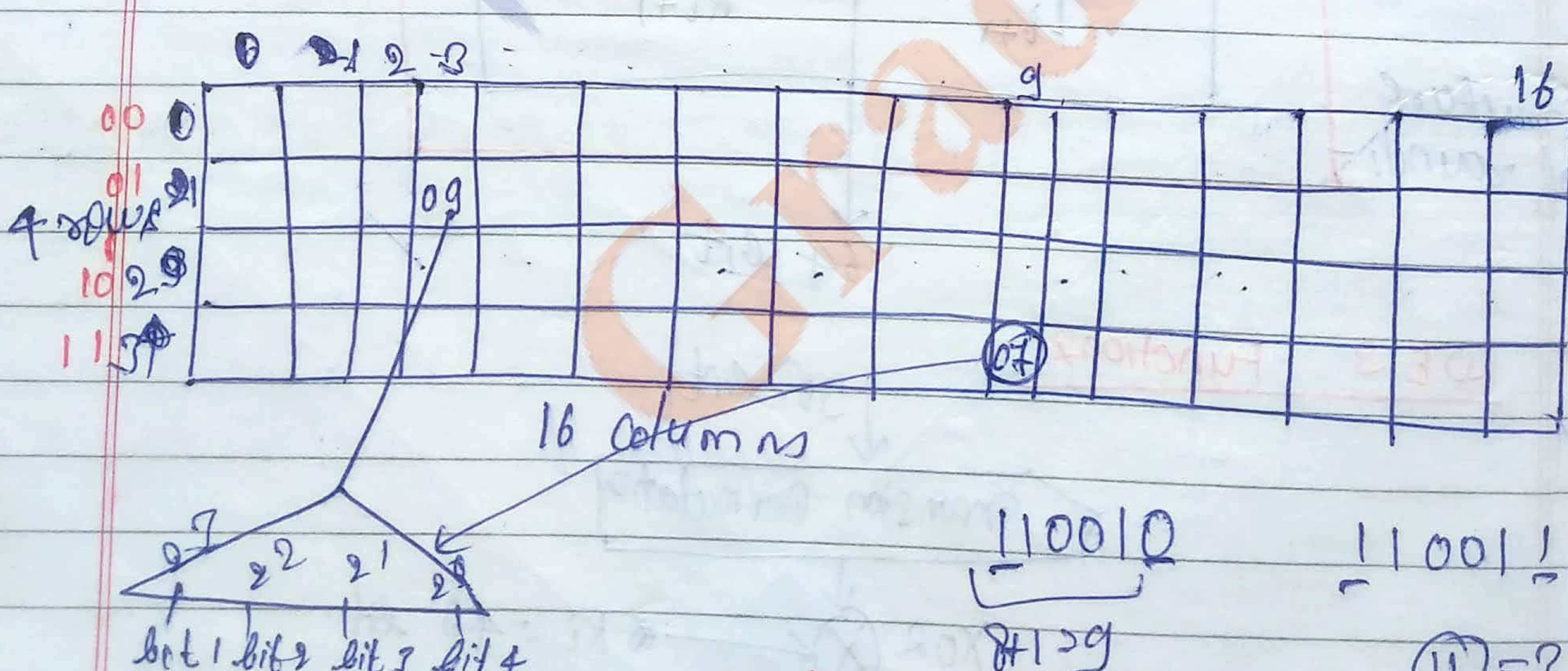












SARAA 1 1 = 07 output

110010

8+1=9

(10) → row no.

110011

(11) = 3 row no

Date : / /
Page No :

Key = 64-bit

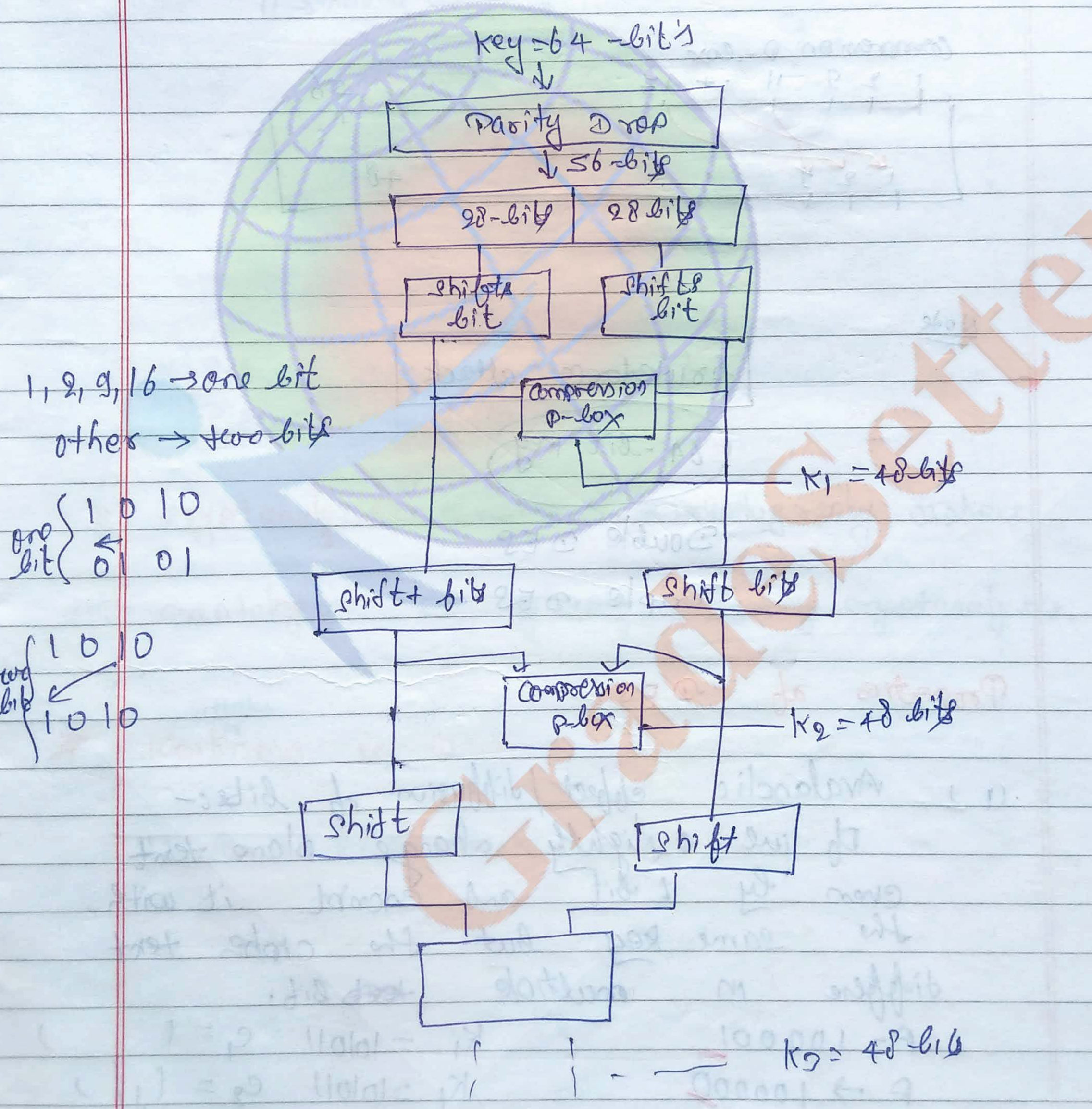
↓

Parity drop

↓ 56 bits.

1 2 3 4 5 6 7 8 9 10 11 -- 16 ------ -- 64

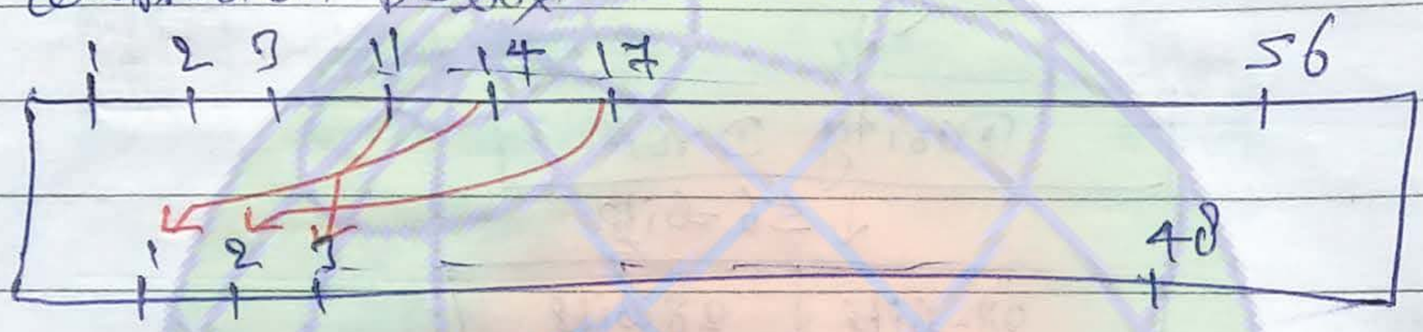
8, 16, ..., 64 → drop



Date : / /
Page No :

14 bit	17 bit	11	24	01	05	28

Compression P-box



Note

brute force attack

64-bit key

Double DES

Triple DES

Properties of DES:-

(1) Avalanche effect / diffusion of bits:-
If we slightly change plane text even by 1 bit and encrypt it with the same key but the cipher text differe in multiple bits.

P - 100001 K_1 = 10101 C_1 = ( )

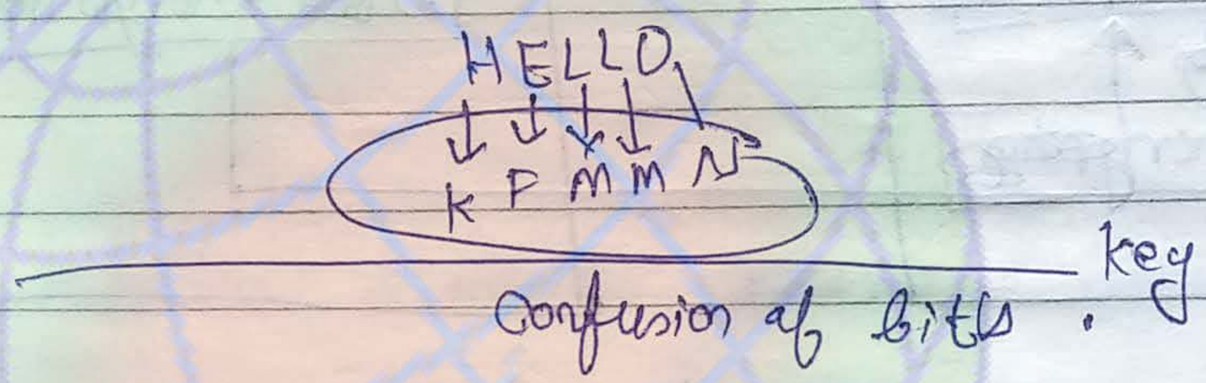
P → 100000 K_1 = 10101 C_2 = ( )

बहुत सारा change हो गया

Date : / /
Page No :

(11) Completeness -
one bit in the ~~cipher~~ cypher text depends upon multiple bits of plain text

P ⇒ 100001 K_1 = 101011 C_1 = 10101
P → 100000 K_2 = 10101 C_2 =



* S-box :- Confusion & Diffusion
P-box :- only diffusion

* Cryptanalysis :- Breaking of cryptography ciphers

criptology - cryptography + ~~Breaking~~ cryptanalysis.

* Weakness in DES - attacks or

(1) Brute force attack -

Date : / /
Page No :

Public IP are provided by DNS, ISP
Public IP's are unique

Private IP's are used in labs
outside, the organization Public IP.

NAT - network address translation

security policy or security mechanism

SP is defined as what type of security measures are allowed or not

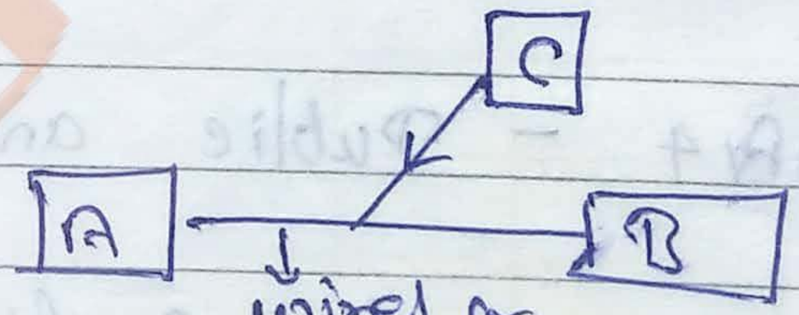
security mechanism - are programs for implementing security policy

threat: Potential voilation of security
It may or may not allowed.

Attack - is defined as those actions which causes the voilation of security.
The person who performs these actions is called attackers.

keylocker software

Network security



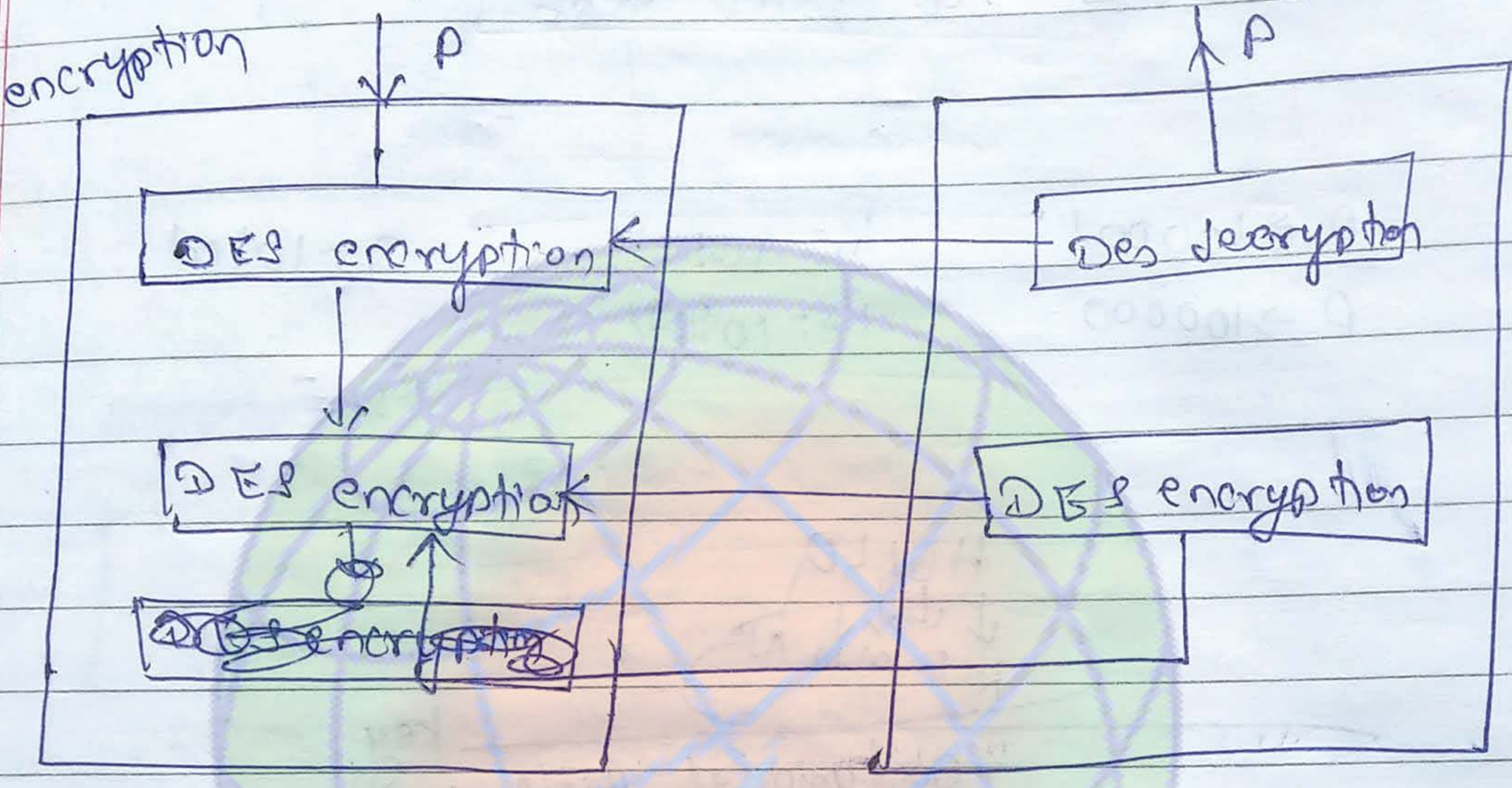
Twisted pair CAT 6
coaxial cable
optical fibre

Basic objective is to share resources.

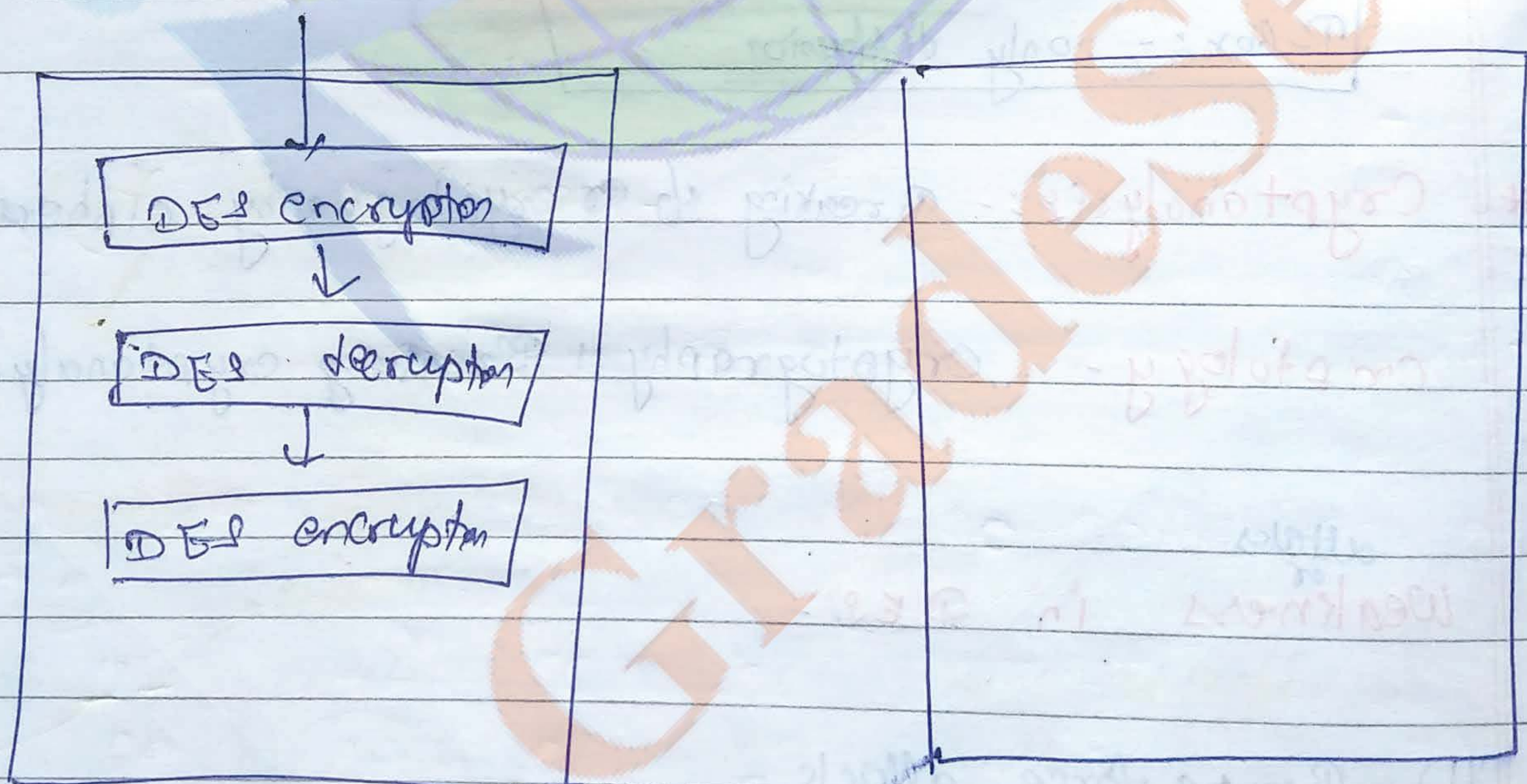
SARAA

Date : / /
Page No :

DES encryption



double DES



Triple DES (3) $= K_1 = K_2$

Triple DES (3) $= K_1 \neq K_2 \neq K_3$

Date : / /
Page No :

AES: Advanced encryption system

↳ NIST
↳ based upon Rijndael algorithm
↳ Vincet Rijmen and Joan Daemen

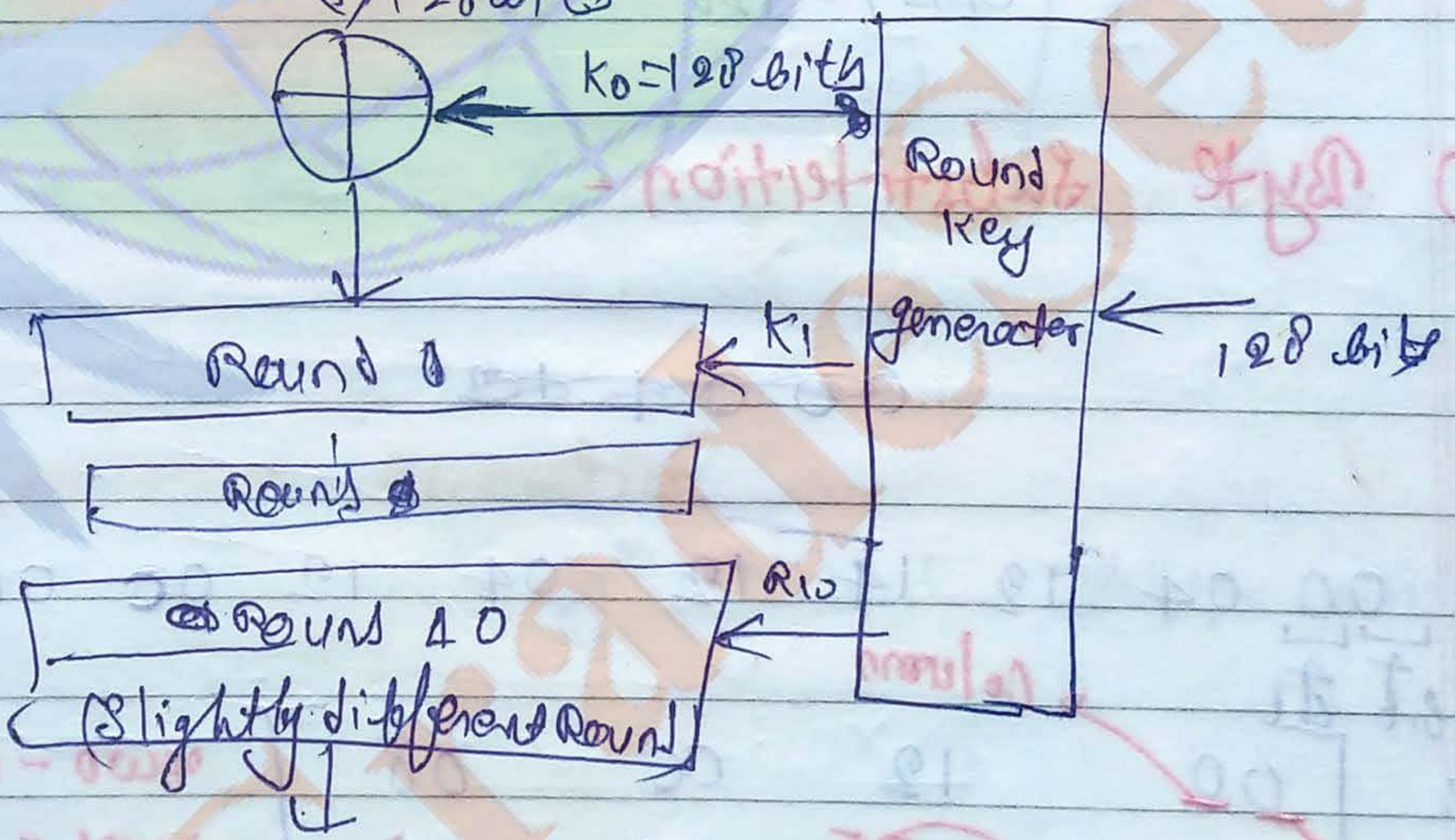
→ Size of datablocks: 128 bits

Number of Rounds	size of key
10	128
12	192
14	256

(rounds will increase)

↳ faster & more secure in respect of DES.

encryption cipher



- take input of 128 bit.

Date : / /
Page No :

operations:

- Byte Substitution
- Byte permutation
- mixing of column
- Add Round key

* IDEA:- (International data encryption standard)
  - Blow Fish
  - RC5
  - CAST-128

① Byte substitution -

~~0 0 0 4 12~~ 32 x 4 = 128 bit

P → 00 04 12 14 12 04 12 0C 00 00 13 11 08 28 19

bit bit

State = | 00 12 0C 08 |
| 04 04 F2 00 23 |
| 12 12 13 19 |
| 14 00 11 19 |

row - no shift
row 1 -

= | 63 C9 FE 30 |
| F2 F2 63 26 |
| C9 C9 7D D4 |
| FA 63 [illegible] D4 |

Column

Date : / /
Page No :

	0	1	2	3	4	5
0	63					
1						
2						
3						
4						

(2) Byte Permutation -

row 0 — no shift
row 1 - shift left by 1 byte
row 2 - shift left by 2 byte
row 3 - shift left by 3 byte

$$\begin{bmatrix} 63 & C9 & FE & 30 \\ F2 & 63 & 26 & F2 \\ 7D & D4 & C9 & C9 \\ D4 & FA & 63 & 82 \end{bmatrix}$$

3) mixing of column operation
- we have to multiply constant matrix with every column

$$\text{Constant matrix: } \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} \times \begin{bmatrix} 63 \\ F2 \\ 7D \\ D4 \end{bmatrix}$$

⇓
or

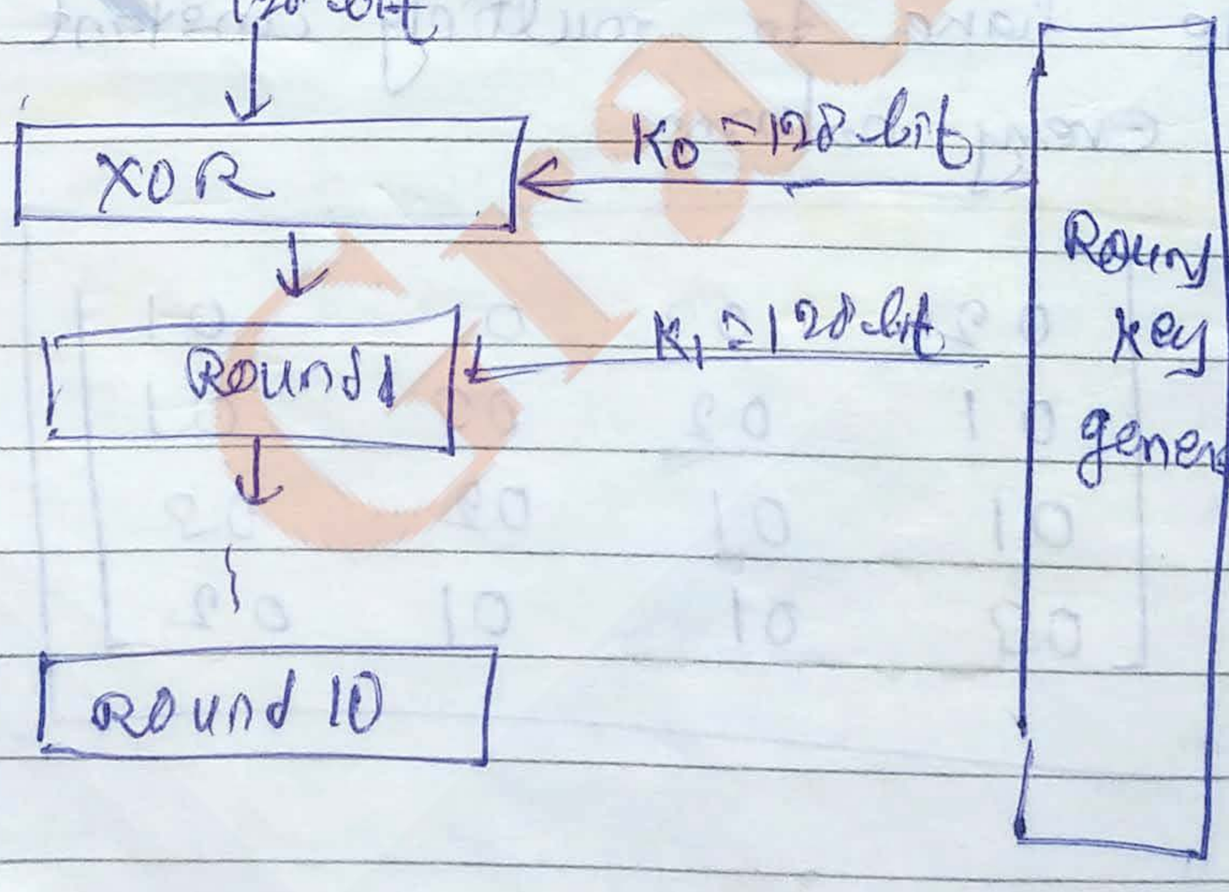
$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} \times \begin{bmatrix} 87 & x \\ F2 & y \\ 7D & z \\ 04 & v \end{bmatrix}$$

$$\begin{bmatrix} ax + by + cz + dv \\ ex + fy + gz + hv \\ ix + jy + kz + lv \\ mx + my + oz + pv \end{bmatrix}$$

$$\begin{bmatrix} 02 \times 87 + 03 \times F2 + 01 \times eg + 01 \times 82 \\ 01 \times 87 + 02 \times F2 \\ \\ \\ \end{bmatrix}$$

Add round key:-

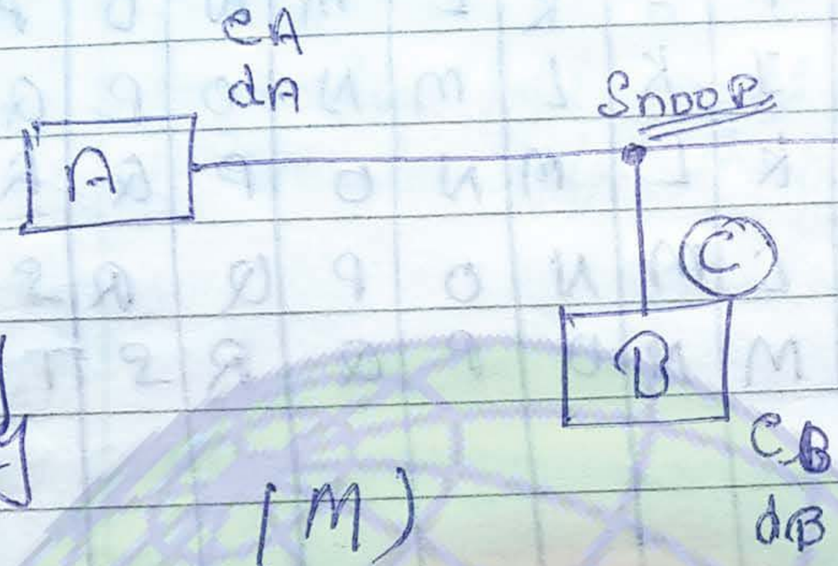
- simple addition, we have to perform addition with round key. simple matrix addition ei performe key ei also in form of matrix



In symmetric key

Date : / /
Page No :

* Public key cryptography-



C - Public key
d - Private key

(M)

receivers public key - encryption.
receivers Private key - decryption.

$C = e_C(M)$

$P(m) = d_C(C)$

★ Vigenere cipher :-

It is developed by Blaise De Vigenere. It is basically polyalphabetic substitution cipher. In this we have to use

P	→	5	7	
K	→	XXZ	XYZX	

This is symmetric key!

Date: / /
Page No:

Vigenere table:-

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

P → ATTACKAT[illegible]

K → LEMONLEM

C → LX - - - - -

Now

Key determines → row

Plain text determines → column

Decryption:

C → LX

K → LEMONLEM ← Scanning this and finding the cipher text and corresponding to it find the plain text.

P → A

Date : / /
Page No :

e!-

R	S	T	U	V	W	X	Y	Z
R	S	T	U	V	W	X	Y	Z
S	T	U	V	W	X	Y	Z	A
T	U	V	W	X	Y	Z	A	B
U	V	W	X	Y	Z	A	B	C
V	W	X	Y	Z	A	B	C	D

← circular left shift of 0 column.
← circular left shift of 1 column
← circular left shift of 2 columns

ê and finding
cipher text
responding
ns the
ain text.

Date : / /
Page No :

Stream & Block cipher -

Stream cipher
↓
operation performed on individual bits or alphabet

eg. vigenere, XOR cipher

- XOR cipher
  P → 1101
  K → 1001
  C → 0100

Block cipher
↓
encryption is performed on some block

eg. DES, AES
↓ ↓
Block size: 64 bit, Block size: 128 bit

- vernan cipher -
  Given by Gilbern vernam 1918

Plain text ⊕ → XOR operation is performed with Random or Pseudo random bits (key) of same length. for the generation of cipher text

One time Pad

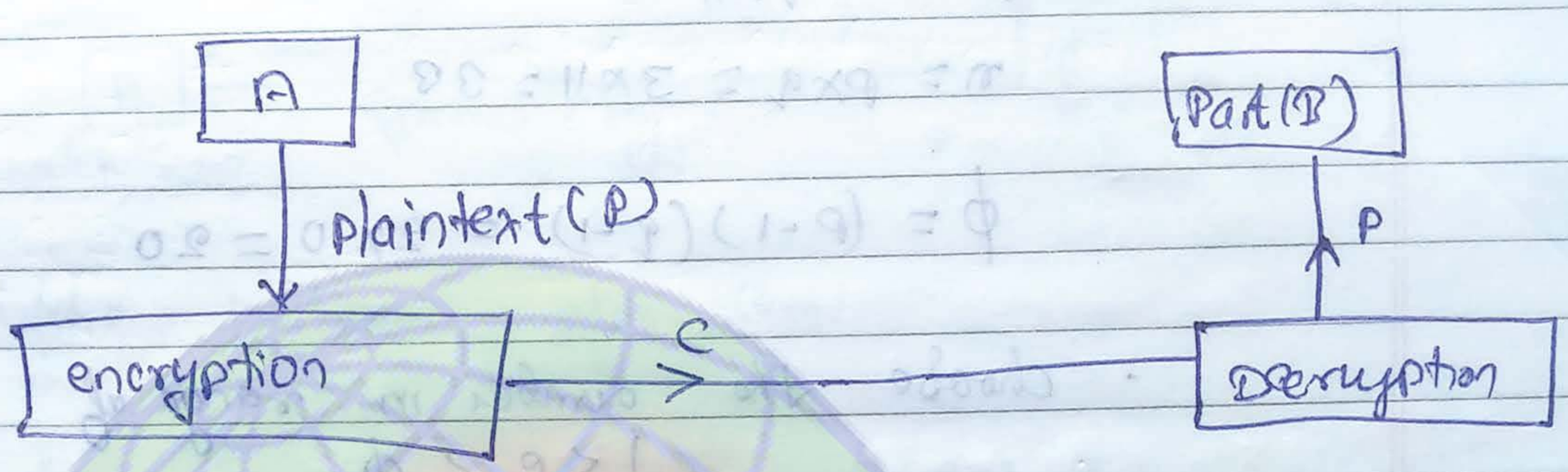
SARAA

Asymmetric key Cipher

Date : / /
Page No :

RSA ⇒

Inventer :- Rivest, Shamir, Alleman



$C = P^e \bmod n$ — एनक्रिप्शन के लिए

$P = C^d \bmod n$ — डिक्रिप्शन के लिए

Step's of algorithm for key generation (B)

(i) chose two large prime number P and Q

(ii) calculate

$n = P * q$

(iii) then calculate

$$\phi = (P-1)(q-1)$$

(iv) Now receiver choose a random integer (e) that is the public key in the range of

$$1 < e < \phi(n)$$

(v) then calculate (d), such that

$$(d \times e) \bmod \phi = 1$$

(vi) Now announce Public key (e, n) while keeping secrete private key (d, ϕ)

Date : / /
Page No :

Pg 71,

Network security - is defined as provisions & policies adopted by a network administrator to prevent and moniter unauthorized access, misuse, modification or denial of computer, network and network accessible resources N.S. involves the authorization of access to data in a network that is controlled by network administrator.

Unauthorised access -
misuse
modification - Illegaly intercept the data & modify it.
denial of service

* Security is provided by -
(i) Authentication - username, password
(ii) Antivirus - protect from viruses, worms, trozan house.

Card + Pin — two factor authentication
card + Pin + OTP + biometric system — 3-factor authentication

Virus - virtual information resources under
- seas
- does not replicate Independently

worms - Replicate Independently

(iii) Encryption & Decryption cryptography -
(iv) Firewalls

* Encryption - Data is converted into some form
* cryptography - art of secret writing

Date :
Page No :

eg) example of RSA

$p = 3 \qquad q = 11$

$n = p \times q = 3 \times 11 = 33$

$\phi = (p-1)(q-1) = 2 \times 10 = 20$

- choose the number in range of

$1 < e < \phi$

let

$e = 7$

compute d

$(d \times e) \bmod \phi = 1$

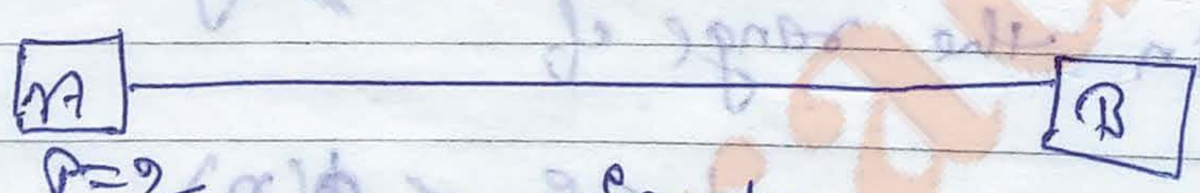
$(d \times 7) \bmod 20$

if $d = 3$

$(3 \times 7) \bmod 20 = 1$

Public key $(e, n) = (7, 33)$

Private key $(3, 20)$



$P = 2 \qquad C = P^e \bmod n$

$= 2^7 \bmod 33 = 29$

$P = C^d \bmod n$

$= 29^3 \bmod 33 = 2$

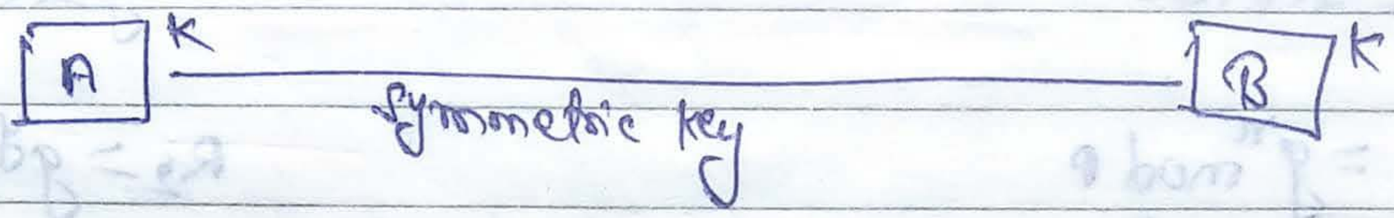
* RSA algo only works when $p < n$

(size of plain text should be less than n)

Date : / /
Page No :

so,
Basically it is uses for small messages.

Note:



★ Diffie hellmon algorithm:

(1) chose two numbers p and g.
p is large Prime number
g is random number
Both p and g are public

(2) A choose a large random number x.
and calculate
$R_1 = g^x \bmod p$

(3) B choose a large random number y and
Calculate R_2
$R_2 = g^y \bmod p$

(4) A sends $R_1 \rightarrow$ B while x = secret
B sends $R_2 \rightarrow$ A while y = secret

(5) A calculate
$K = (R_2)^x \bmod p$
B calculate
$K = (R_1)^y \bmod p$
$\rightarrow (g^y \bmod p)^x \bmod p$
$\rightarrow g^{xy} \bmod p$ ✓✓

SARAA

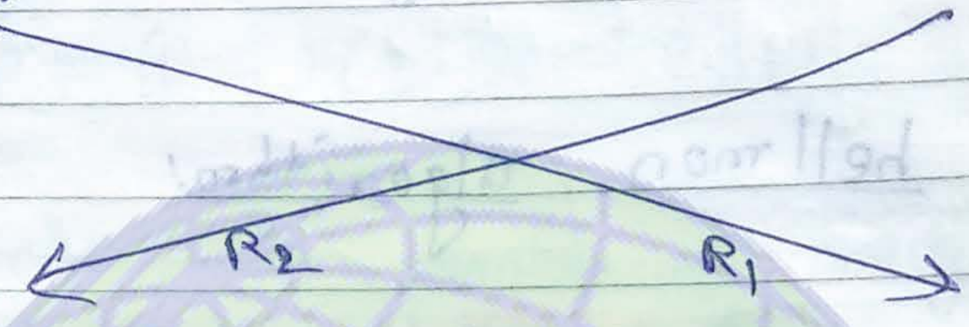
Date : / /
Page No :

x = secrete

$R_1 = g^x \bmod p$

y = secret

$R_2 = g^y \bmod p$



$K = g^x (g^y \bmod p) \bmod p$
$= g^{xy} \bmod p$

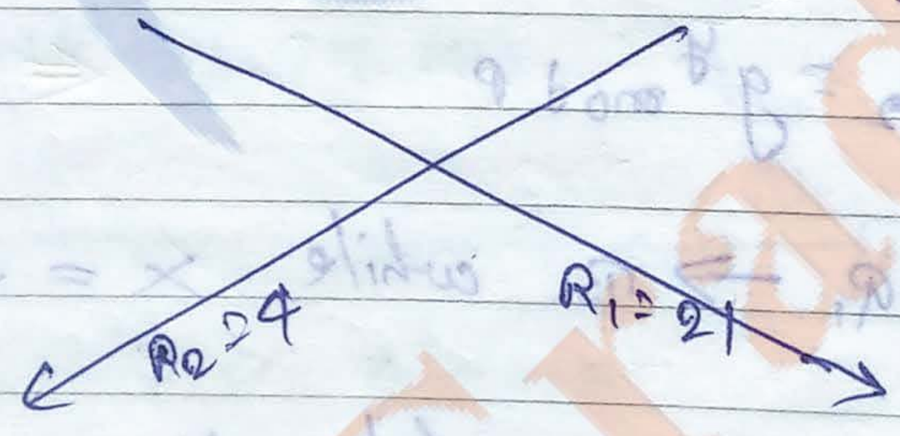
$g^y (g^x \bmod p) \bmod p$
$= g^{xy} \bmod p$

eg. $g = 7$, $p = 23$
(g: any random number; p: prime number)

A → $R_1 = g^x \bmod p$ B $y = 6$

$x = 3$ $= 7^3 \bmod 23 = 21$

$R_2 = g^y \bmod p$
$= 7^6 \bmod 23$
$= 4$



User A
calculate K
$(R_2)^x \bmod p$
$= (4)^3 \bmod 23 = 18$

User B
calculate K
$(R_1)^y \bmod 23$
$(21)^6 \bmod 23 = 18$

☆ Markel Hellman Knapsack cryptosystem:-

Date : / /
Page No :

Type of attack
(i) Active
(ii) Passive
(iii) Snooping
(or) Spoofing - ip spoofing
(iv) Denial of Service attack
(v) Phishing
(vi) Sql injection attacks
(vii) Dns attacks

* Virus, Worms & Trojanhorse

Virus
Worms
Trojanhorse } malicious Program

Antivirus software

Virus - need some file for their replication
- (mostly with the .exe file they can replicate)
- they need execution file
⇒ vital information resource consuming

Worms - they replicate independently
not need file
basically standalone program

Trojanhorse - hidden code
- system dec
- hidden malicious program ~~that comes with the software etc.~~

battel of "Troy"
Trojan
Greek

hidden is some software Packages.

Date : / /
Page No :

Virus - In computer virus attach themselfs to files of program infecting each computer, It comes across as ills spares they replicate with the help of executable files, which means a person has to actually run the program per the virus per becomes active The virus slow down the system and sometimes damages the files of our system

Worms - Worms are similar to virus but they have the capability to travel without any human action, they self replicate, they dont have to attach, themselfs to a program instead they use computer networks to send malicious software to other computer.
They are extrimly dangerous because they can replicate themselfs sucess. And to major damages even to server
eg: blaster work, morris worms

Trogenhorse - The trogenhorse Programs, hide all sort of milicious goodies just like when the greeks came a huge wooden horse to the trogens after the horse goes within the verge of their city greek soldiers came out of the hollow horse and they were able to capture tog at first glance the trogens seen to be legitmater or authentic software they are successful in duping the users once installed, they can make changes to our computer

SARAA

Test:- DES, AES, RSA, ciphers - substitution, trans, mono, poly, cryptanalysis of DES, AES; avalanche effect, completeness, strength, weakness in DES, double DES, triple DES → symmetric

and deleting our files. They do not replicate themself.

eg netbus, Blandes thread
↓
Is a sophistigated attack that bundles some of the worst affect of virus, worms, trojans and milicious code into one single threat.

The blanded thread can use server and internet vernability to miciack then transmit and also spread and attack.

Rabit or Bacterian - These are those milicious programs that consumes all resources of system, network etc.

logic Bomb - It is a attack, that occurs on specified date.

SARAA

symmetric / classical
Asymmetric / public

Date : / /
Page No :

symmetric & Asymme. key : RSA, substitution ciphers — monoalphabet, polyalph caeser ciphe, vernam cipher, visnear cipher with the help of 26/26 table,
Threats, components of network security
↳ confidential
↳ integerity

★ merkel-hellman knapsack
→ 1975
↳ Ralphe Merkel & merkel hellman

n-bit message — $W = \{w_1, w_2 \text{ ——— } w_n\}$
of non-zero natural numbers.

– pick a random inter q → such that $q > \sum_{i=1}^{n} w_i$

Now select a random integer 'r' such that gcd of r and q is 1. then, calculate the sequence

$$\beta = (\beta_1, \beta_2 \text{ —— } \beta_n)$$

$$\beta_i = r w_i \bmod q$$

Public key $= \beta$
Private key (w, q, r)
message $d = (d_1, d_2 \text{ - - - } d_n)$

$$C = \sum_{i=1}^{n} d_i \beta_i$$

$$= d_1\beta_1 + d_2\beta_2 + \text{——} + d_n\beta_n$$

Date :
Page No :

$\omega = \{\omega_1, \omega_2 \ldots \omega_n\}$

Decryption -

$S = z^{-1} \bmod q$

$e^1 = es$

$e^1 = 175 - 60$

$= 115$

$= 0$

{25, 50, 60, 175, 350, 500}

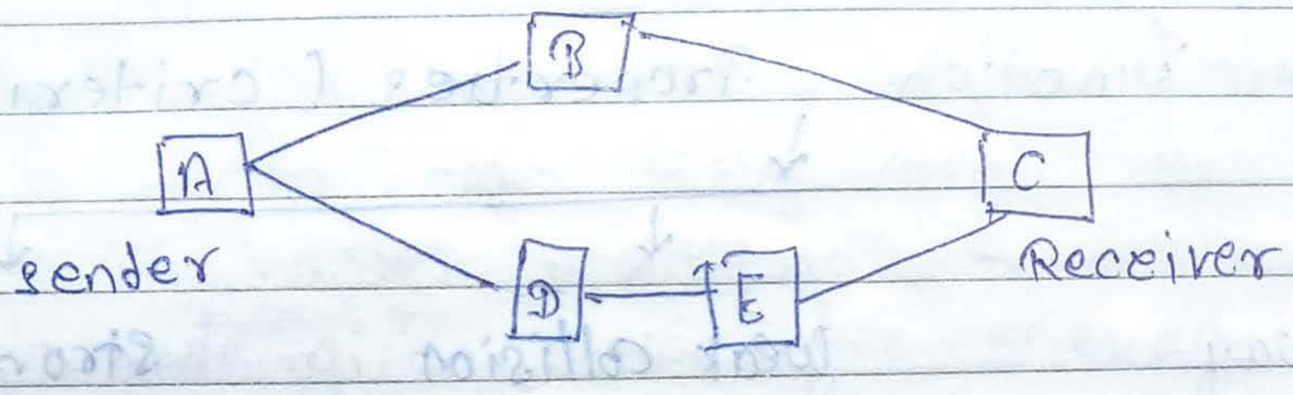
1000

(1) Phishing - Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as username, Password and credit card details by masquerading as a trustworthy entity in an electronic communication.

SARAA

Message Integrity :

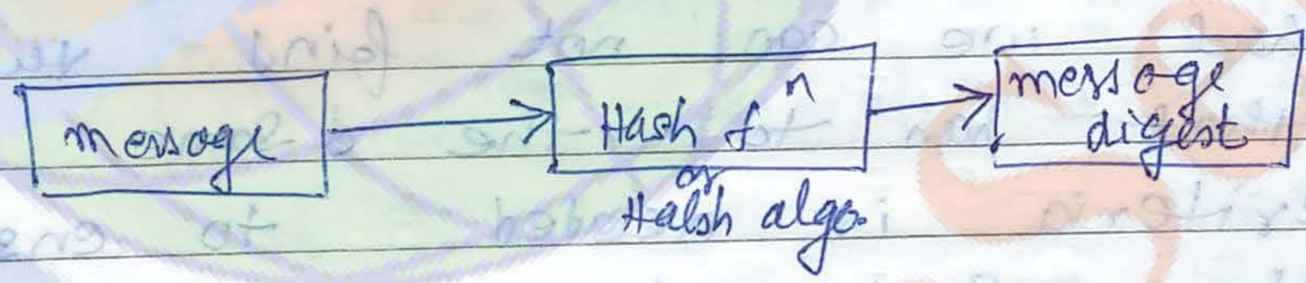
Date : / /
Page No :



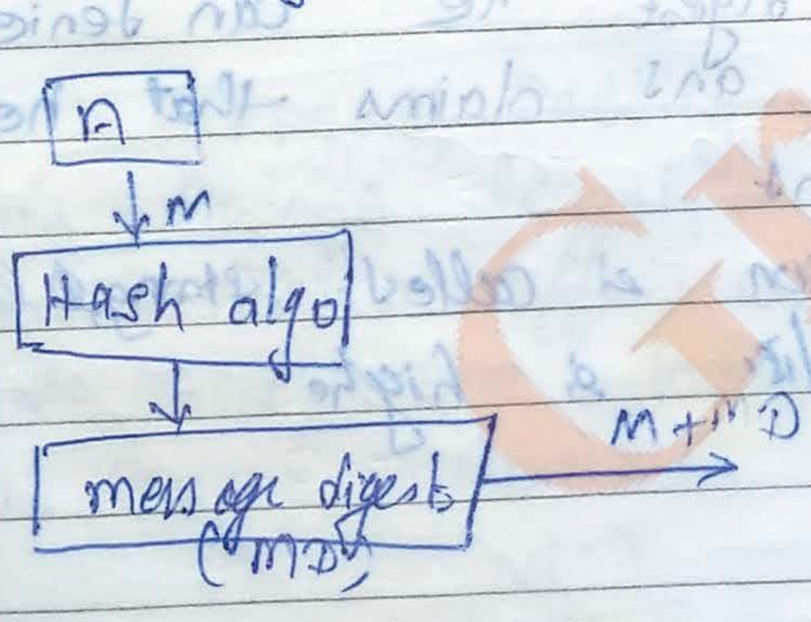
A $\xrightarrow{M}$ C

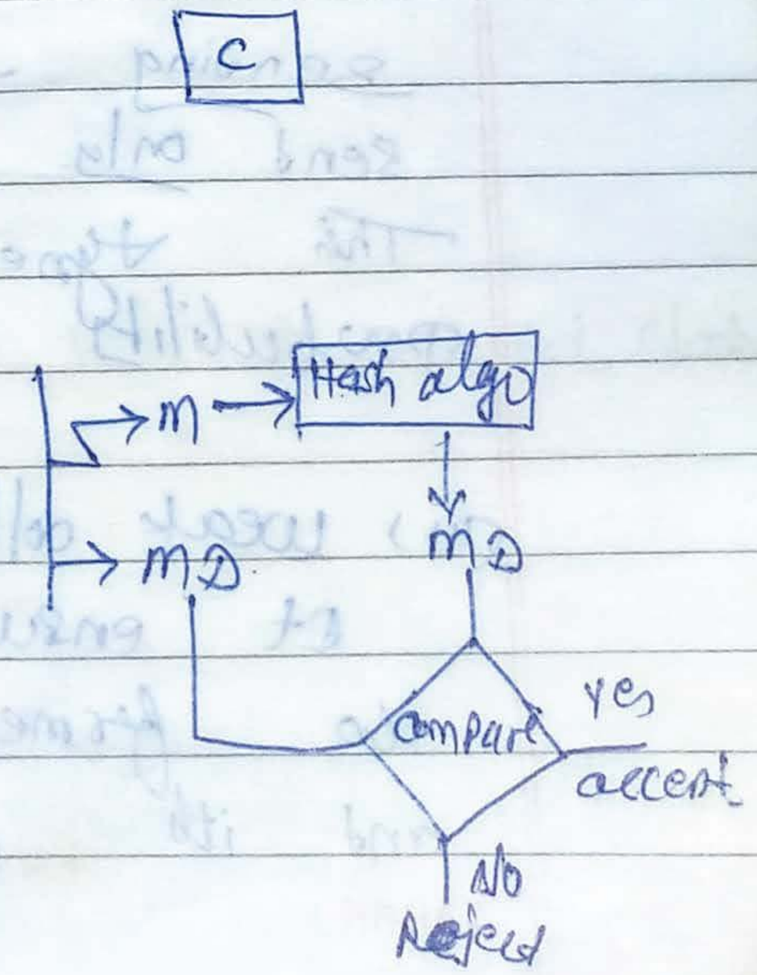
(1) MD4 - message digest 4
(ii) MD5 -
(iii) SHA-1
(iv) SHA-2

* message Digest -
  1. Also known as finger Print of message



How message digest helps of protecting the message :-





Date : / /
Page No :

Network security services (components)

These are divided into 2 classes -

message
- Privacy or confidential or secrecy (only authorized users are known to message)
- message Integrity
- message authentication
- non recidiation

Entity - authentication
- something known
- something possess
- something Inherent

Date : / /
Page No :

transaction data integrity

Hash function Properties (criteria)

One way

$m \rightarrow MD$

$m \not\leftarrow MD$

weak collision registance

Strong collision registance

$m_1 \rightarrow MD_1$

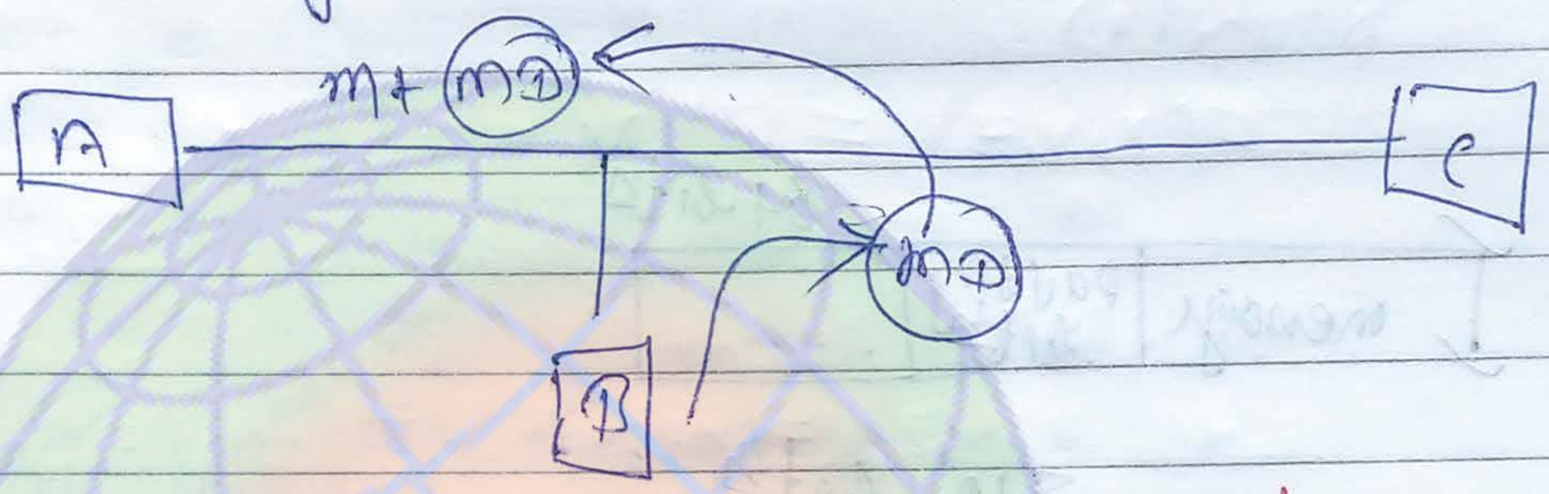
$M_2 \rightarrow MD_2$

(i) One way :-
Hash function must have one feature, a message digest is created by one way hashing fun^n. we must not be able to re-create the message from the digest. No one can make a document from a finger Print

(ii) Strong collision -
This Properties states and ensures that we can not find two message, that has to the same digest. this criteria is needed to ensure that the sender of the message can not cause Problem by forging the message. If the Senter can create two messages, that has two the same digest he can denie, sending the first and claims that, he can send only the recent
The type of collision is called strong, because probability of collision is highe.

(iii) weak collision -
It ensures that message can not easily be formed if sender's create a message and its digest and sends both to the

receiver, this criteria ensures that malicious user's can not easily create another message, ~~that~~ hasses exactly to the same digest in other words given specific message and its digest. It is impossible to create another message, with the same digest. This is known as weak alg.



→ to maintain message integrity

1.) ☆ Message Digest 4 (MD4)
└ published in RFC, 1320.
└ Ron Rives, sized MD 128 bits

Comes in = 1990
Break in = 1992

~~then,~~

Comes

MD5

(i) Append padding bits
(ii) Append length
(iii) Initialize buffer.
(iv) Device the input message into 512 bit blocks.
(v) Process blocks

v(i) ——————
——————
——————

64 bits that exists multiple of 512 bits
└ 512x1 : 512 - 64 = 448
512x2 : 1024 - 64 = 960

SARAA

Date: / /
Page No:

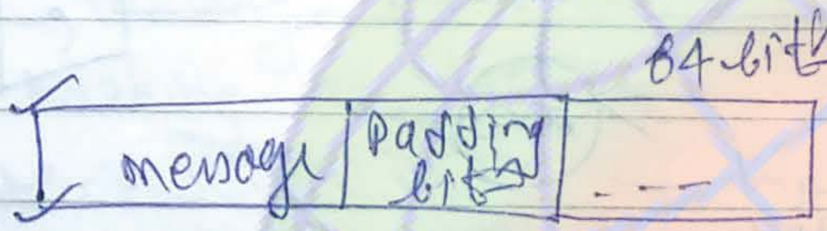
400 ---- 0
padding bits (1-512 bit' as added)

382

64 bits less than exact multiple of 512.

512*2 = ( ) - 64
= 448

Now 448
382
066 ← 66 add 66 padding bits



★ Four buffers

32 bits ← A = 01 23 45 67
32 bits ← B = 89 ab cd ef
32 bits ← C = fe dc ba 98
32 bits ← D = 76 54 32 10
128 bits

(i) Add padding bits! -

960
message | padding bits | length
64 = 1024
470

490
512 x 1 = 512 - 64 = 448
512 x 2 = 1024 - 64 = 960
960
490
470 ← Padding bits are added.

(ii) Append length - -

(iii) Initialise buffers:-

MD4 = 128 bits (output is 128 bits)

$\frac{128}{4} = 4$ bits

128 bit's
- 32 bits = A = 01 23 45 67
- " = B =
- " = C =
- " = D =

(iv) Processing of the message

(iv) Ans) Divide the input into 512 bit blocks

1024

B1 B2

512 512

(v) Processing of the message

(a) Divide the input blocks (512) into 16 sub blocks of 32-bit each

B1

m[0] m[1] ... m[15]

B0 B15

(b) Copy the value of

A = AA
B = BB
C = CC
D = DD

SARAA

Date : 1 1
Page No :

(c) There are three rounds of 16 operations that are performed on A B C D & our message block m[0] ..... m[15].

Now,

for every round there are some function,

Let us suppose

for Round 1, the function is

Round(1)

$F(X,Y,Z) = XY \vee not(X)\, Z$

Round(2)

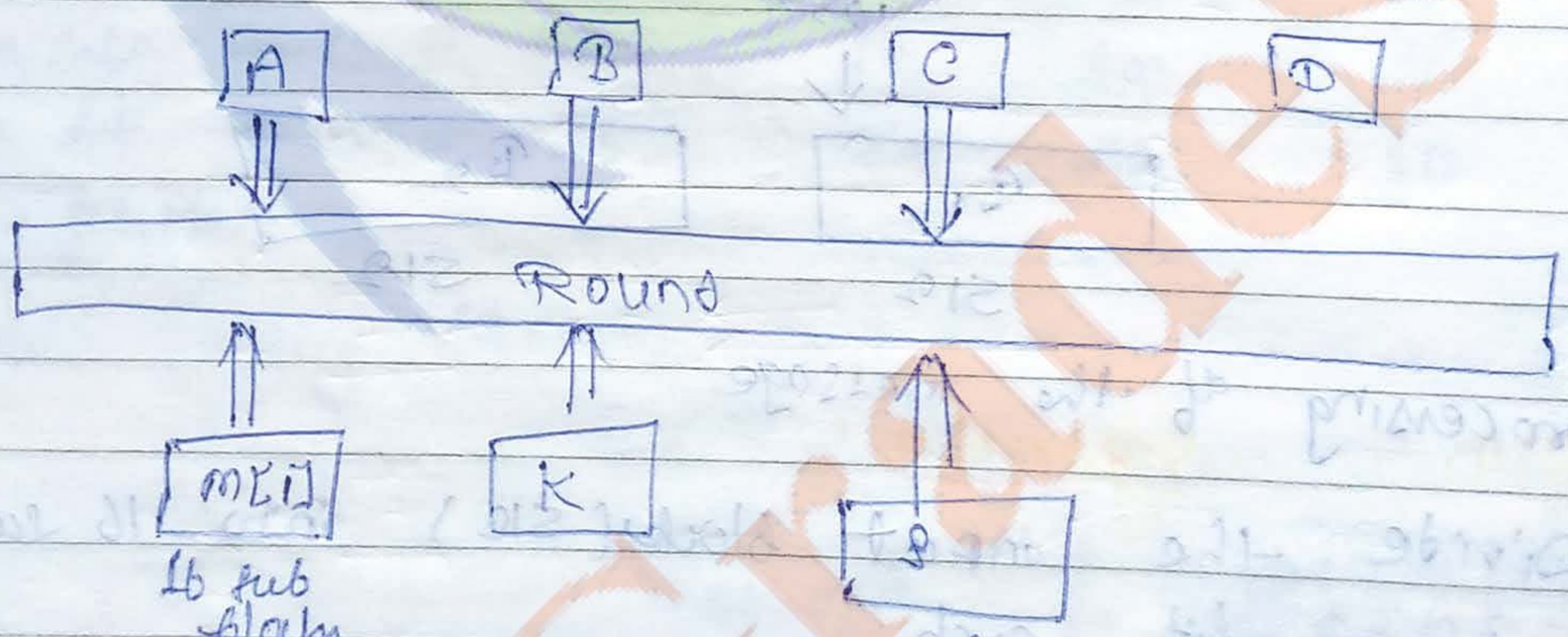
$G(X,Y,Z) = XY \vee XZ \vee YZ$

Round(3)

$H(X,Y,Z) = X \text{ XOR } Y \text{ XOR } Z$

for Round 1 =
for second =

every round takes the values

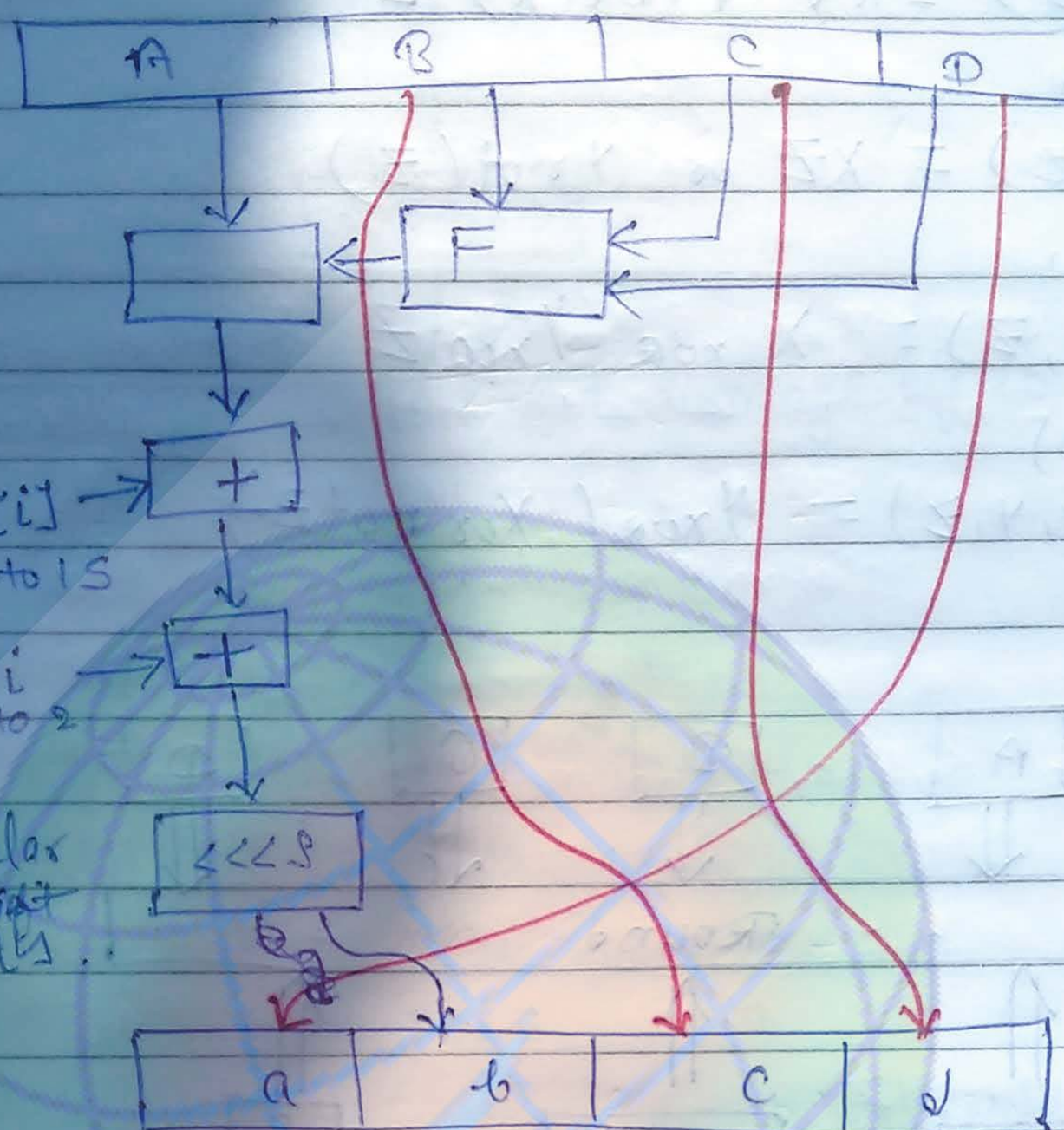


eg. 10101 1
Circula left shift by 1 bits.

value of K for round(1) = 0

for round (II) and round (III) there are some constant values.

Date : / /
Page No :



for 8 bits = 3 bits
for 32 = 5 = 7 bits
11 bits
19 bits.

A = AA + A
B = BB + B
C = CC + C
D = DD + D

(11) MD5 Algorithm :-
↳ published RFC, 1321

{ In MD4, there was a possibility of collision problem. So to solve it MD5 arises

fill 5.2 all are same as above

Ans (v)

(C) There are four rounds of 16 operations each.

Now,

Date : / /
Page No :

Round (1)

$F(x, y, z) = xy$ or $\bar{x}$ $not(x)$ z

Round (2)

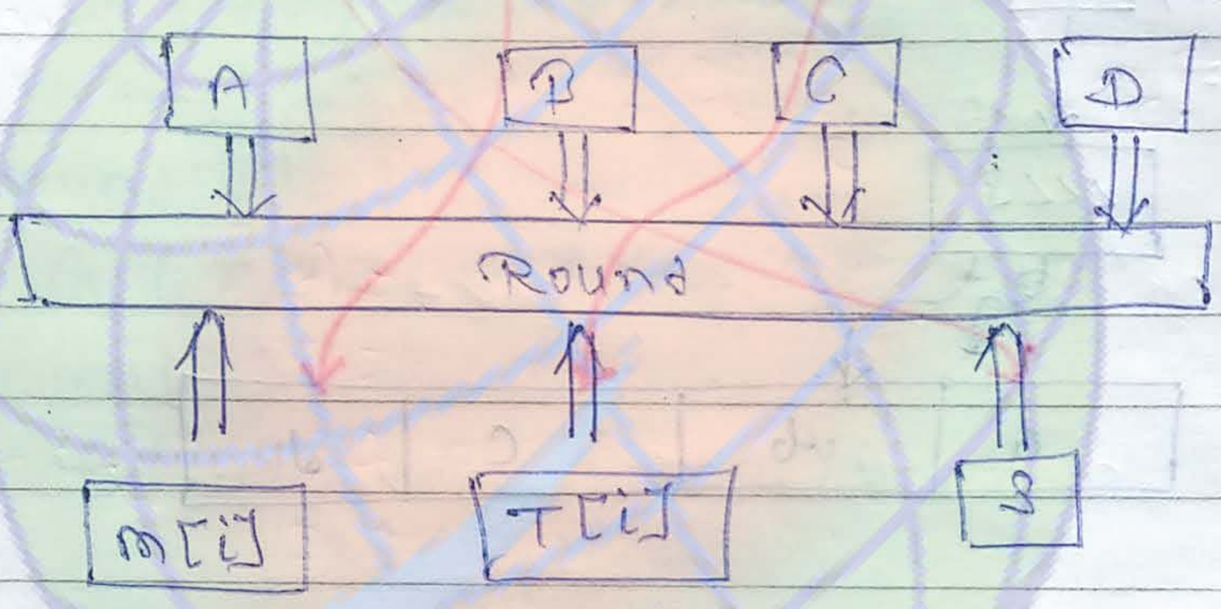
$G(x, y, z) = xz$ or $y\ not(z)$

Round (3)

$H(x, y, z) = x$ xor y xor z

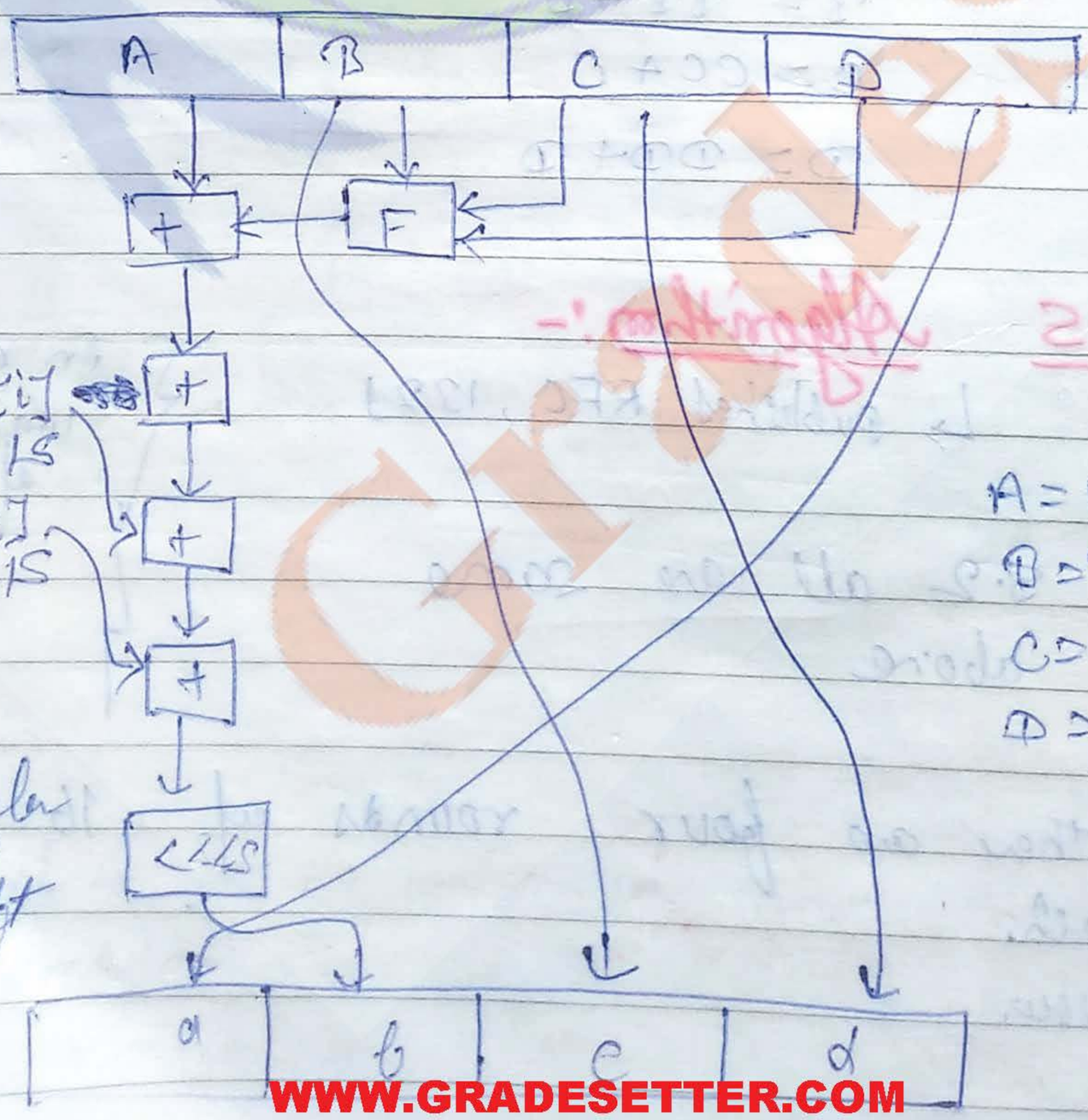
Round (4)

$I(x, y, z) = y$ xor $(x$ or $not\ z)$



i = 0 to 63

circular left shift by s-bits.



A = AA + A

B = BB + B

C = CC + C

D = DD + D

Date : / /
Page No :

Note

message

↓

MD 4 / MD 5

↓

128 bit message digest.

★ SHA (secure hashing)

SHA-0 → 1993
SHA-1 → ~~1993~~ 1995
SHA-2 → 2005
SHA-3 → 2015

syllabus

collision

↓

Hash alg.

↓

MD

(1) SHA-1 — 160 bit message digest (1995)

message

↓

SHA-1

↓

160 bit

step 1: Add Padding bits

message	Padding bits

100 - - - - 1

1000 bits 472 bits.

512 x 1 - 64 = 448
512 x 2 - 64 = 960
512 x 2 - 64 = 1472

Date : / /
Page No :

Step 2nd -

Append length

message	padding	length
← 536 →	← 472 →	← 64 bits →

Now, exact multiple of 512 bits

Step 3rd:

Initialize buffer on ~~chaining~~ chaining variable.

352 = 160 bits

- A =
- B =
- C =
- D =
- E =

Step 4th.

Divide the input message into 512 bit blocks.

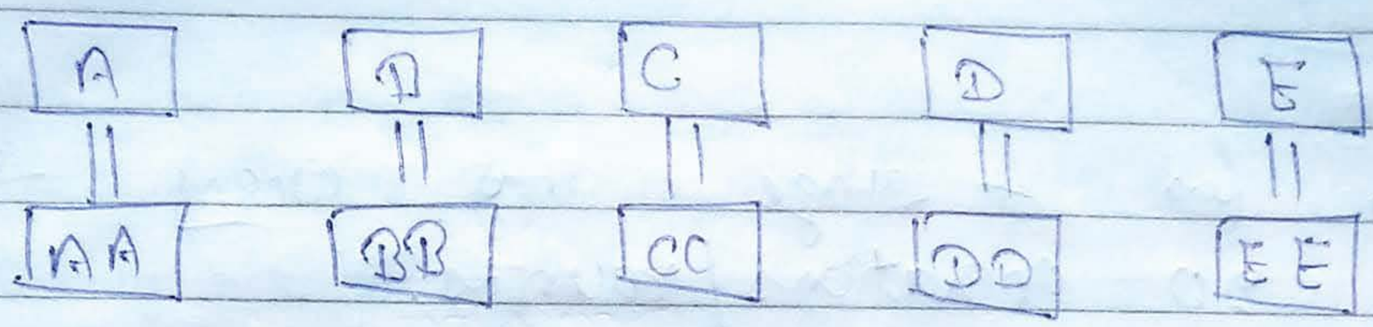
message

Step 5th.

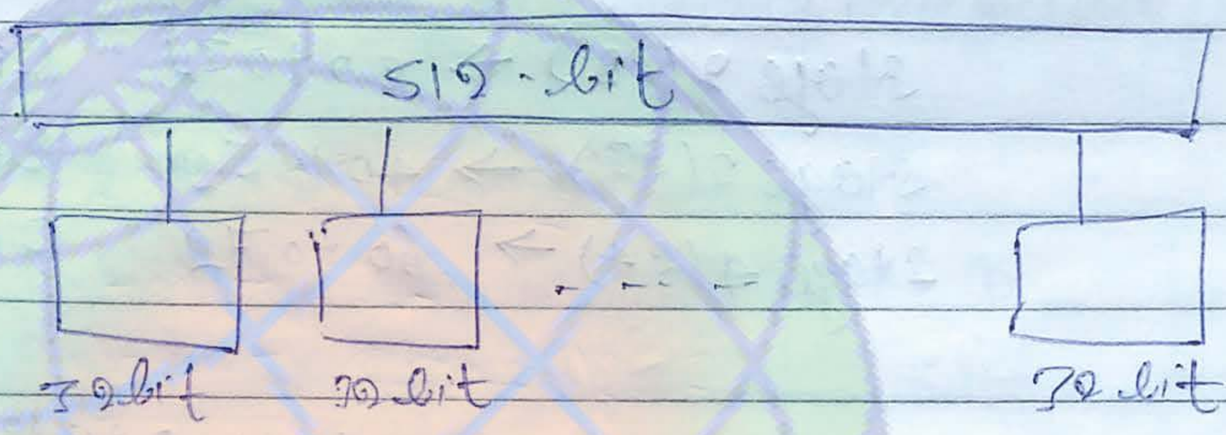
Processing of blocks.

5.1) Copy the values of fine chaining variable.

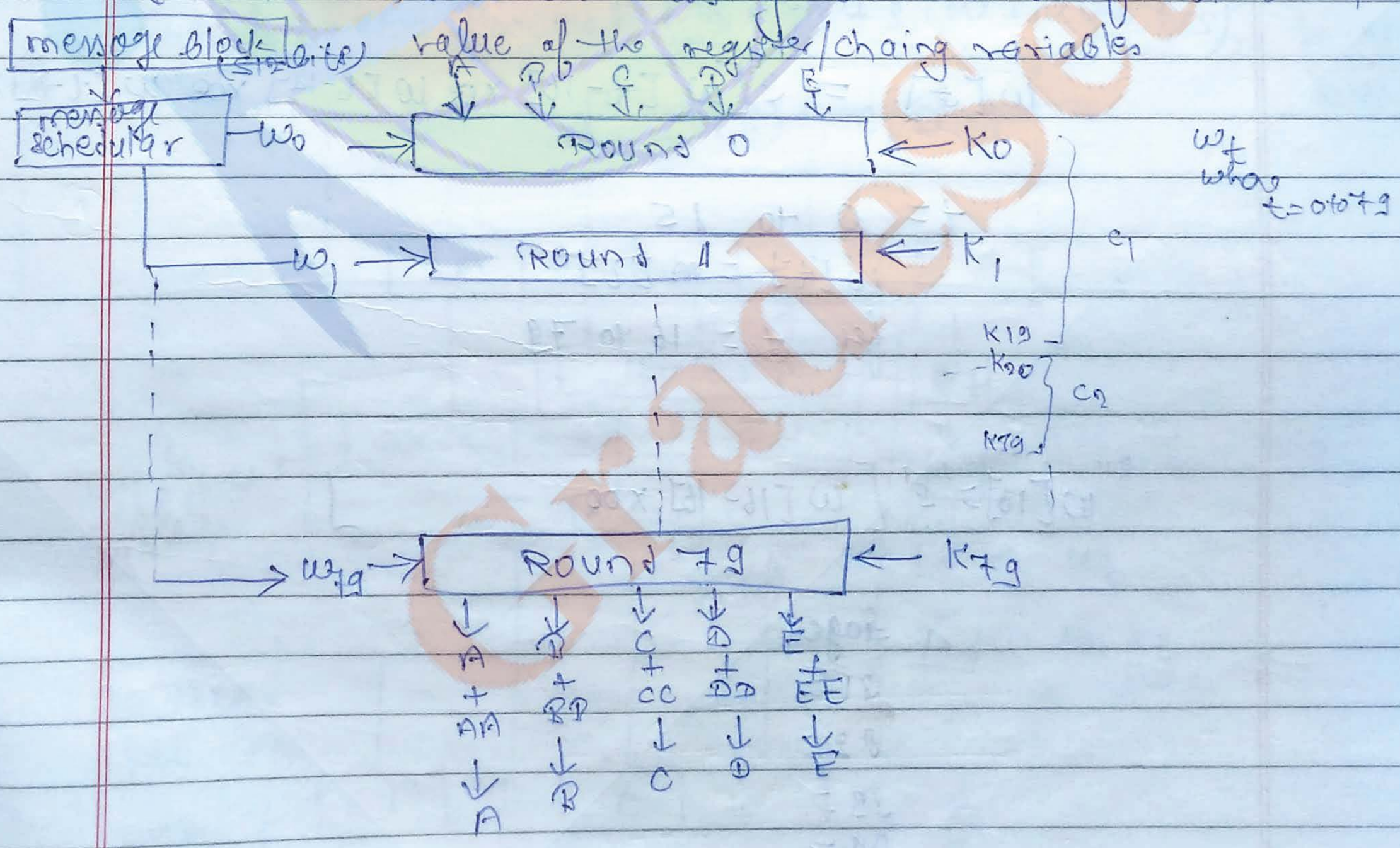
Date : / /
Page No :



5.2) Divide the 512-bit blocks with 16-sub blocks of 32-bit each



In SHA 1, we are using 80 rounds of operation



w_t where $t = 0 \text{ to } 79$

Here is a constant K

SARAA

Network security services (Component's of network security)

- → message - combination of bit's
- → entity - object, Person

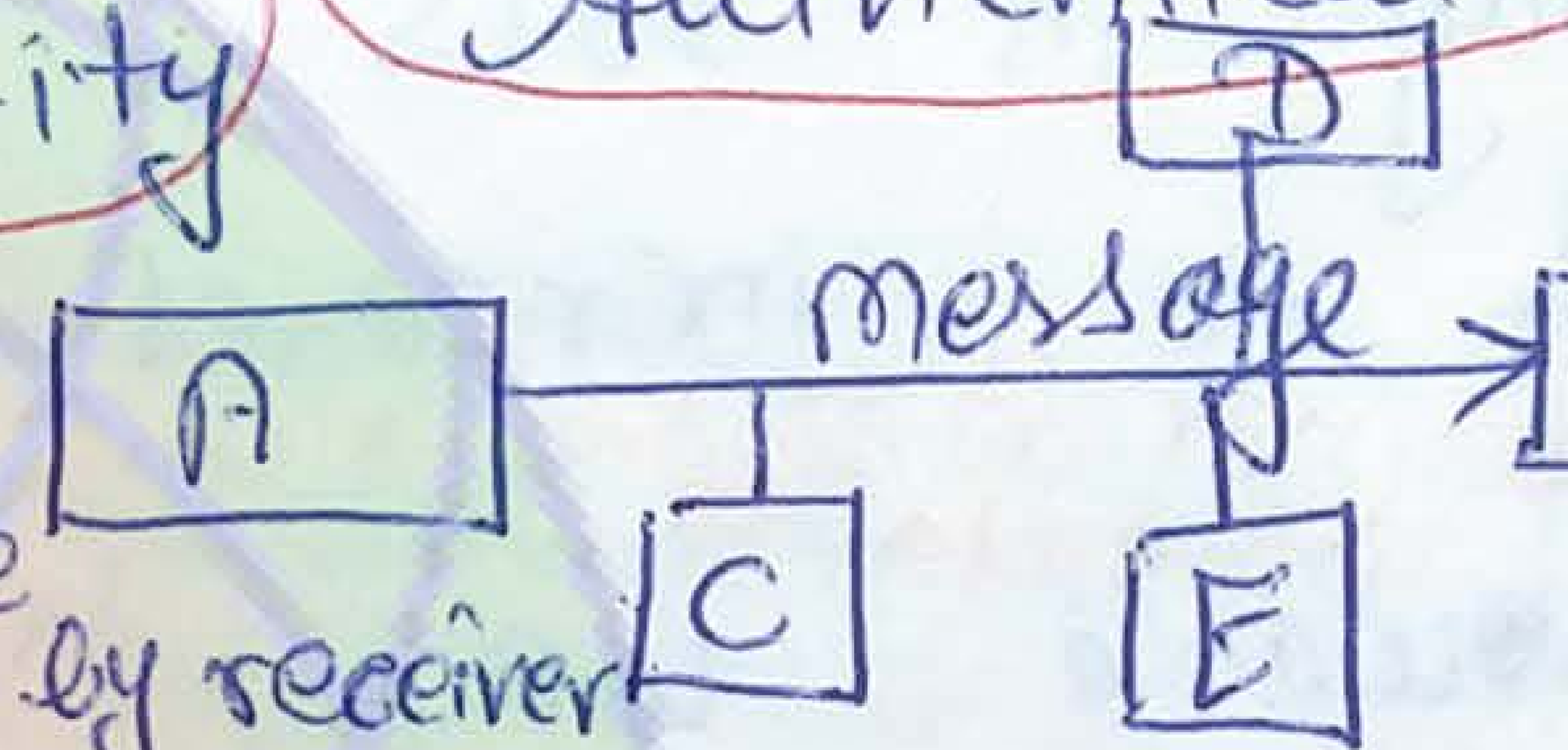
Principle of security or

* message → Privacy or Confidential or secrecy ~~security~~ (keep msg secret) ← Cryptography

message → message Integrity → Same data should be received by receiver (checksum, hash function)

message → message Authentication (msg authentication at receiver side (that it is send by true sender))

message → Nonrepudiation (Receiver must have proof that A sends data) → Digital Signature



* Entity → Authentication

- → Something known, eg Pin no, Password, usernames
- → Something Possessed, eg ATM card
- → Something Inherent, eg. Biometric, Fingerprint

* Challenge response system:-
↳ Basically with the help of some Question and answer we login into the system

* Vulnerabilities:-
L weakness or loop holes that exists in the software. Package.

* Symentic, ~~Dells~~ → Internet security threat report 2016

(i) In 2015 every on an average a new zero day vulnerabilities is found. The total found vulrenabiliti es increased by 125% compare to Previous year

Date : / /
Page No :

So,
there are 4 stage and every stages has 20 operations / rounds.

4 stage — 20 operation

stage 1 (S1) → 0 to 19 CB_1 = --
stage 2 (S2) → 20 to 39 CB_2 = --
stage 3 (S3) → 40 to 59 CB_3 = --
stage 4 (S4) → 60 to 79 CB_4 = --

K_1 → 0 to 19 → C_1
K_2 → 20 to 39 → C2
K_3 → 40 to 59 → C3
K_4 → 60 to 79 → C_4

circular left shift by 1 bit

$w[t] = S'[w[t-16] \text{ XOR } w[t-14] \text{ XOR } w[t-8] \text{ XOR } w[t-3]]$

$t = 0$ to 15
$w[t] = m[t]$
for $t = 16$ to 79

for $w[16] = S'[w[16-16] \text{ XOR } \ldots]$

4 stage
S1 =
S2 =
S3 =
S4 =

Date : / /
Page No :

for stage 1 :-

(B And C) OR (NOT (B) AND d)

for stage 2 :-

B XOR C XOR D

for stage 3 :-

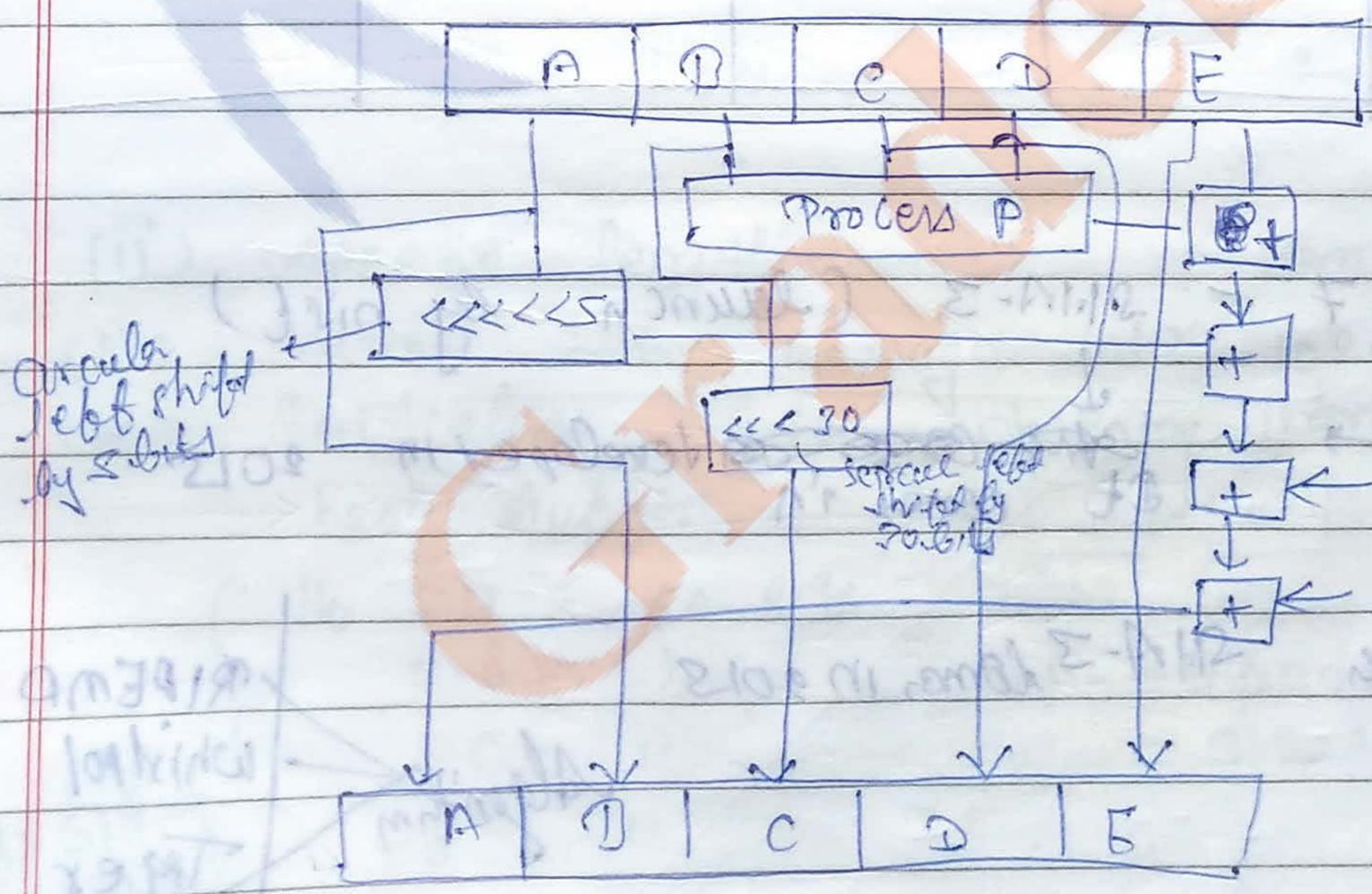
(B AND C) OR (B AND D) OR (C AND D)

for stage 4 :

B XOR C XOR D

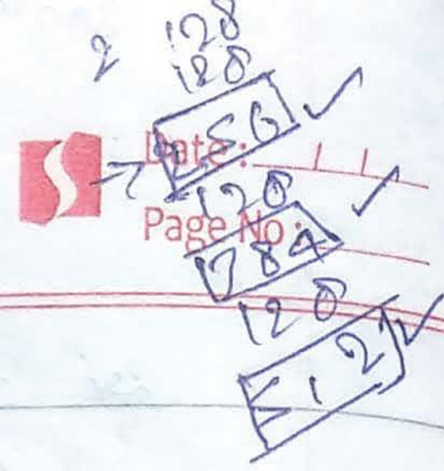
Then, final Output is calculated as

Output (a) = (E + Process P (B, C, D) + S^5(A) + W_t + t_{15}), A, S^{30}(B), C, D)



(This is one round round operation)

SARAA



* SHA-2

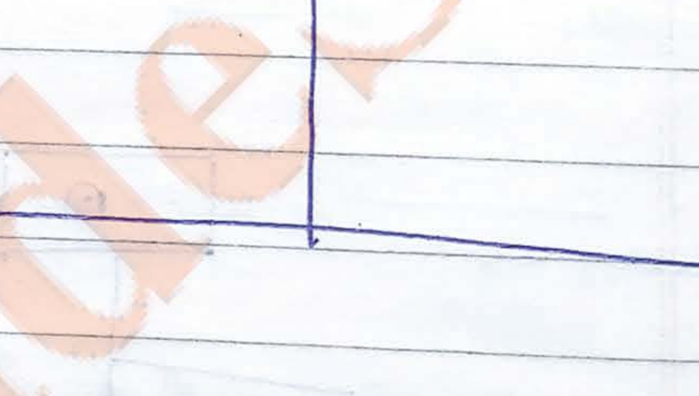
→ comes in 2002 → SHA-256
SHA-384
SHA-512

→ In 2005, NSA revised comes into the market → SHA-224

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
message digest	160	224	256	384	512
Block size	512	512	512	1024	1024
Word size	32	32	32	64	64
No. of steps	80	64	64	80	80

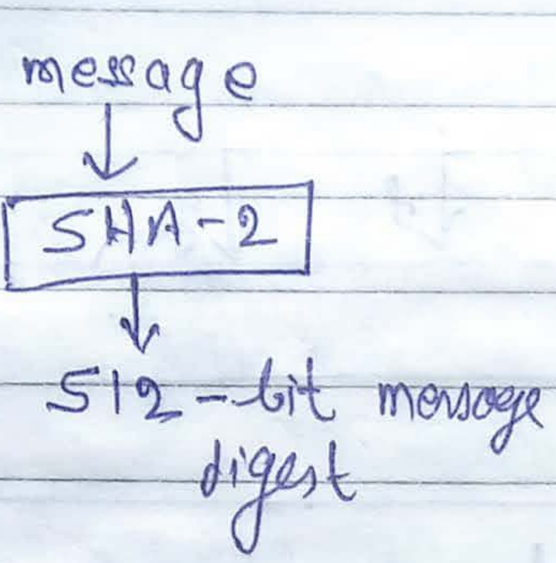
→ 2007 - SHA-3 (launch by nist)
↓
It comes in developed in 2015

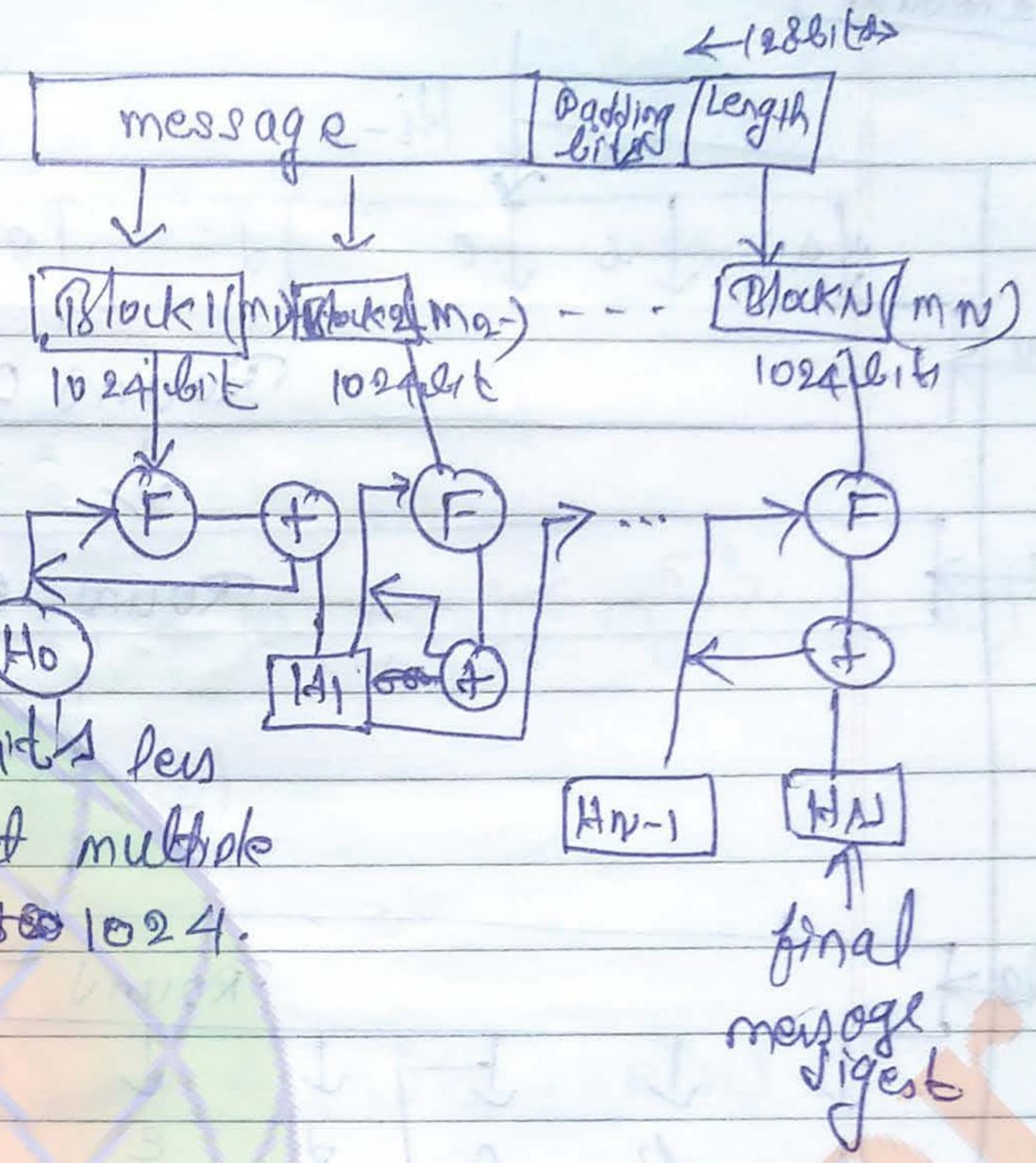
⇒ Latest is SHA-3 comes in 2015



Date: / /
Page No:

SHA-512 :-





(1) Add padding bits

128 bits less than exact multiple of 1024.

100 - - - -

880 ← message

1024x1 = 1024-128 = 896

100 - - - -

(ii) Append length -

(iii) Divide the message into 1024 bits blocks.

(iv) Initialize the chaining variable or hash buffer

64x8 = 512

H_0 = a = 64 bits
= b = "
= c = "
= d = "
= e = "
= f = "
= g = "
= h = "

H_0 = a b c d e f g h
= 512 bits

How function F works:-

m_i = 1024 bits

message scheduler

Hi-1

a b c d e f g h

w_0 → Round 0 ← k_0

w_1 → Round 01 ← k_1

w_{79} → Round 79 ← k_{79}

a b c d e f g h

+

$i = 0$ to 15

$w_i = (m_{s_1} - - - - m_{s_{16}})$

16 to 79

512

* How message scheduler works:-

1024

s_0 s_1 - - - - s_{16}

64bit 64bit

w_t =

$t = 0$ to 15

$w[t] = s[t]$

Date : / /
Page No :

$$W_0 = S_0$$

$$W_{15} = S_{15}$$

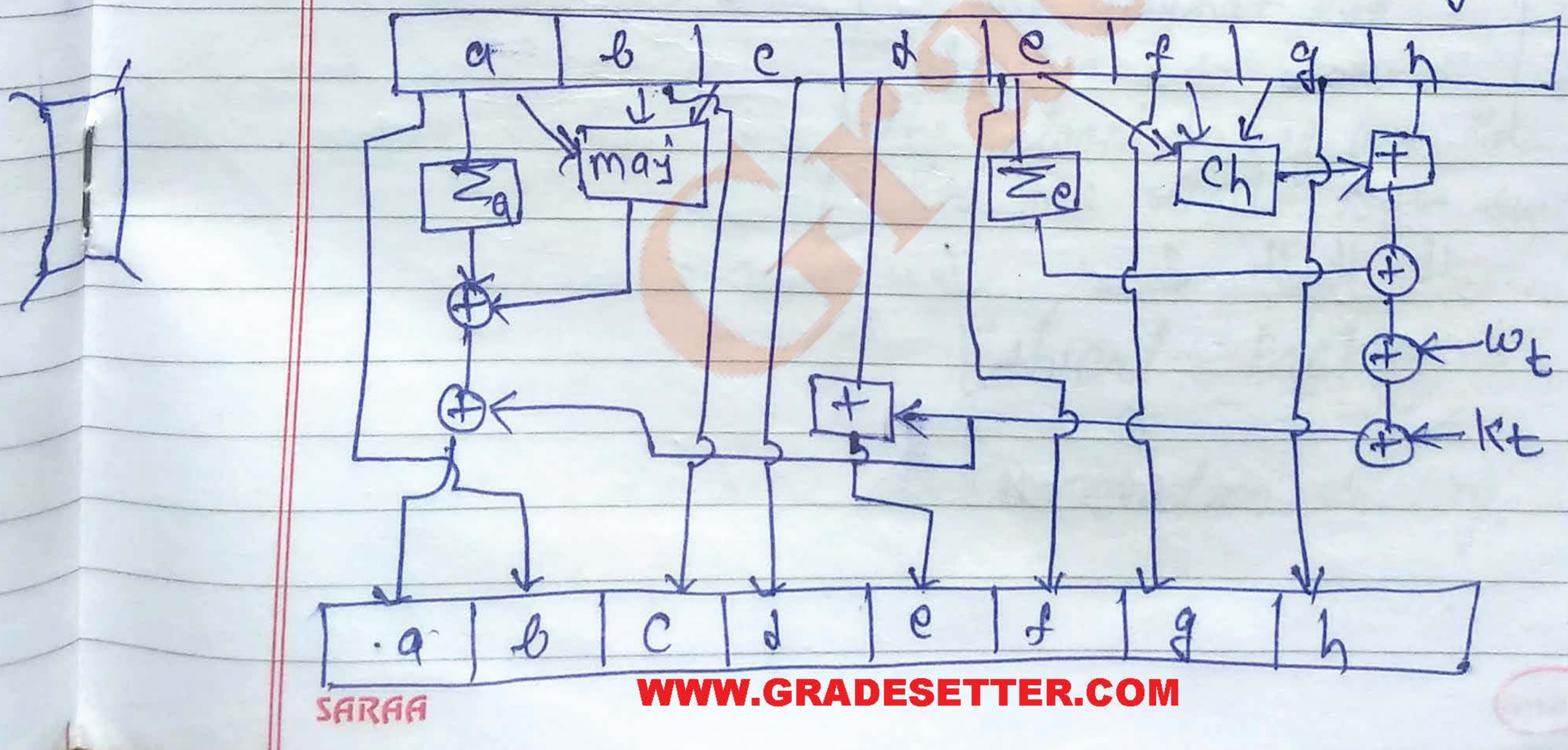
$$W_t = \overrightarrow{q}^{512}\left[w(t-2) + w(t-7) + \sigma_0^{512}(w[t-15]) + w(t-16) \right]$$

$$\sigma_0^{512} = ROTR^1(x) \oplus ROTR^8(x) \oplus SHR^7(x)$$

$$\sigma_1^{512} = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^6(x)$$

$ROTR^n$ - circular right shift of x by n-bit

$SHR^n(x)$ - left shift of x by n-bit by padding zero (0) to the right.



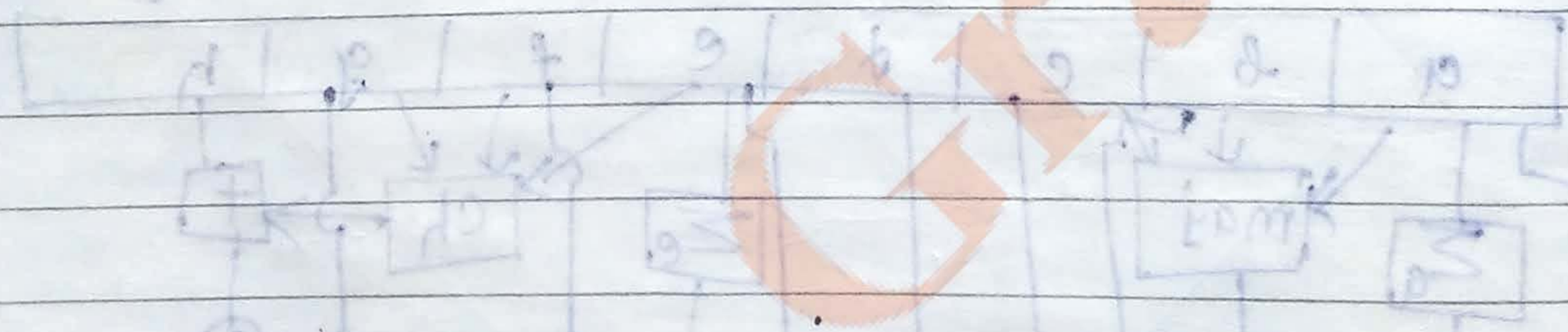
Date : / /
Page No :

$ch(e,f,g) = (e \text{ AND } f) \text{ XOR } (\text{NOT } e \text{ AND } g)$

$Maj(a,b,c) = (a \text{ AND } b) \text{ XOR } (a \text{ AND } c) \text{ XOR } (b \text{ AND } c)$

$\Sigma_a = \text{ROTR}^{28}(a) \text{ XOR } \text{ROTR}^{34}(a) \text{ XOR } \text{ROTR}^{39}(a)$

$\Sigma_e = \text{ROTR}^{14}(e) \text{ XOR } \text{ROTR}^{18}(e) \text{ XOR } \text{ROTR}^{44}(e)$



Ethical Hacking

Date: / /
Page No:

(1) Hackers:-

→ Hackers are highly skilled people/programmer.
→ they misuse the skill.

⇓

Type of hackers

(penetrate the network and test security)

Blackhat hackers

⇓

these hacker whose objective is
- malicious intent
- wrong object.
- still or destroy the data.

→ (Destroy the data)

Whitehat hackers / Penetration tester

⇓

perform hacking for good purpose

⇓

objective
↳ check the security of computer system or networks.

⇓

security professionals.

⇓

they using the same techniques like blackhat and grayhat but objective is to checking the loophole if possible (they give report to the owner)

Grayhat hackers

⇓

they perform the hacking for fun purpose.
- fun picture display
- they illegily inter into the network
- Not destroy the data

⇓ ⇓ ⇓ ⇓ ⇓

Ethical hacking
or
Penetration testing.

(2) Ethical hacking → action is performed with the Permission of organization.

It is the process of attempting to gain access to the resources without knowing, the username, passwords, or other normal means of access.

((with the Permission of the upper management))

Black box	white box	grey box
NO information is given to the ethical hacker only permission is given ⇓ same as Original hacking.	Information is Provides ⇓ Some time, user level access is Provided.	little bit information. is Provides. or limited information is Providing.

3.) Objectives / Reason for Performing ethical hacking / penetration testing :-

(i) To find the vulnerability or loop holes in systems or network configuration.

(ii) to justify the management to section the budget.

(iii) security training for network staff.

(iv) to test new technologies before Production.

SARAA

Date : / /
Page No :

(V) To reach legal requirement.

vulnerability - loop hole / weakness

windows :- service pack 1 ⟷ Remove vulnerability.
↓
service pack 2

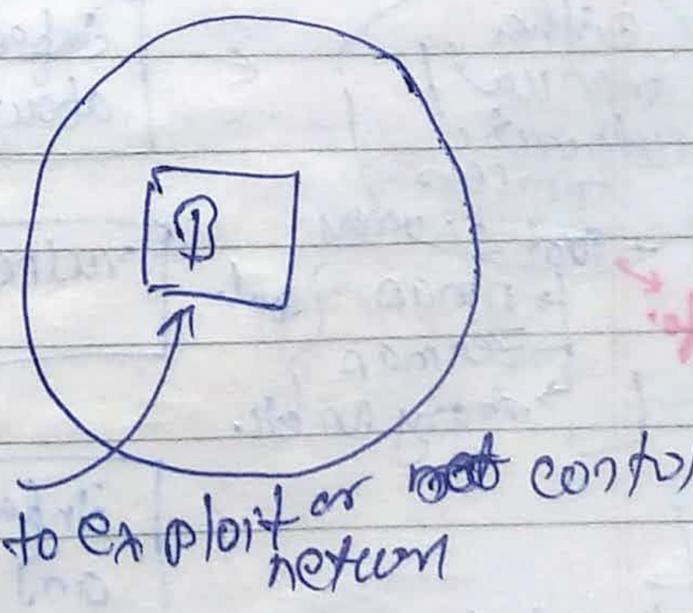
* Types of vulnerability →

- XSS (cross site scripting) → Result's in link authentication वाला पेज वो यहाँ नहीं थी।
- SQL injection → with the help of Query.
- Buffer overflow → improper authorised execution.
- Insufficient logging vulnerability

* Exploit - exploitation

payload -

payload is a software code, that is used to control system.



(ii) In 2015, over a half a billion data of companies is stolen & lost by hackers, which is 23% in

(iii) Fishing attack was increased by 55% as Compare to Previous year.

on average one million attacks was blocked on each day in 2015.

which is increased by 117% as Compare to 2014.

(iv) Ransomware was increased by 35% as Compared to Previous years.

hackers encript the file of web server and demand hefty amount of money for giving the key of decryption. They threaten to public data online or delete. If ammount is not paid to them.

(v) According to this report IOS operating system is most vulnerable as Compare to android, windows operating system

i) In 2015, 78% website are having vulrenability, out of which 15% are found to be critical. The

1 in 3172 website are found with malware in 2015.

5585 is the new vulrenability found.

viii) The distributed deniel of service attack is most

And they mostly used ICMP floodations attack, where a large number of bing request, machine not able to perform work properly.

x → virtual machine – vmware ✓
virtual machine ✓

Kali Linux ⇒ 2.0
→ software tools, which are uses for doing ~~kali linux~~ ethical hacking

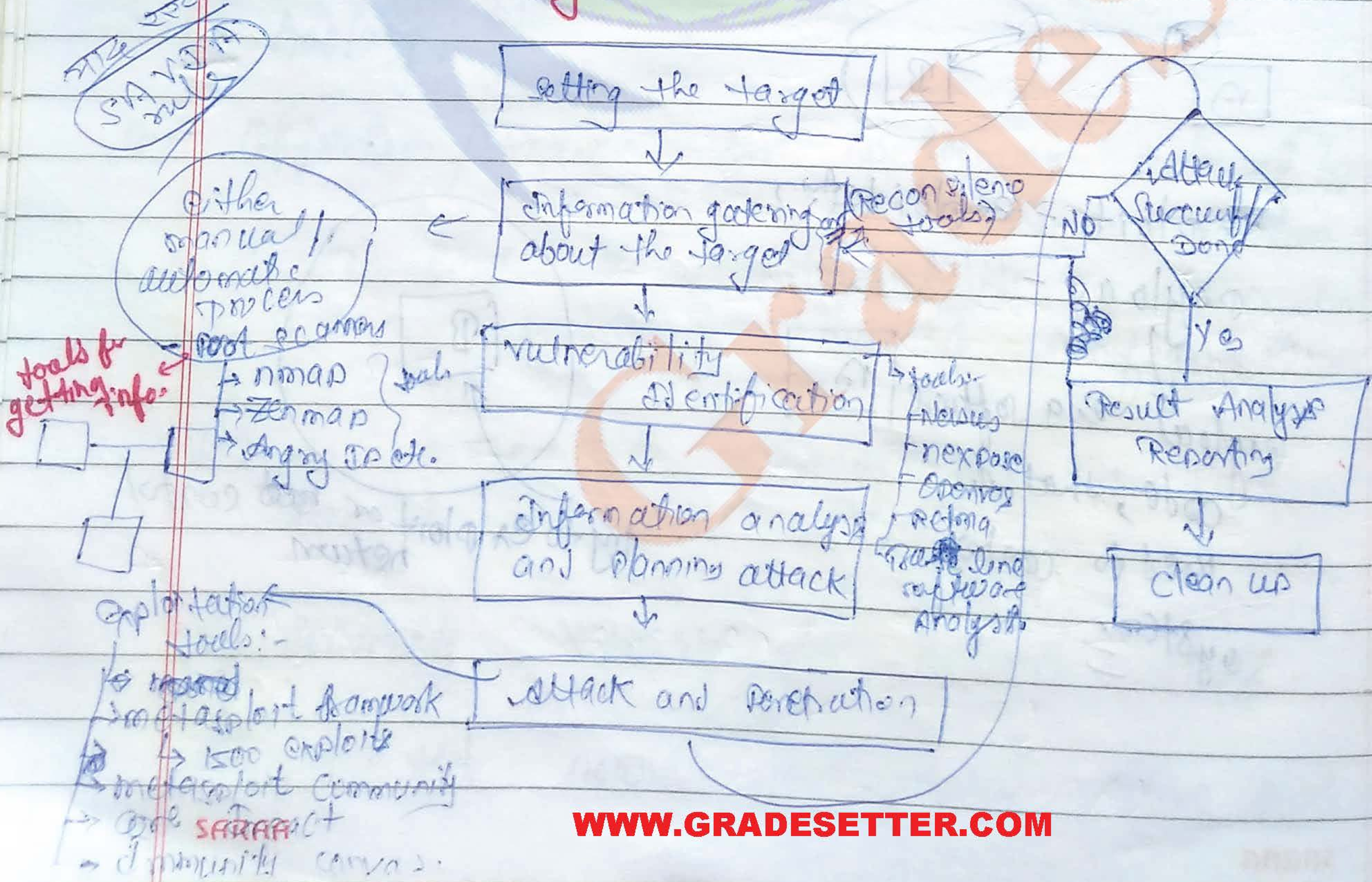
Enjoy tutorial

★ **Hackers & crackers:–**

Hackers ↓ subpart → crackers → objective – for finan(cial) or hacking with malicious objective or Destroy the system of other resources or criminal action or they are criminals

subpart → penetration testing or ethical hacking

✶ **Penetration testing process / methodology of penetration testing or ethical hacking**



(9) Kali linux

* Social engineering -
↳ Using social

TCP protocol
TCP handshake

Kali linux! Information gatering - Port scanner - nmap.
↳ (nmap)
↳ Information gatering on target machine.

eg door lock है आप नहीं, पर enter नहीं करोगी //
enter नहीं करते हैं
सिर्फ find करते हैं

* (a) Vulnerability assessment (identification)
or
(b) Penetration testing.
↳ enter भी करते हैं,

Process of finding the vulnerability on the software eg. some vulnerability crack windows 10 vulnerability //

* ~~Hack~~ Hacktivism - social or political purpose
↓
~~Hack~~
hacktivist

eg:-> wikileaks
↳ this is a hacktivist group //

Date : / /
Page No :

Email → Electronic mail

↳ send message electronically

Concept of email started : 1965 (in stand-alone system) ↑ at the time network was not come //

MAIL BOX

A
B
C
D
E

stand-alone system

A → E ilel

ARPANET - Advance research Project agency network

↳ 1st email is send by in 1972 by Ray Tomlison using electronic mail. on he was used @ at this time.

name of user @ name of computer
gaurav@rediffmail.com

1976 :- 75% traffic gain
(till only text message was used.) //

Now)

text + audio + video + picture
A send कर सकते हैं

* Three components of architecture of mail :-
(i) User Agent (UA)
(ii) message transfer agent (MTA)
(iii) Message Access Agent (MAA)

SARAA

Date: / /
Page No:

(*) Four scenario

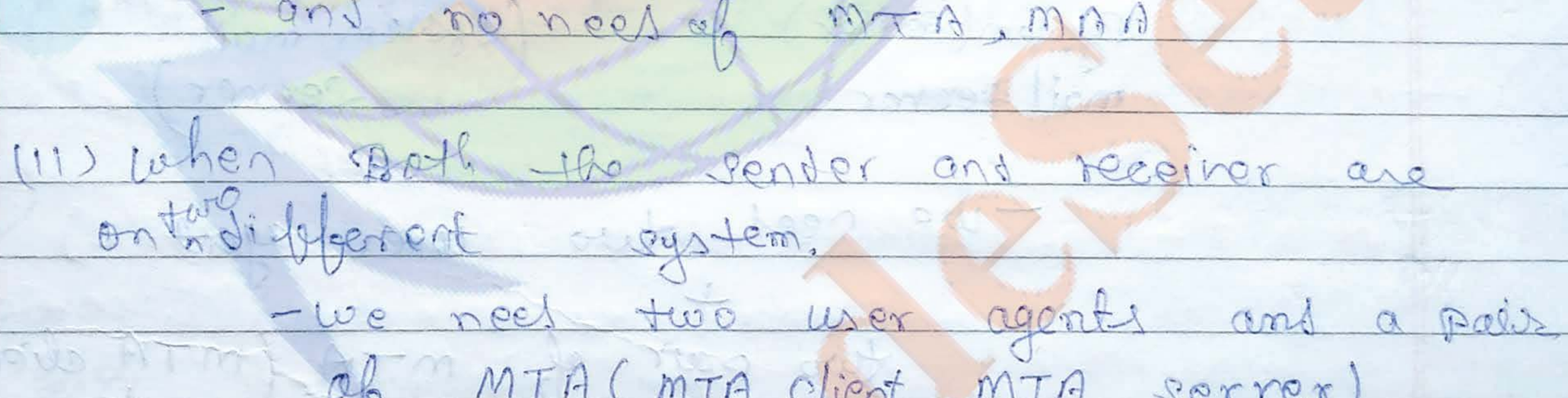
(I) when the sender and receiver are on same system.

(need two User agent)
(UA's)

- and no need of MTA, MDA

(II) when Both the sender and receiver are on two different system.

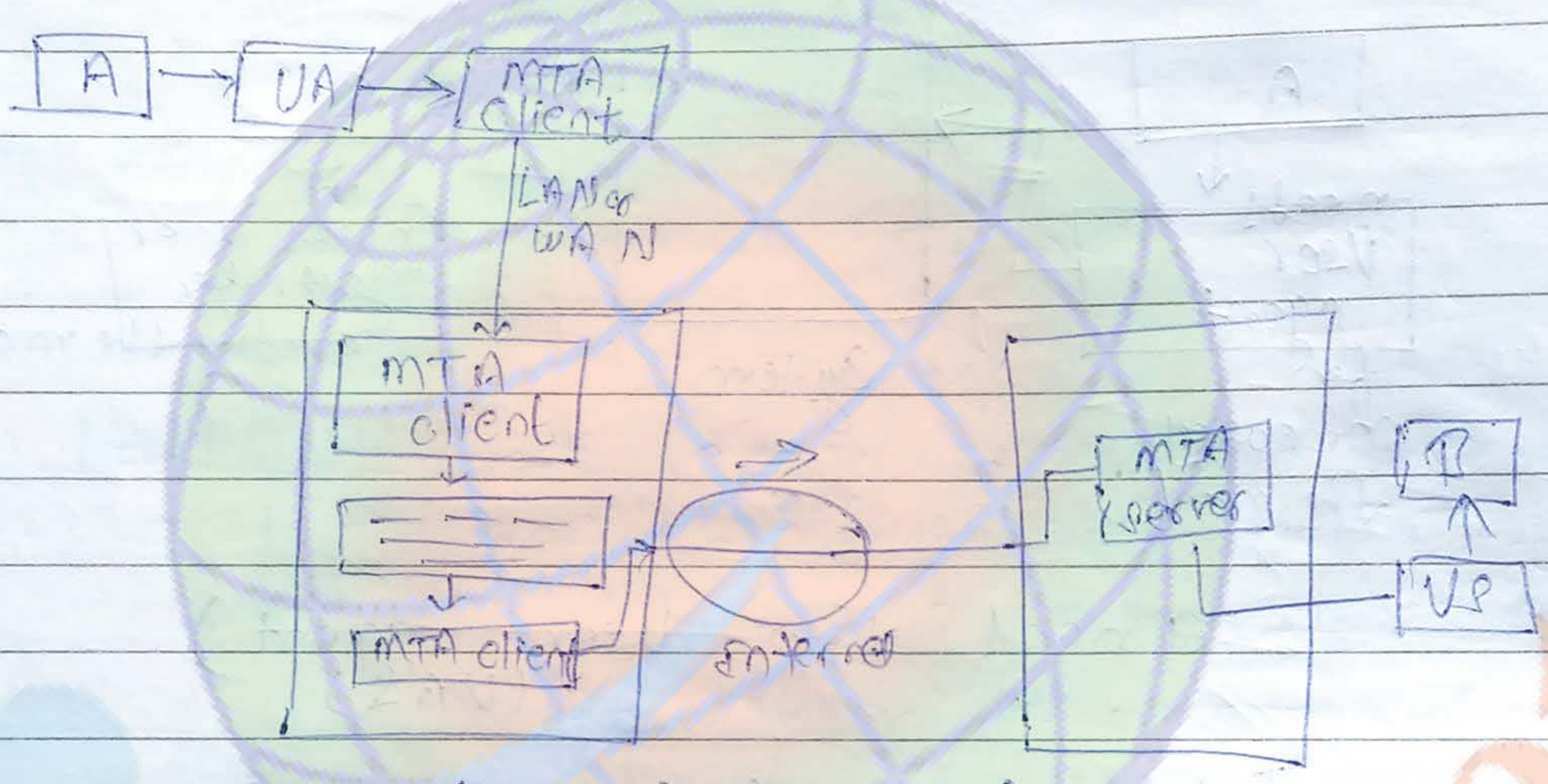
- we need two user agents and a pair of MTA (MTA client, MTA server)



Date : / /
Page No :

(iii) when the sender is connected with the help of LAN/WAN

(iii) when the sender system is connected to mail server with the help of LAN or WAN.



System (sender) mail server

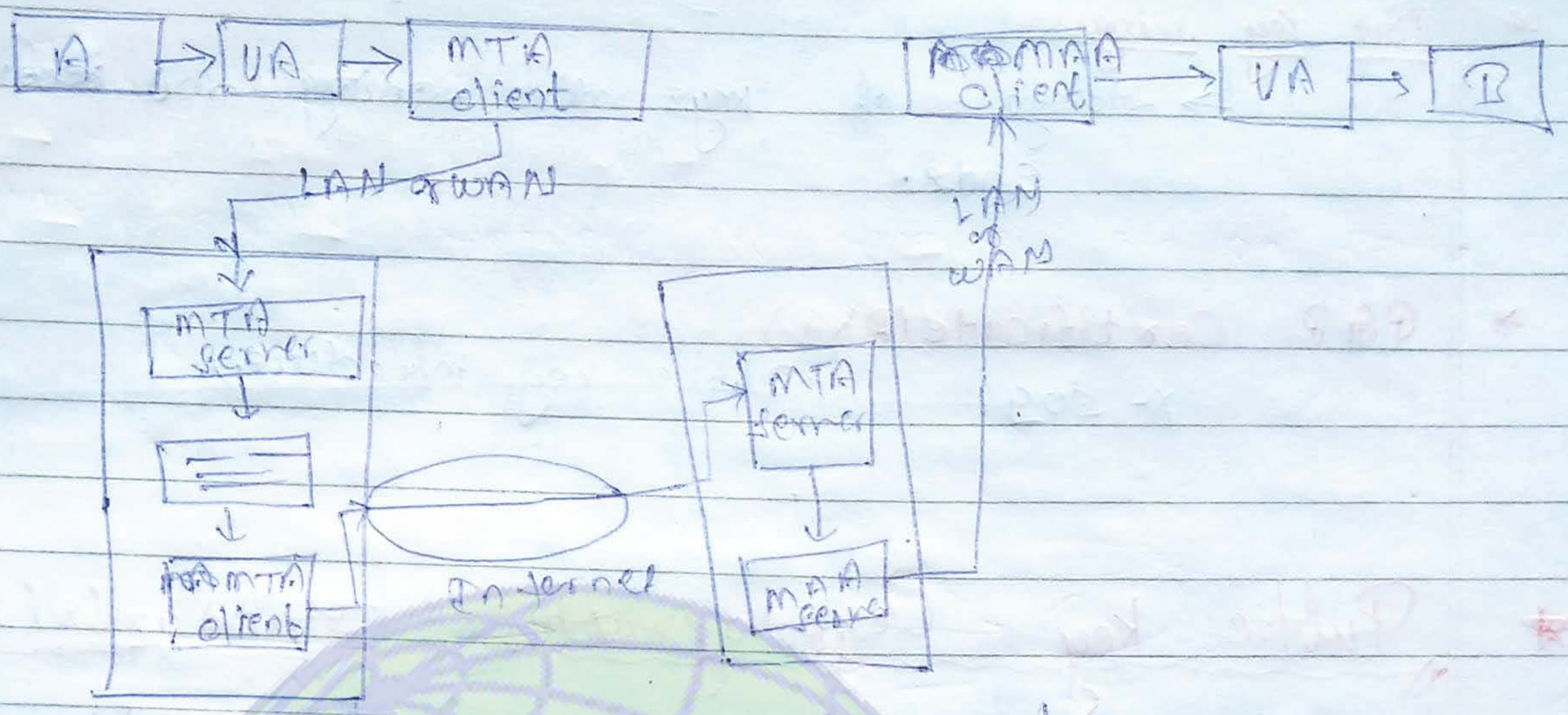
(system mail server)

- we need two user agent
+
two pair of MTA (MTA client + server)

(iv) when the sender and receiver are connected to mail server with the help of LAN or WAN.

- we need user agent
+
two pair of MTA (MTA client + server)
+
One pair of MAA.

Date: / /
Page No:



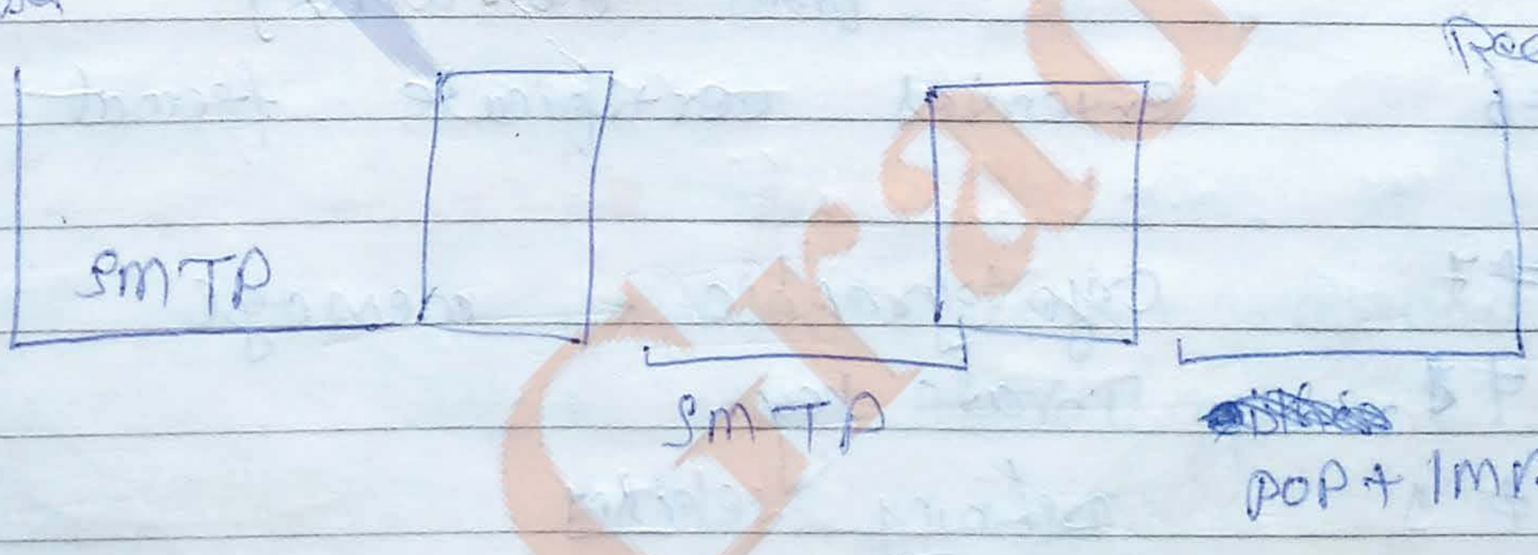
mail Protocol:-

(a) SMTP :- (Simple mail transfer Protocol)

(b) POP :- Post office Protocol

(c) IMAP :- Internet message access Protocol

(MTA) → MAA



(d) MIME : multipurpose internet mail extension.

↳ sky code

(different language को send करने के लिए use होता है)

Date : / /
Page No :

* PGP Key rings :-
  ↳ Storage of keys at sending and receiving ends.

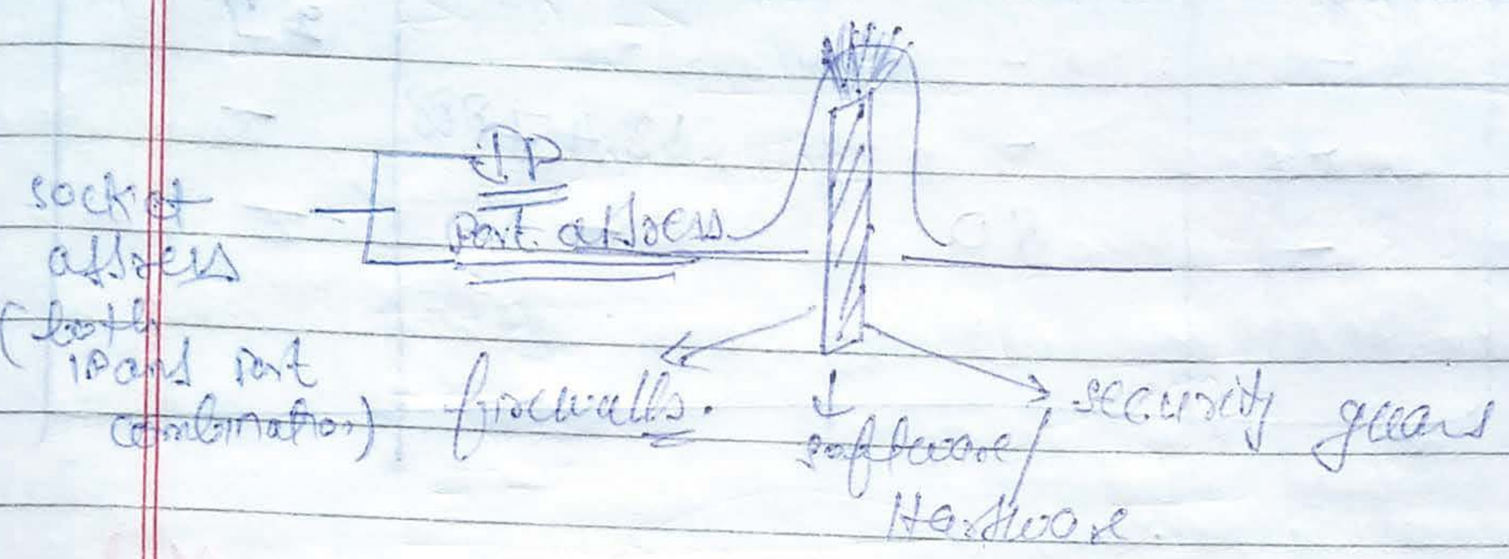
* PGP Certificate (PKI) :-
  X-509
  ↳ Public key infrastructure.

★ Public key Cryptographic standards (PKCS) :-
  ↳ Developed by RSA security
  1990

PKCS #1	RSA algorithm, encryption decryption
PKCS #2	RSA encryption for message digest.
	An In 2010, it merges with PKCS #1
PKCS #3	diffie hellman key exchange.
PKCS #4	RSA key syntax. An In 2010, merged with PKCS #1
PKCS #5	Password based encryption (PBE) (Process of generation of secrete key from password)
PKCS #6	extended certificate format
PKCS #7	cryptographic message
#8	private key
#9	defining selecting
#10	requests
#11	cryptographic tokens.

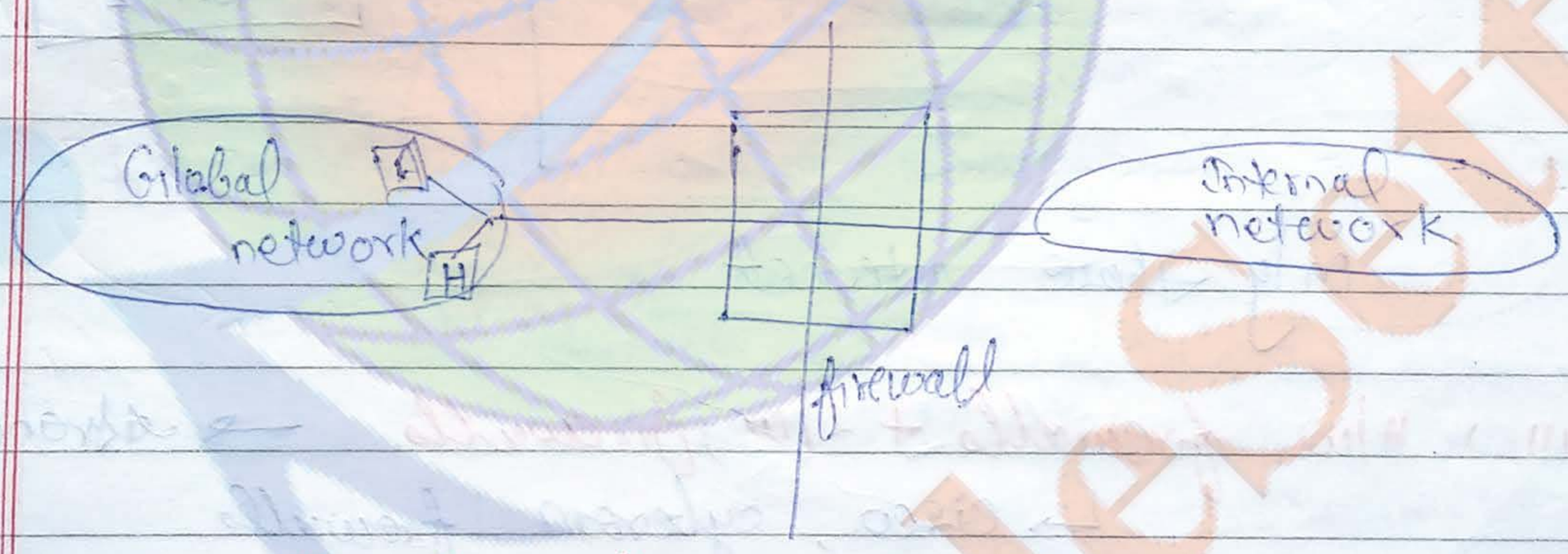
Firewalls

Date : / /
Page No :



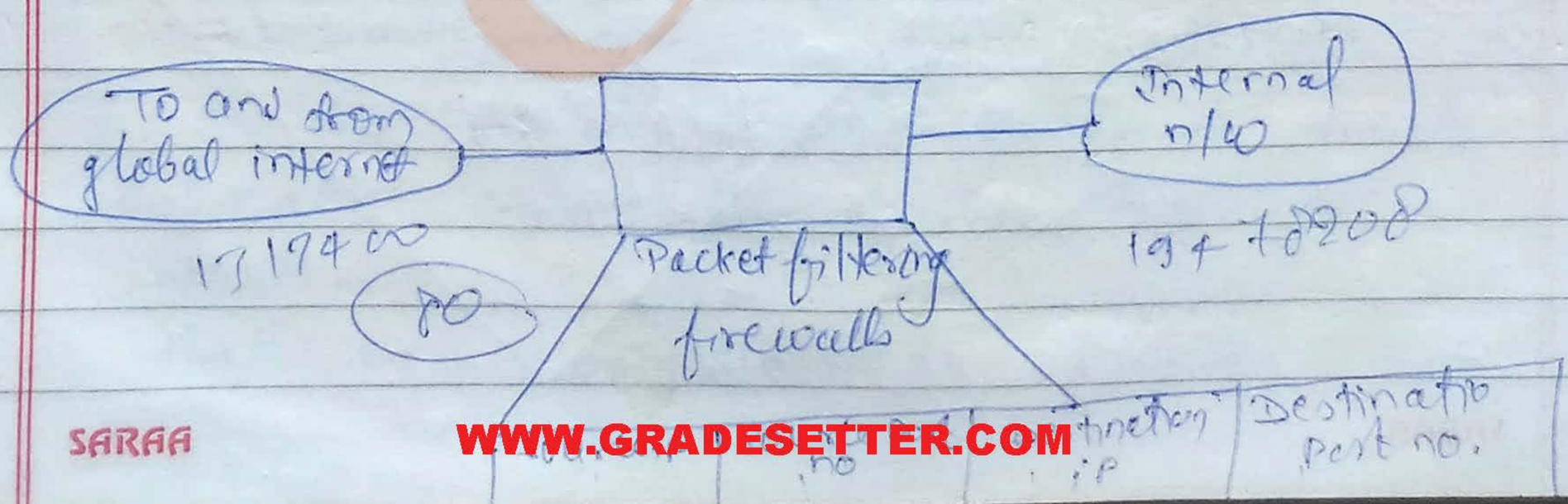
ACL - (Access control list) :-
↳ Router के अंदर access control list होता है।

firewalls:
↳ 1992.
↳ Security Policy.



* Type of firewalls :-

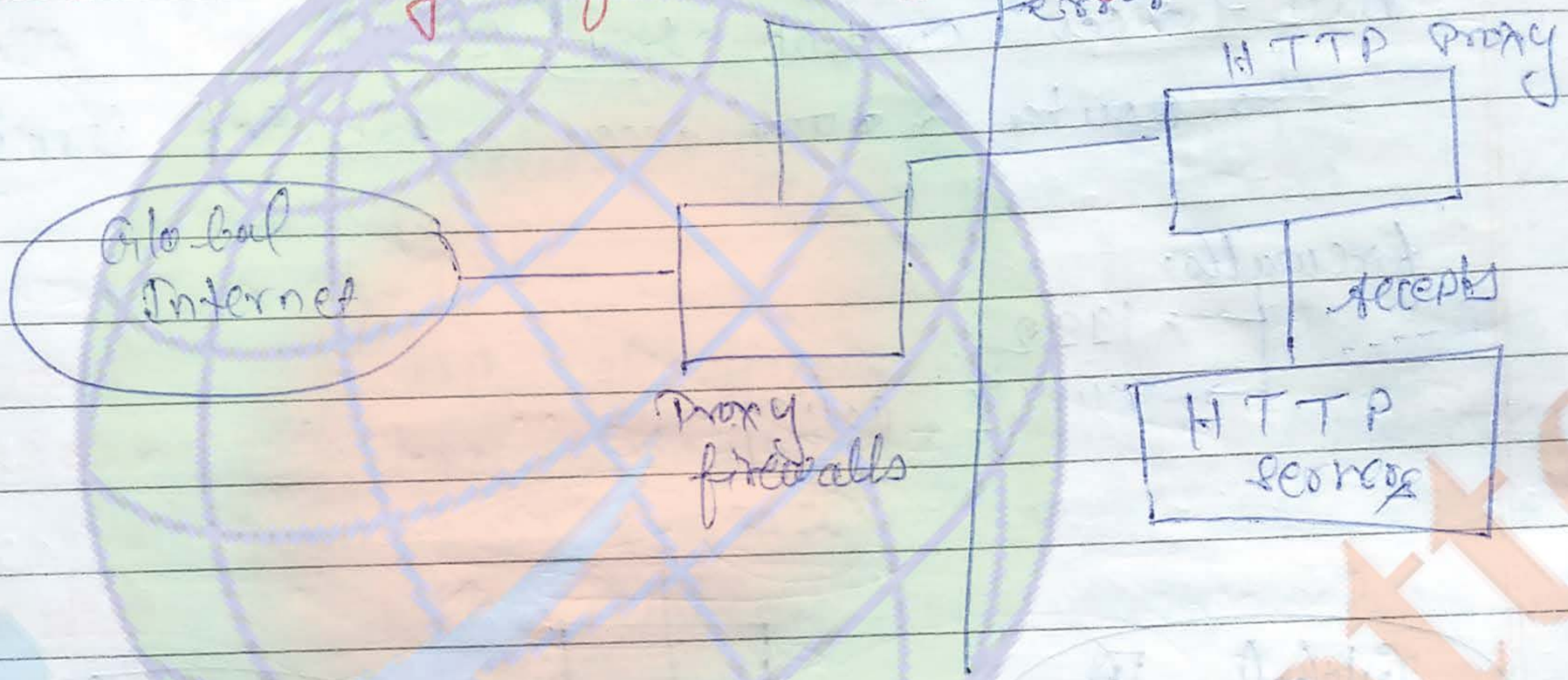
(1) Packet filtering firewalls :-
↳ work on network + transport layers.
↳ filters all incomming and outgoing packets.



Date : / /
Page No :

1313400	—	—	—
—	—	—	27
—	—	1947888	—
—	80	—	—

(ii) Application layer firewalls (Proxy firewalls)



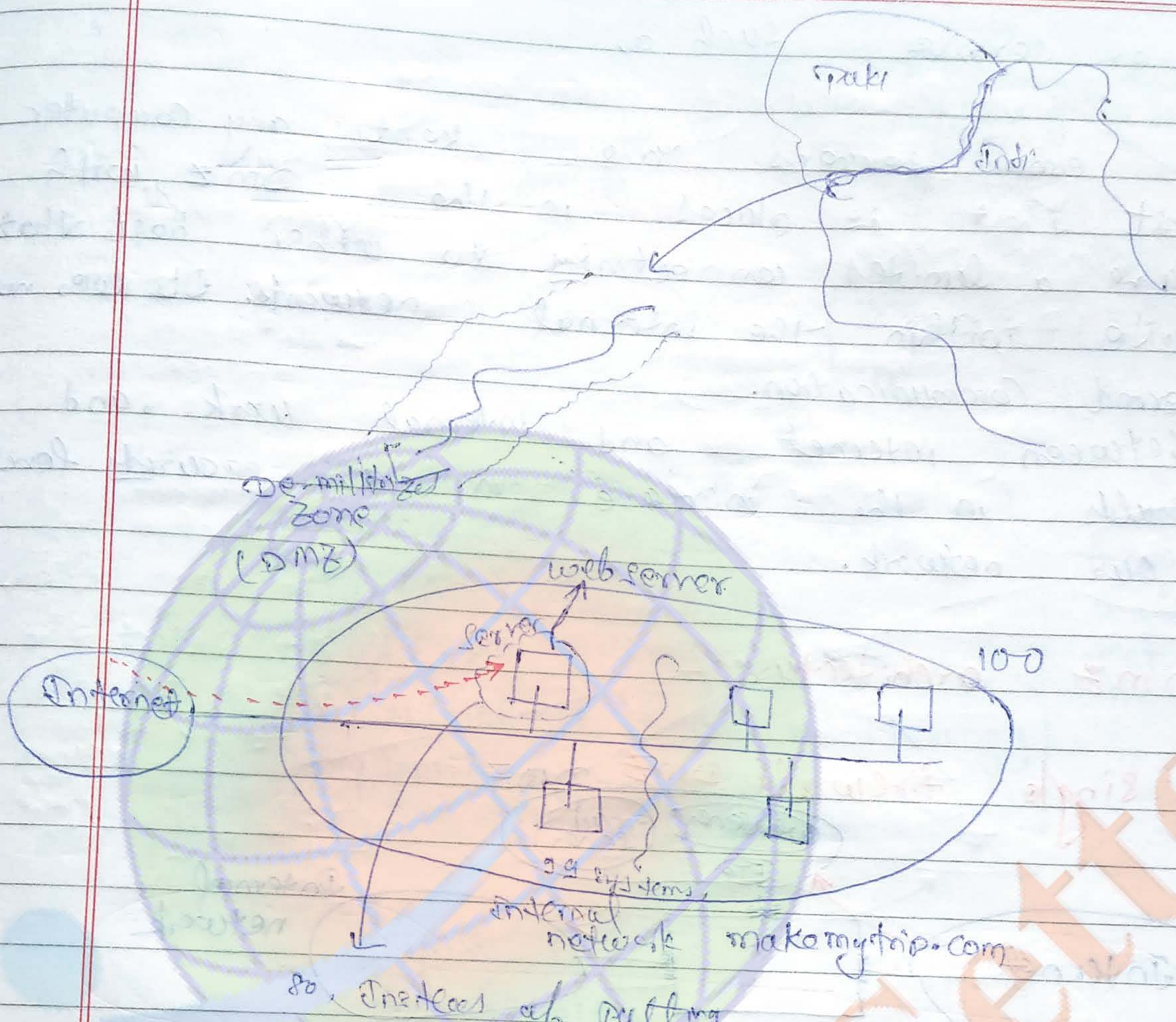
only these connect

(iii) H/w firewalls + s/w firewalls → Advanced paid
↳ Cisco, cyberoam firewalls

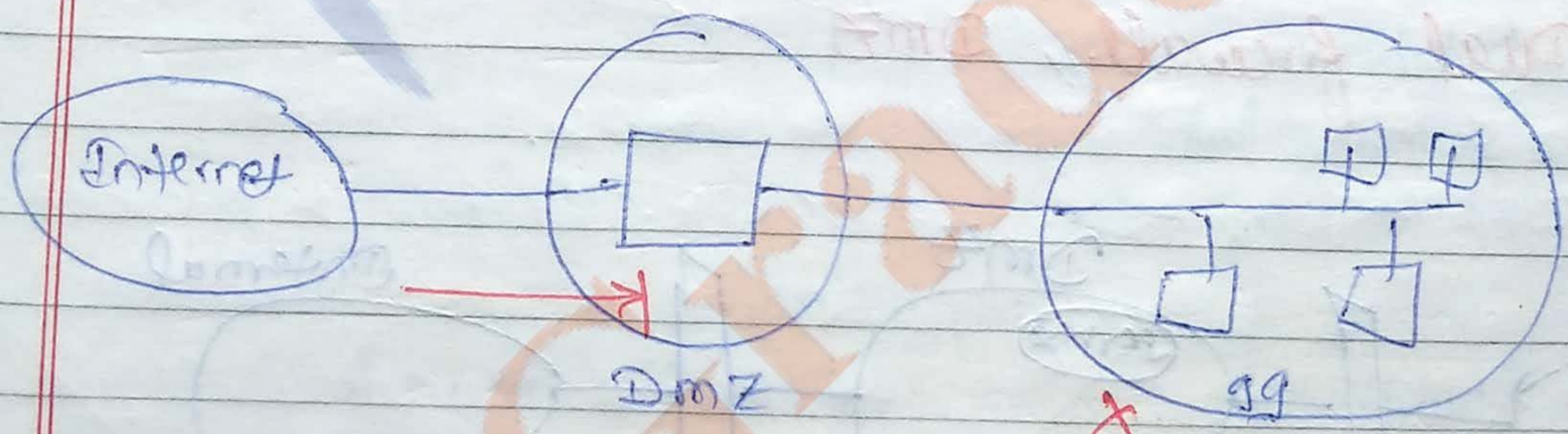
(iv) Software firewalls → basic
L.O.S firewalls

DMZ (De-militarized Zone)

Date: / /
Page No:



80. Instead of putting it internally, DC is putting to



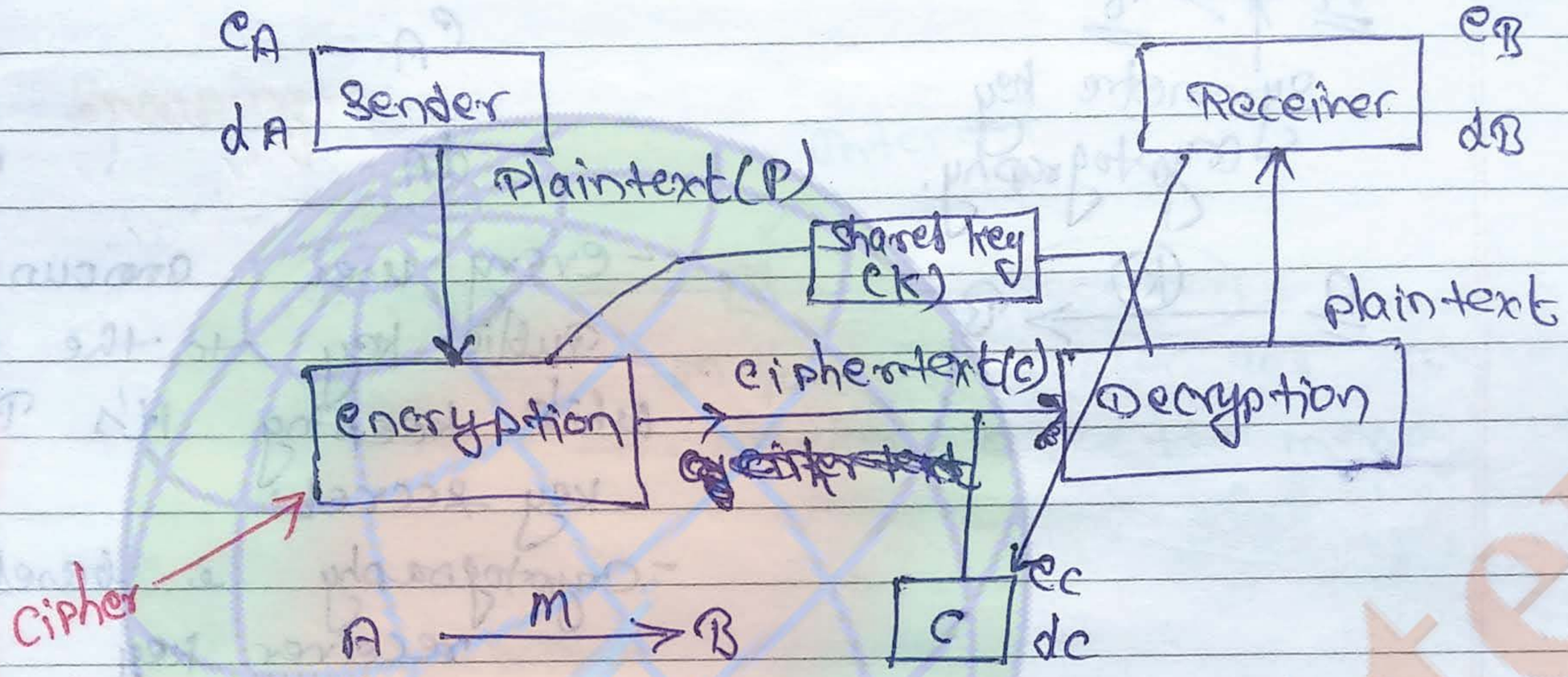
In the de-militarized zone, the most vulnerable components of the computer networks.
that are responsible for proving any

SARAA

Date : / /
Page No :

★ Crypto graphy
hidden (art of secret writing) → art of writing

Cryptography is defined as an art or science of transforming msg to keep the message secret.



Cipher - are the basically encrypted or decrypted algorithm.

cipher text - transformed message.

cryptography

Symmetric key cryptography
or
secret key cryptography
or
classical cryptography
⇓
Same key is used for encryption and decryption purpose

Asymmetric key cryptography
or
Public key cryptography
⇓
Different key is used for encryption and decryption.

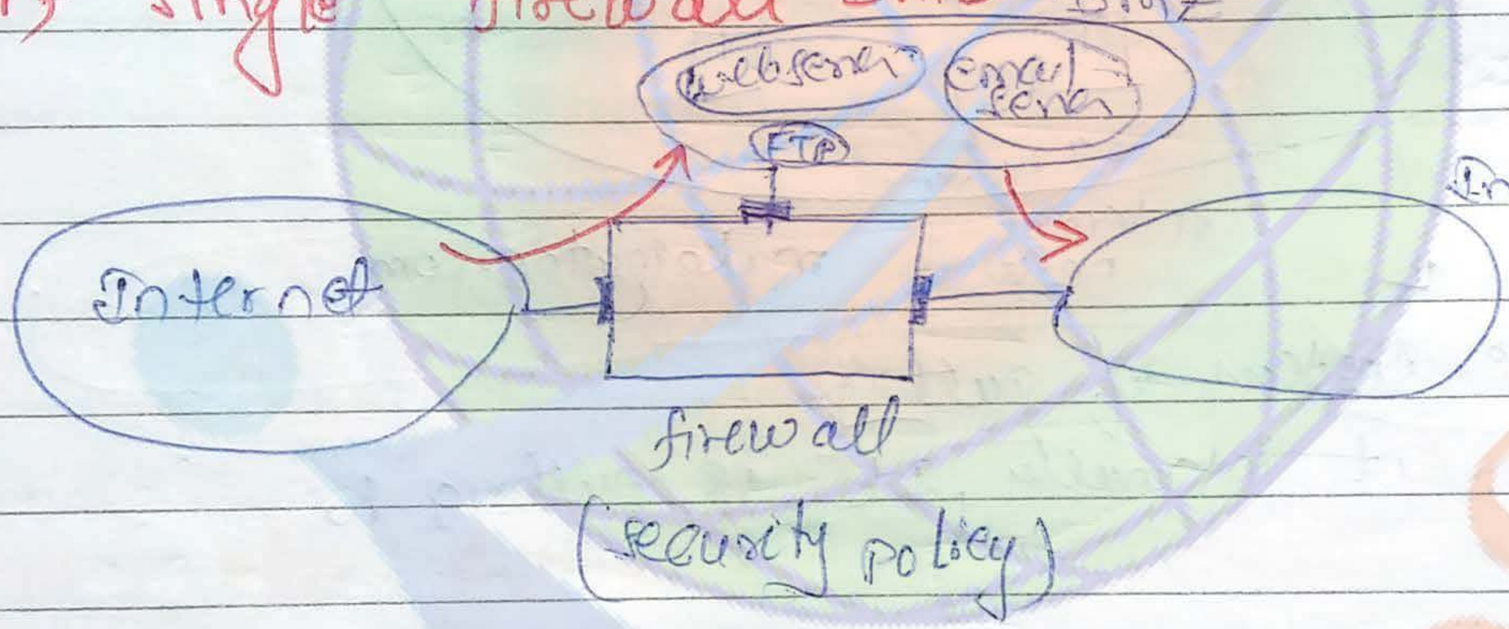
SARAA

user service such as

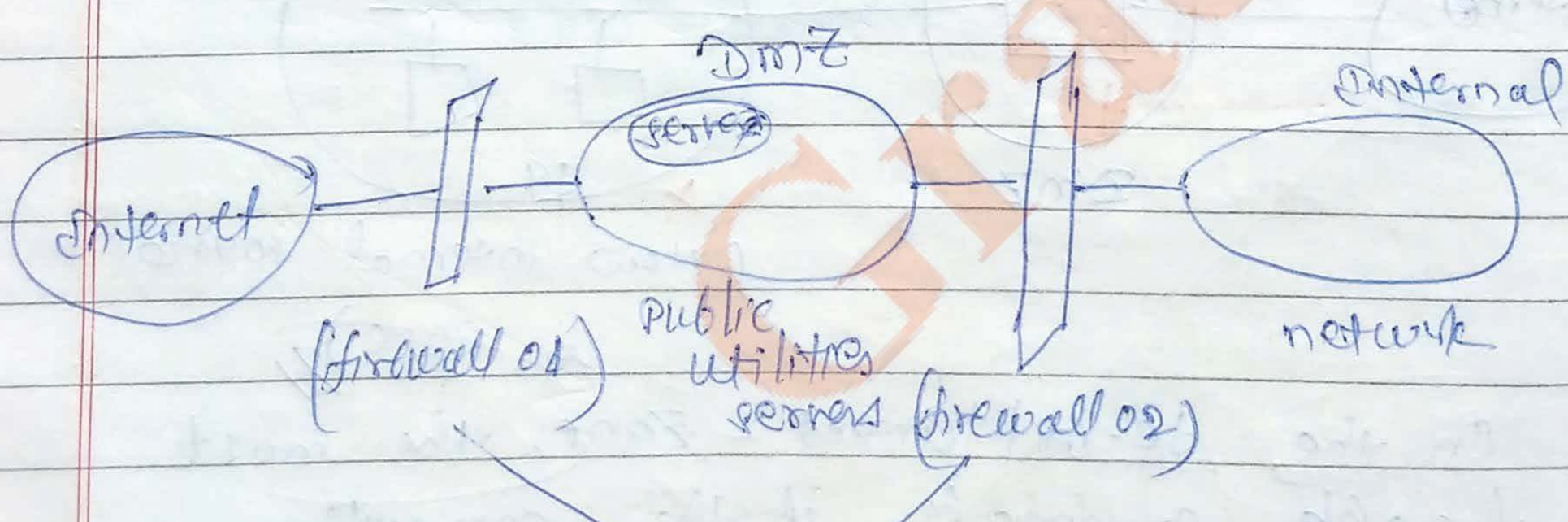
email servers are kept any Computer host that is placed in the DMZ, with have a limited connectivity to other host that reside within the internal network. It does not permit Communication. between internet and internal work, and results in the increase in the security level of our network.

★ DMZ architecture:

(I) Single firewall DMZ



(II) Dual firewall DMZ



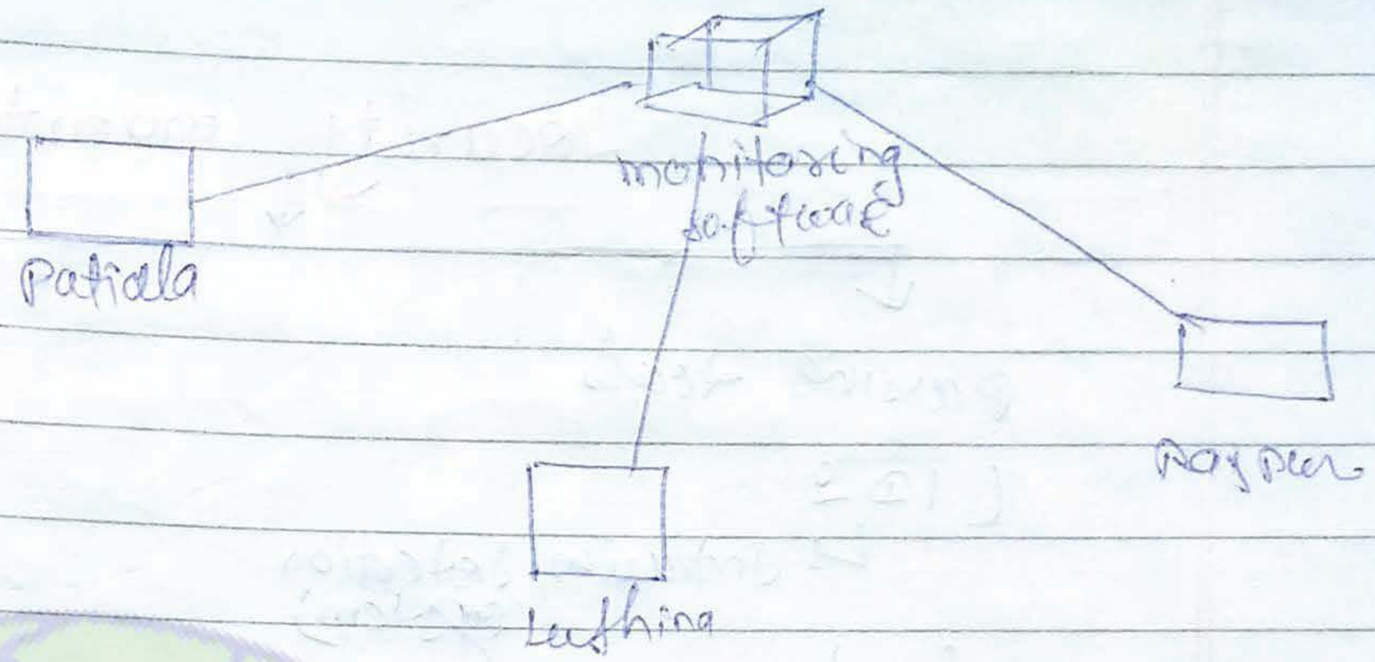
shows the of different Company. (Each Break with the same method.))

SARAA

Devices of monitoring networks

* Network monitoring & Diagnostic devices

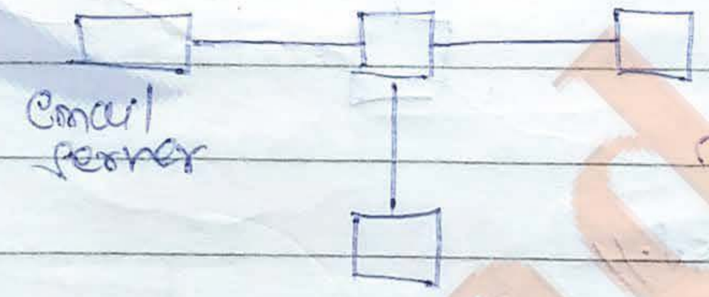
Date: / /
Page No:



- Win Pcap
- PRTG
- Cacti
- Zabbix
- NTM (network traffic monitoring)
- Big Brother

} General Tools for network monitoring

- These softwares are mostly Graphical Interfaces!-



- Snort (W+L) (windows Linux)
- wireshark (W+L)
- Bro (Linux only)
- OSSEC (Open source security)
- Fragroute

} Network security tools for network monitor.

Date : / /
Page No :

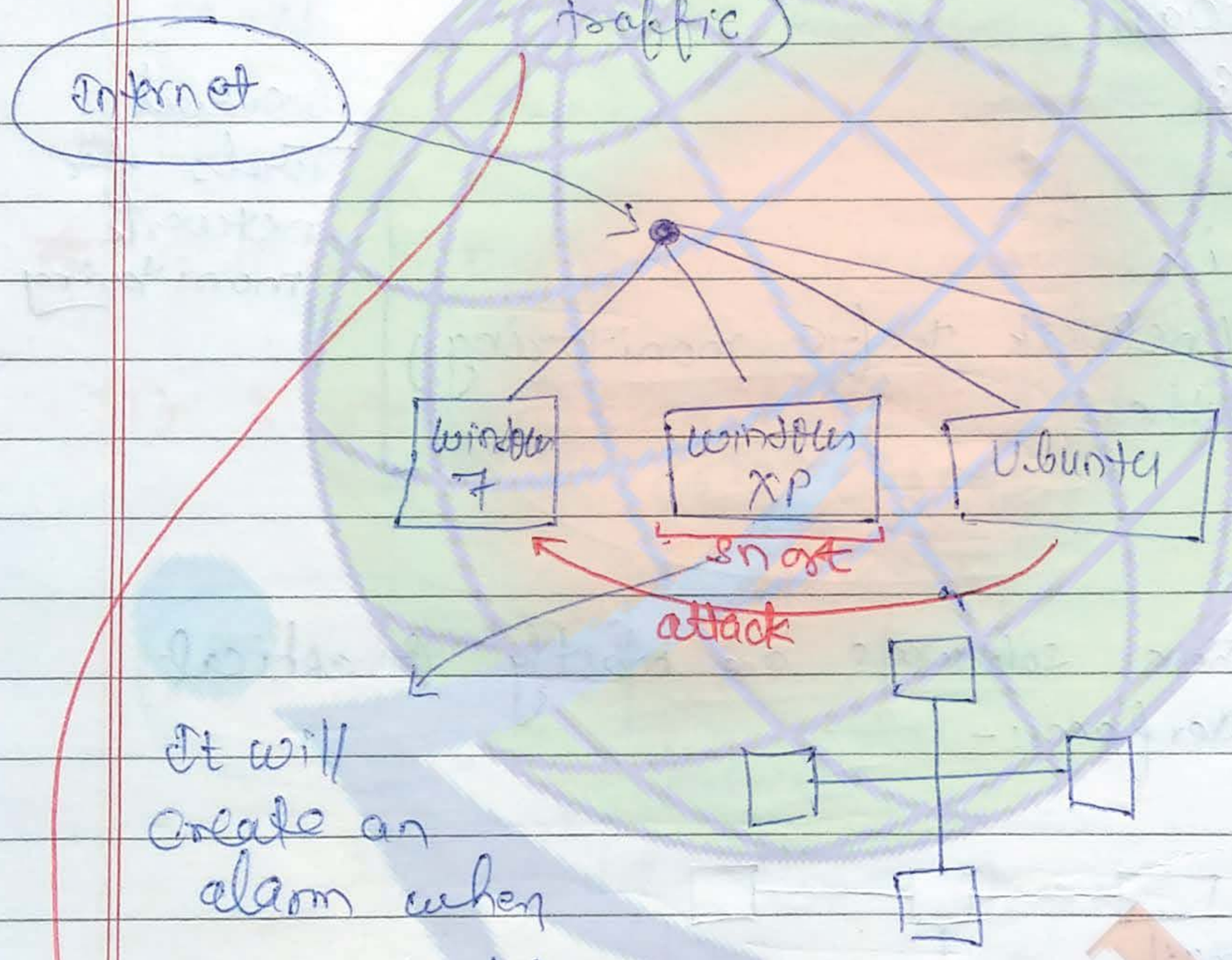
Security monitoring

passive tools

(IDS
↳ Intrusion detection system)
(only monitor the traffic)

active tools

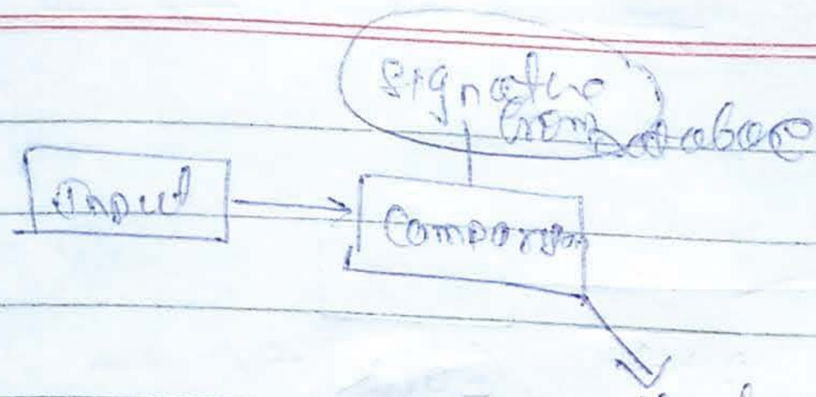
(IPS) or IDPS
↳ Intrusion prevension system)
↓
Intrusion detection and Prevention system.
(It detect the attack and also try to stop the attack or prevent)



It will create an alarm when any unwanted access is happened.//
IDS ← It will detect the attack. (inform)
IDPS ← It will stop the attack. (inform & prevent)

signature based or pattern matching

Anomaly based (statistical based)

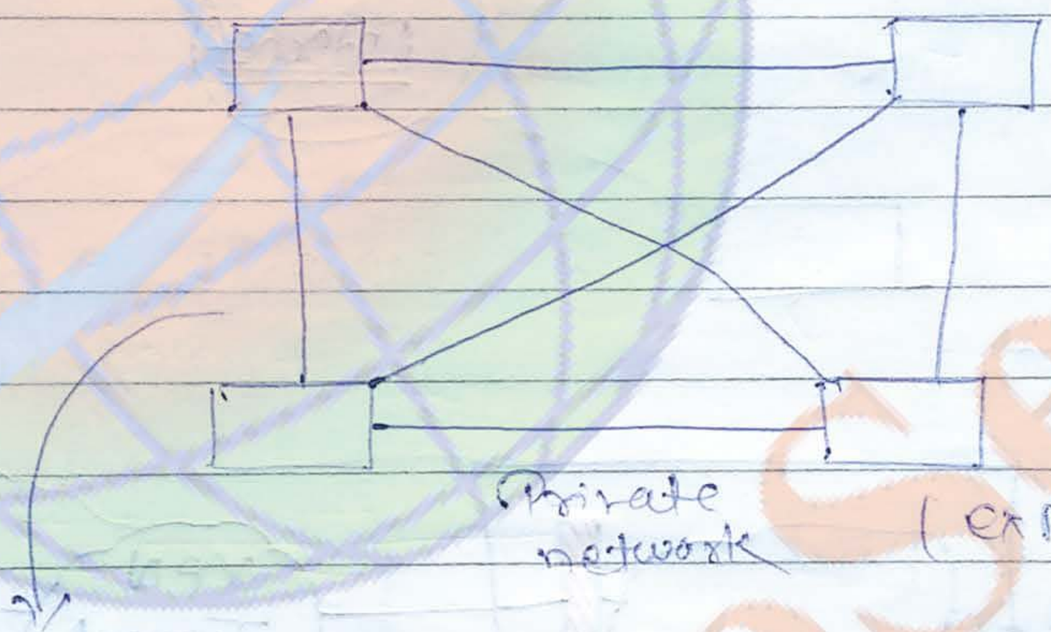


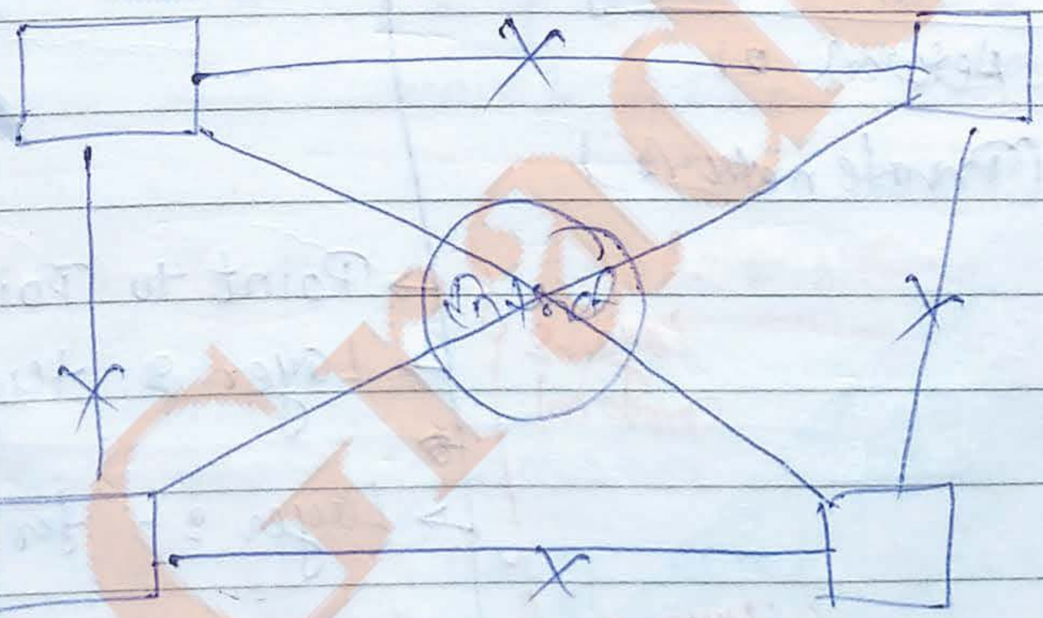
- Database होता है
- No database concept

Kali Linux

* Virtual Private network (VPN) :-

→ Private network over the public network





Public network (SERVER)

dedicated b/w sender and receiver

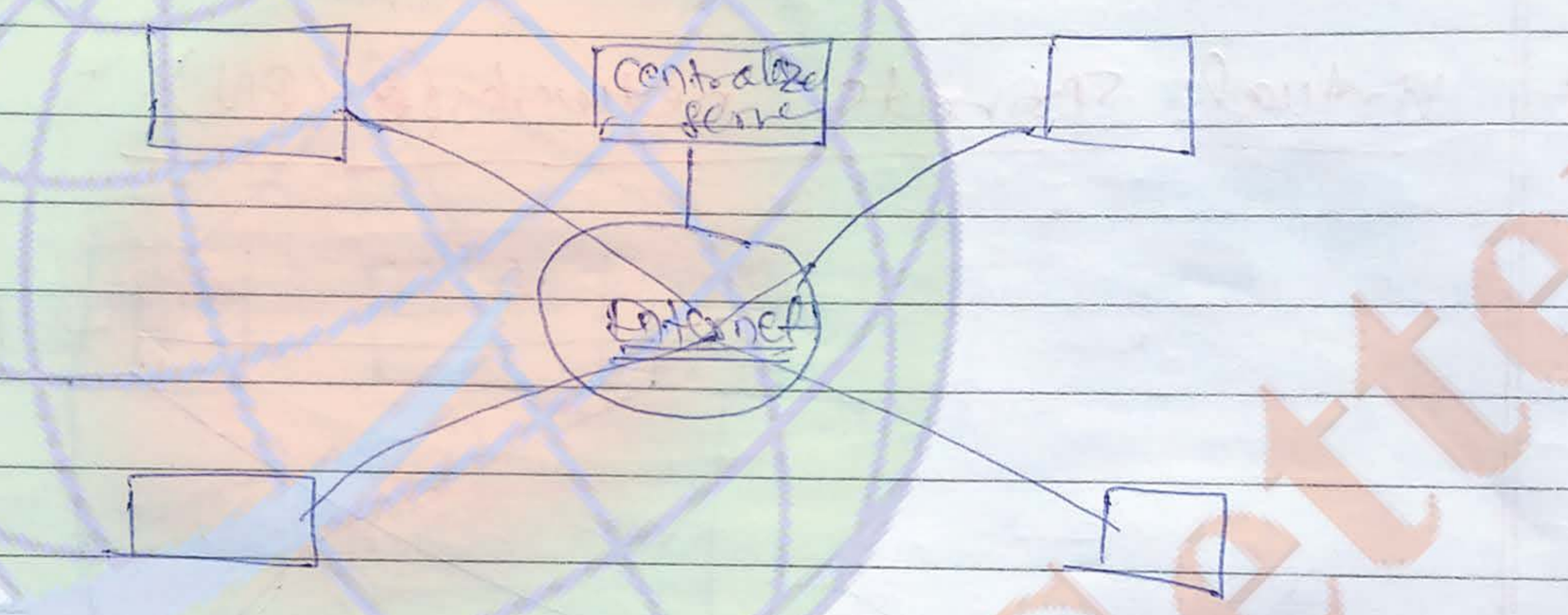
virtual network

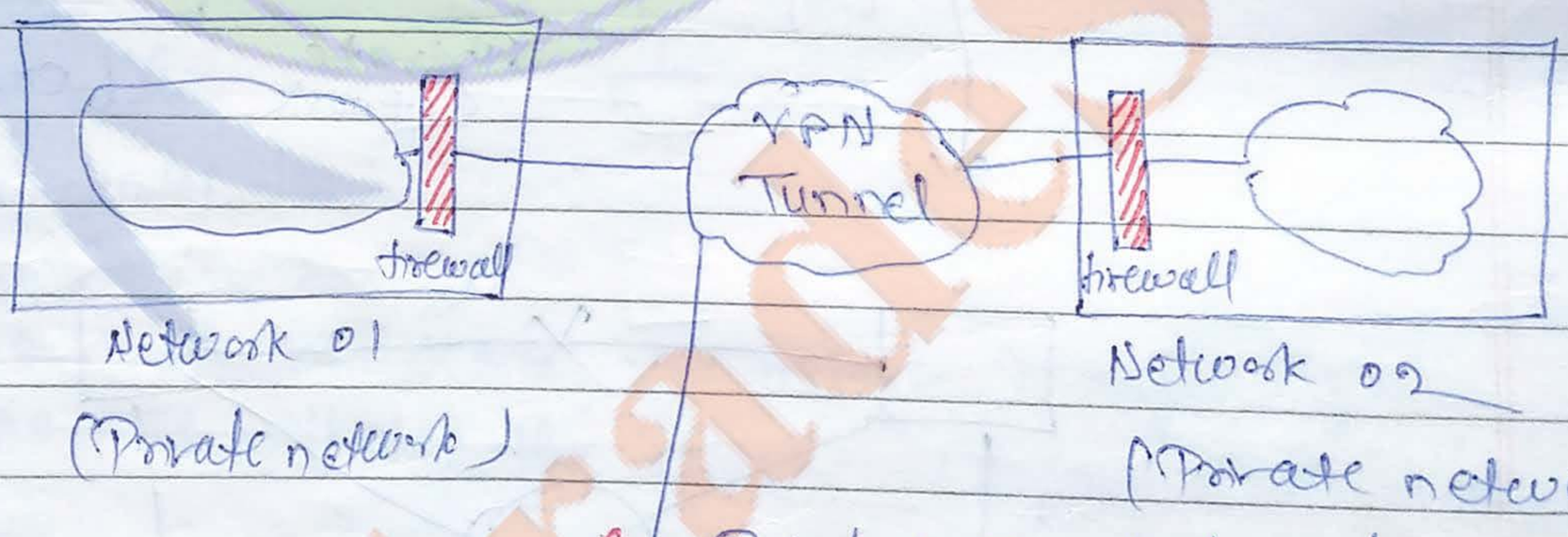
Date : / /
Page No :

(Quality of services)

- Private network over the Public n/w

- Tunneling + security + Quality of service.
  - Authentication service
  - Encryption service
  - Integrated service





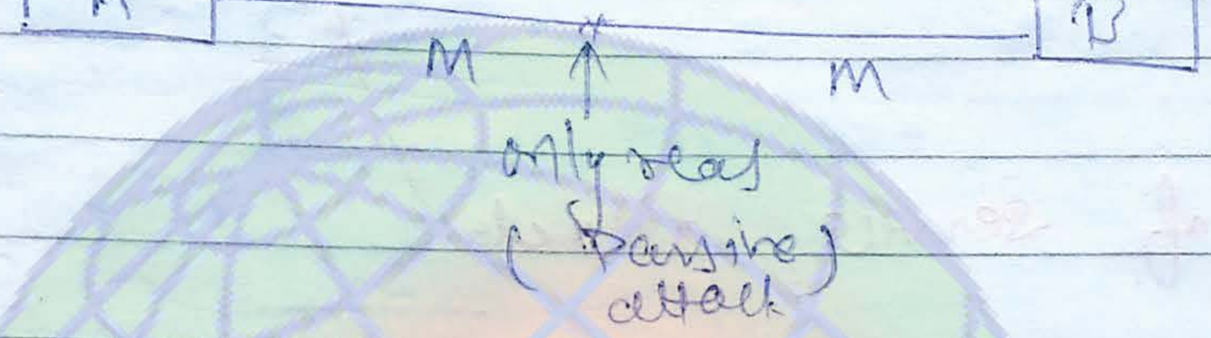
Layer-2 protocol
- Point to Point tunneling Protocol
- Layer 2 - tunneling Protocol (L2TP)
- Layer 2 - forwarded protocol

Layer-3
- IP SEC

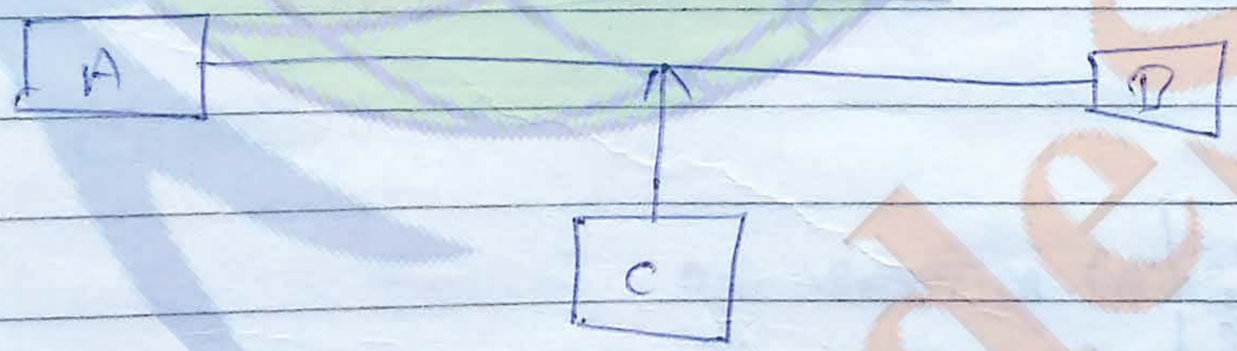
Layer-4 (Transport layer protocol)
- SSL

SARAA

Passive attacks
- only read the data
- Passive wire tapping or Snooping



Active attacks or man in the middle attack
- modification or alteration of data.
(MAN IN THE MIDDLE attack)
eg: CAIN & ABEL



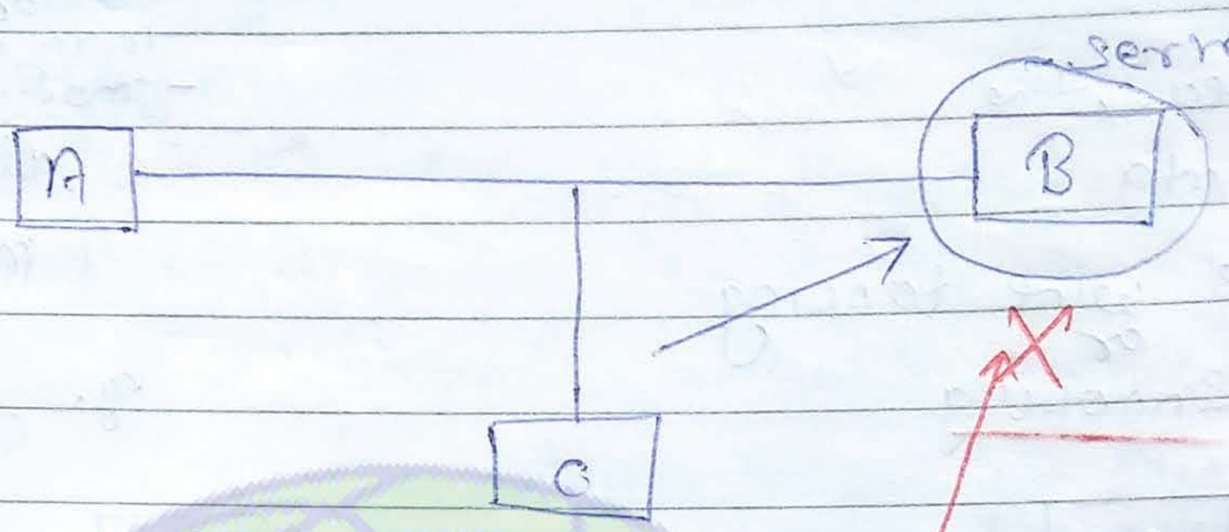
★ MASQUERADING or SPOOFING:-

When some person unauthorisely sends the message using some another person identity.

SARAA

Date : / /
Page No :

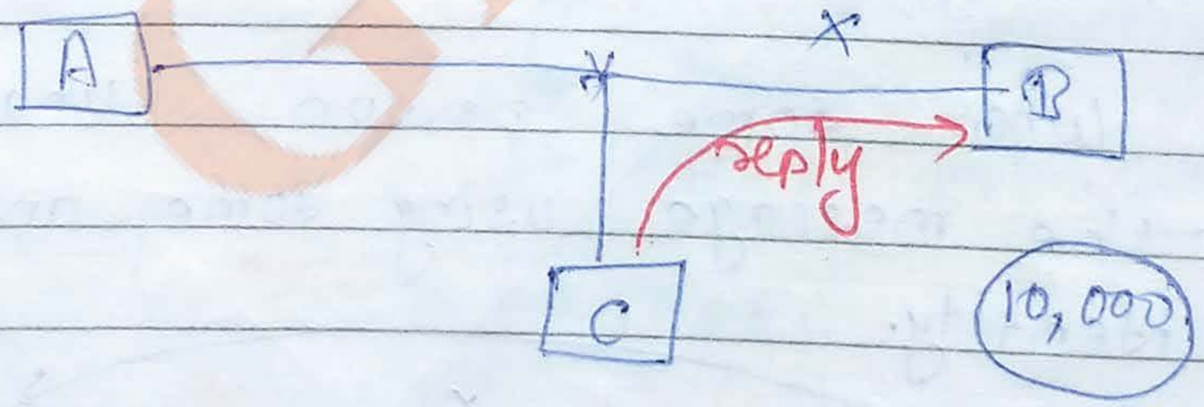
* Delay : (temporary inhibiton of service)
* DOS: long term inhibiton of service



- Denial of service attack

* Phishing attacks:-

* Replay attacks:-



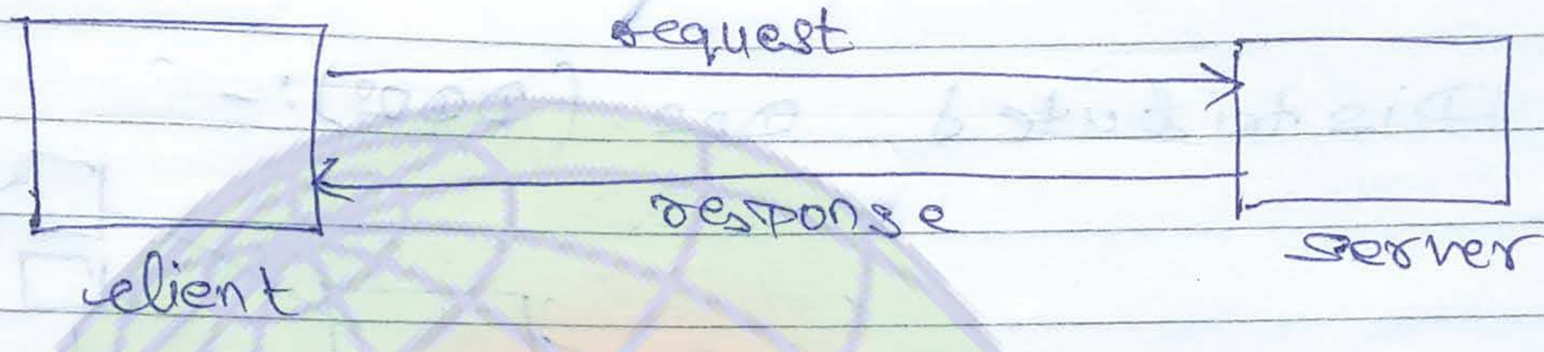
SARAA

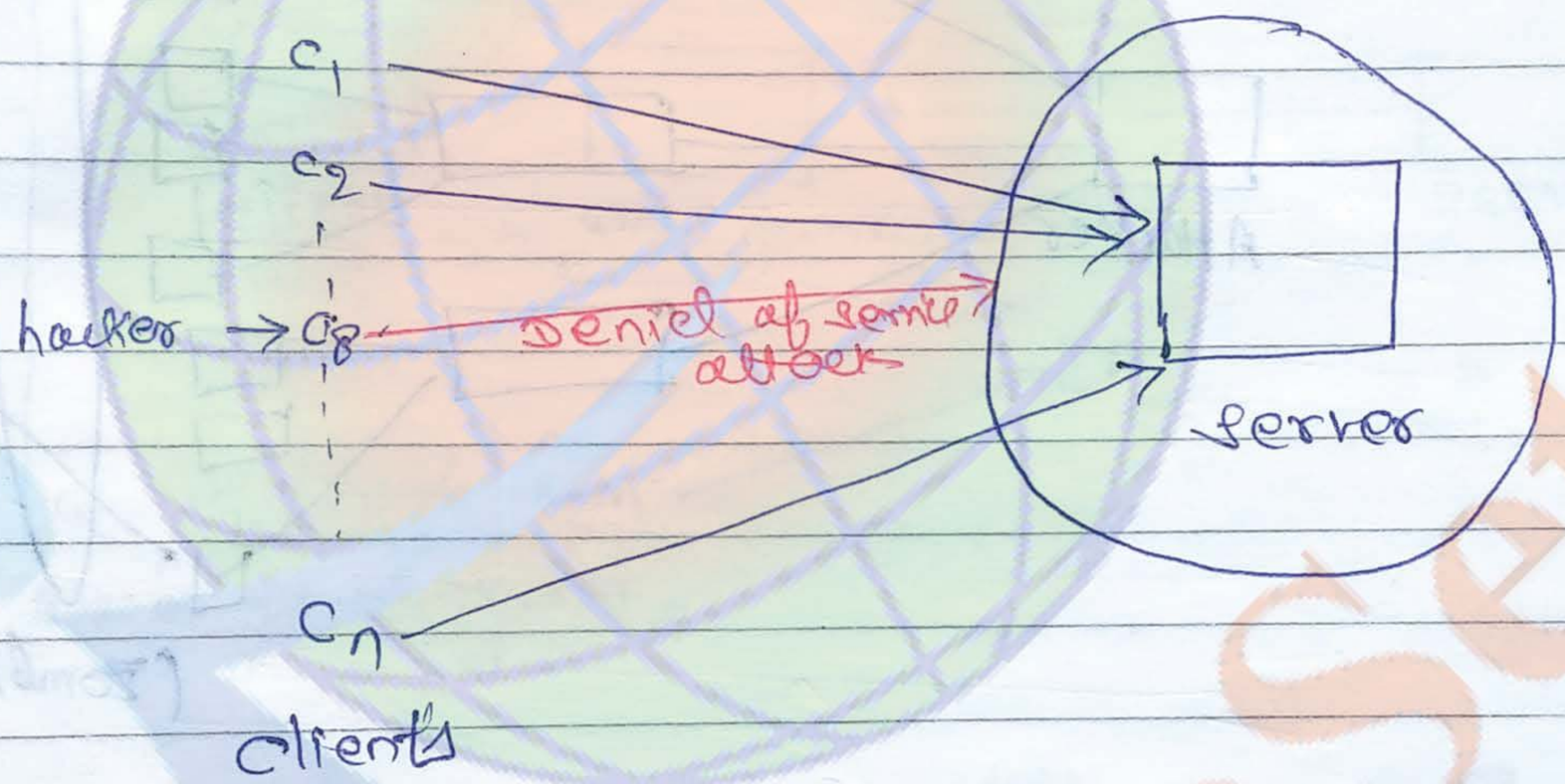
Date : / /
Page No :

* ~~shotter~~ surfing :-

☆ DOS: (Denial of service)

client-server architecture



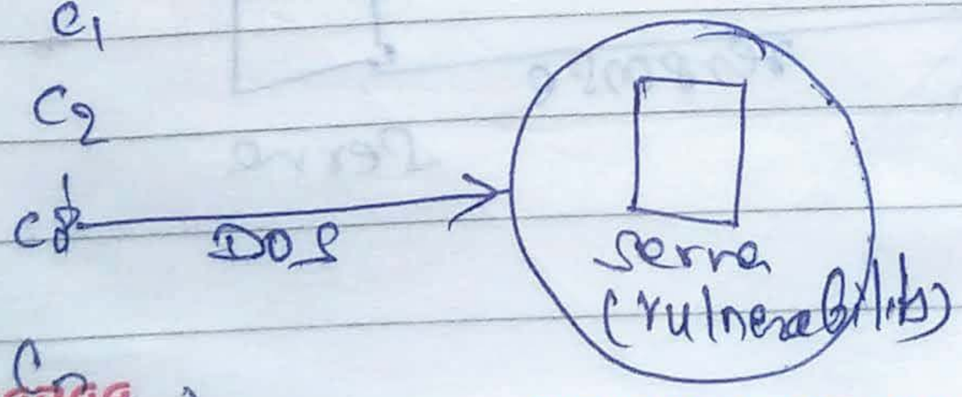


Denial of service (DOS)

Normal DOS

less attack

(single user performing DOS)

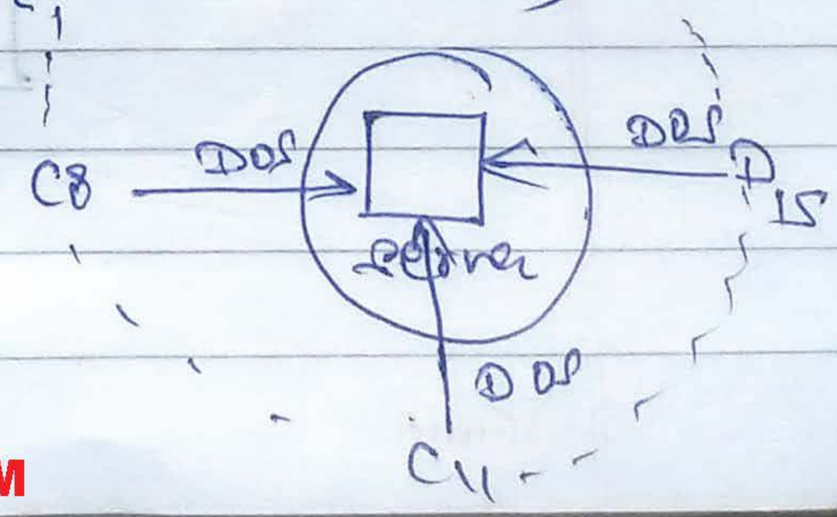


Distributed DOS

(DDOS

mostly attack

(multiple user performing DOS)

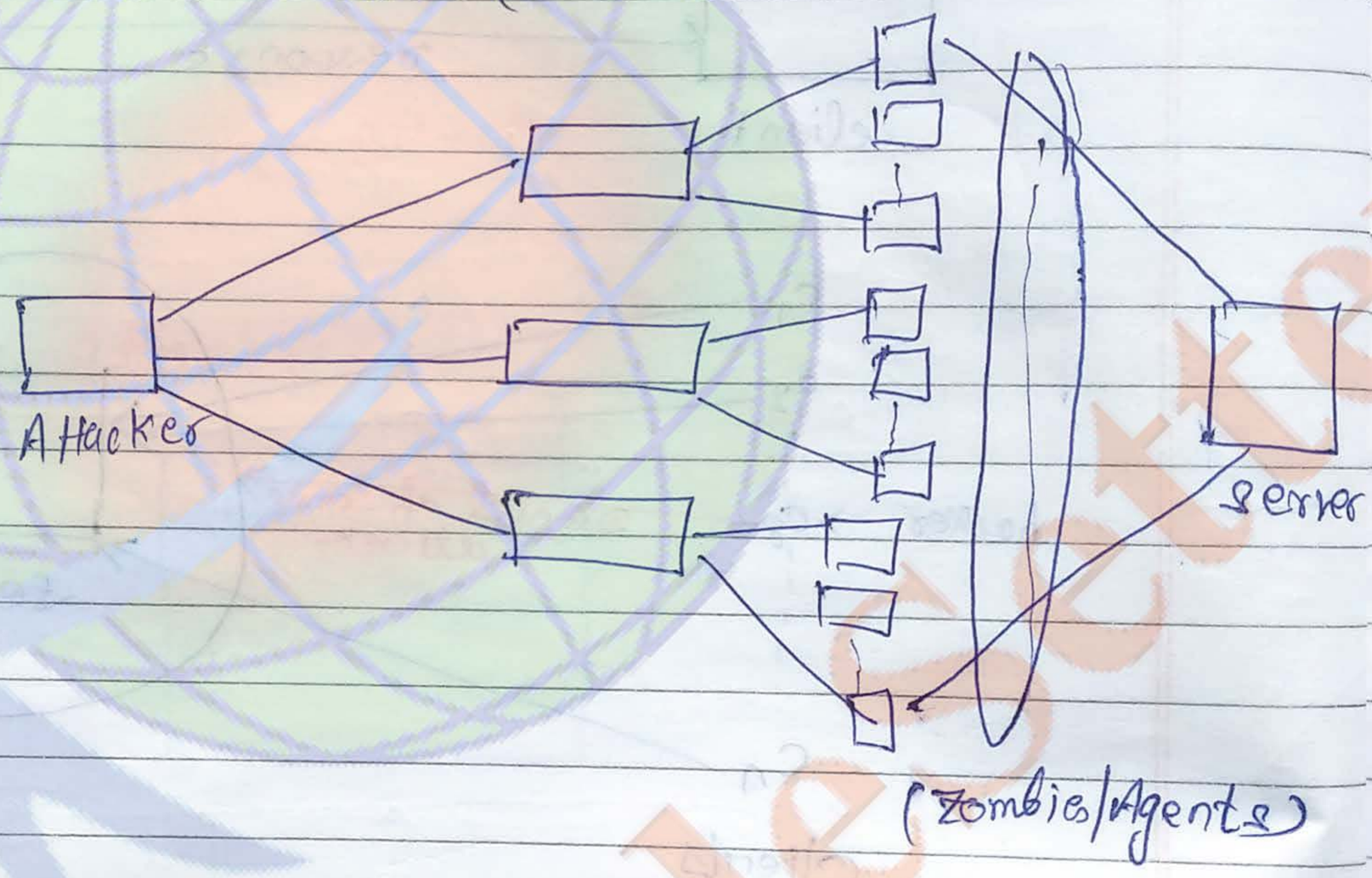


Date : / /
Page No :

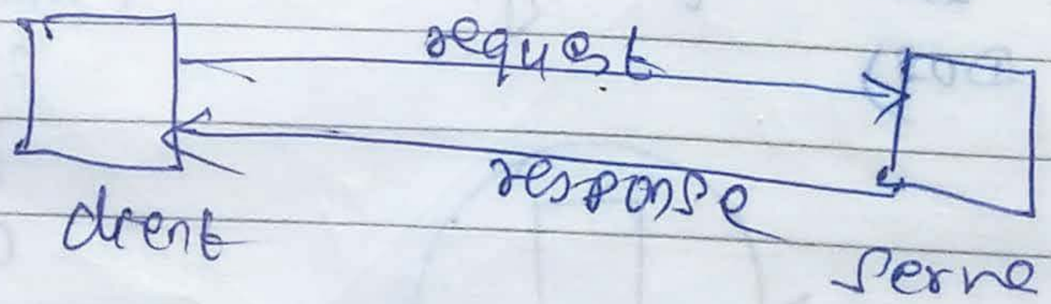
* Zero Day DoS!-

vulnerability
↓
Patch

* Distributed DoS (DDoS)!-



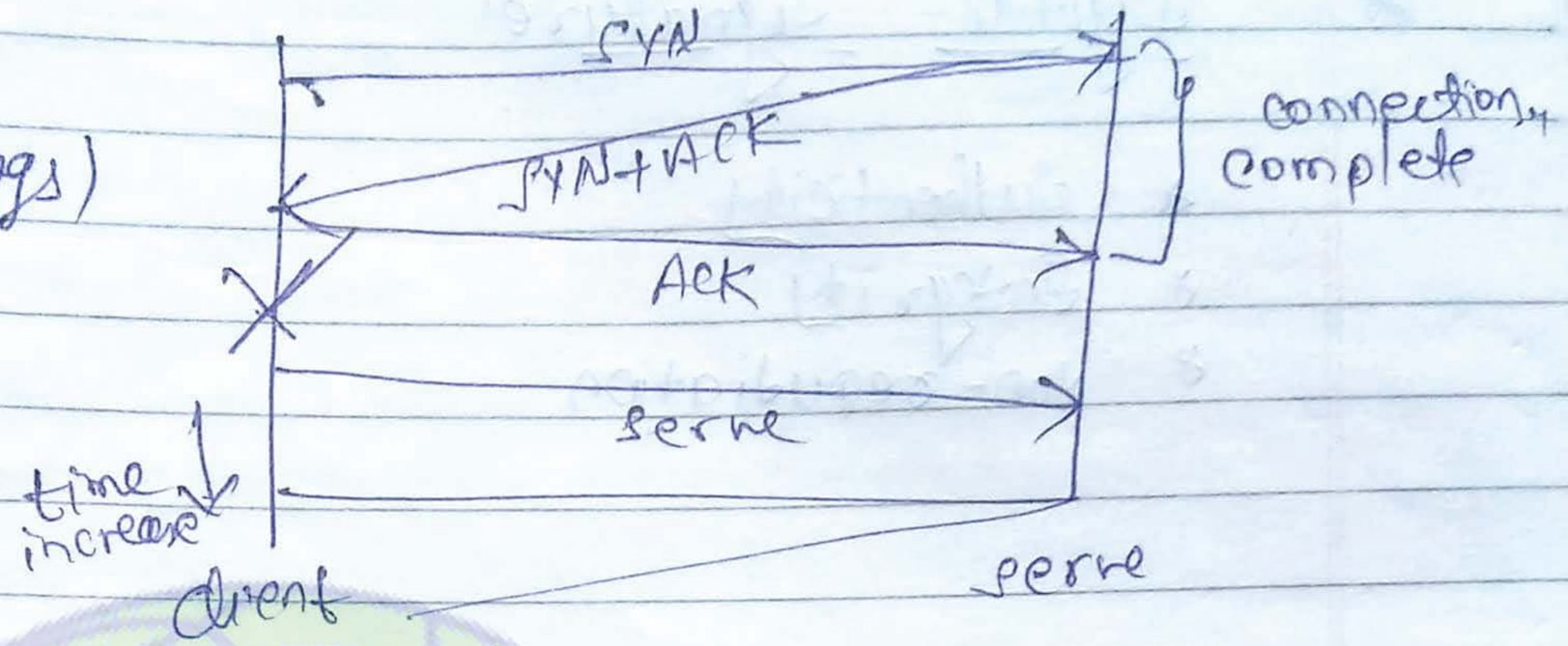
* PING www.google.co.in
TCP/IP ⇒ TCP handshake Process
VoP ↳ SYN
ICMP
S



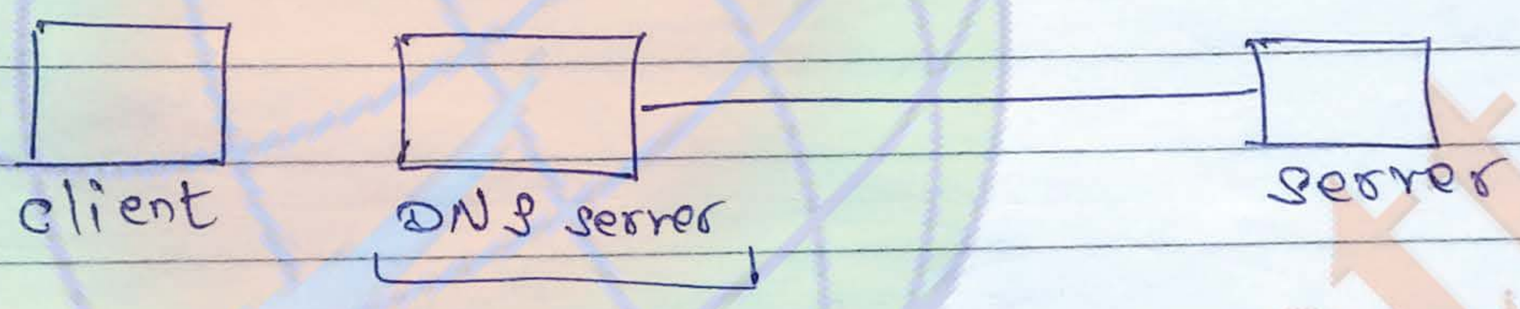
Date : / /
Page No :

* SYN

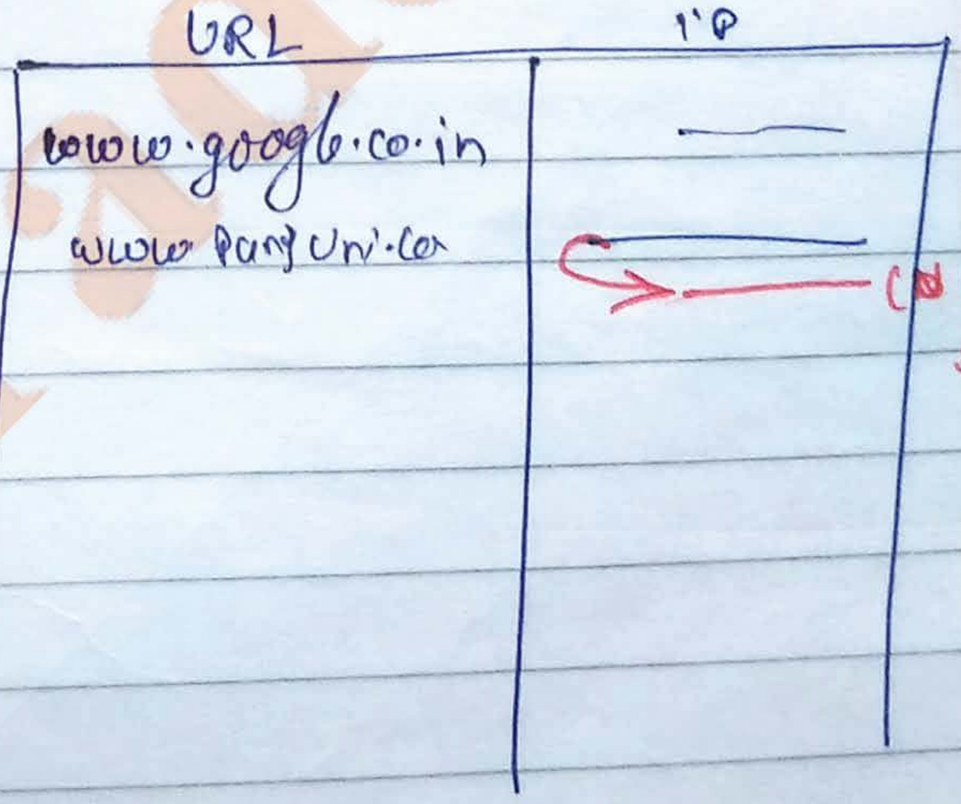
SYN (6 flags)



★ DNS :-



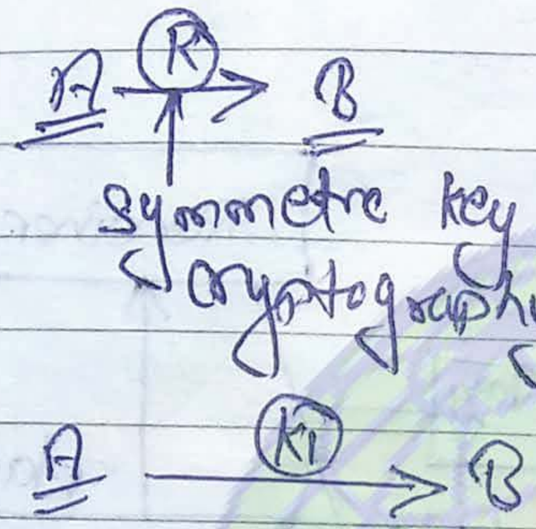
DNS spoofing :



Date : / /
Page No :

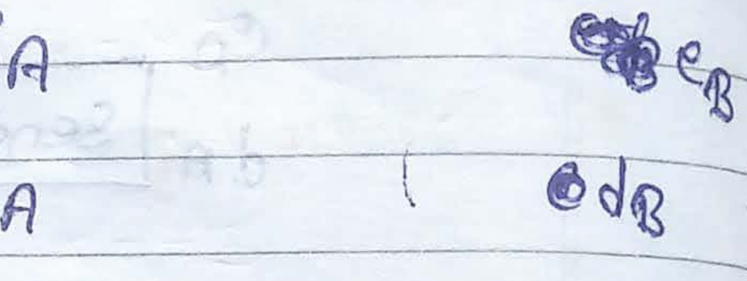
↓↓

mostly the letter (K) is used.
shared key

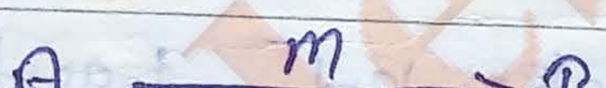


↓↓

every user has two key.
public key (e)
private key (d)



- every user announce public key to the network while keeping its private key secret
- cryptography is based upon receiver key
- encryption is performed by receivers public key and decryption is performed by receivers private key.



$C = E_{e_B}(P)$

$P = D_{d_B}(C)$

$C = e_C(P)$.

$P = d_e(C)$

SARAA

Date : / /
Page No :

★ Digital Signature:

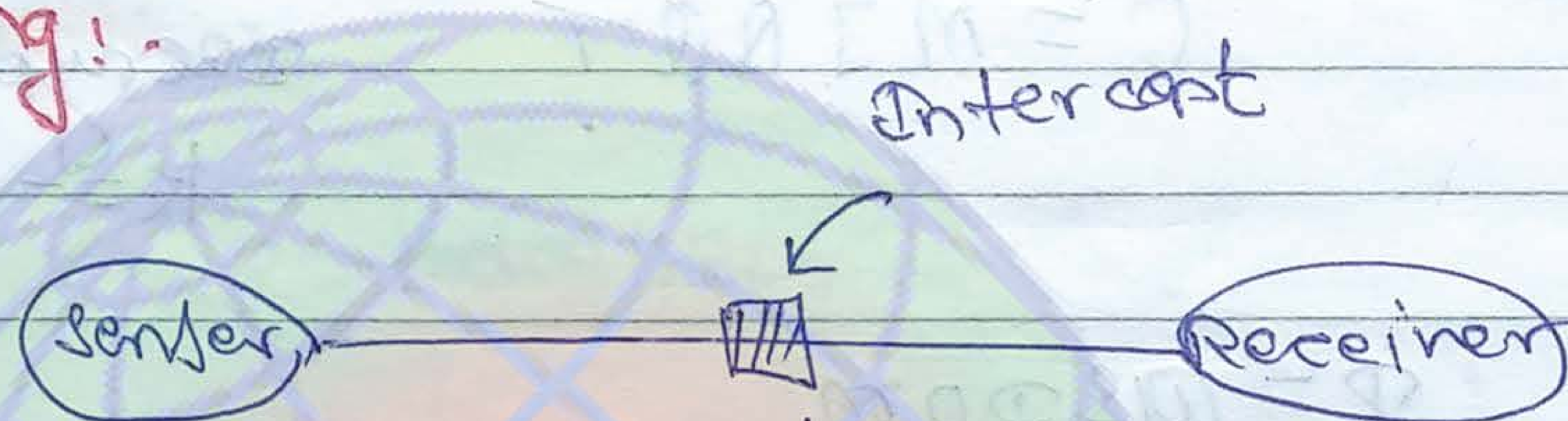
* Authenticity
* Integrity
* Non-repudiation

* Difference b/w Symmetric and Asymmetric key

Symmetric → same key is uses → faster

Asymmetric key → different key uses → slower

* Snooping:-



on b/w the sender and receiver the hacker see the message

Note:

dedicated communication have no possibilities of snooping.

* Symmetric key Ciphers: (Symmetric key algorithms)

- Traditional ciphers (characted oriented)
  - Substitution ciphers (change with another char or number) | Shift ciphers
    - D → E / D → 7
    - D ← E / 1 ← 7
    - mono alphabetic (each occurance of character has to be replaced with same character in the ciphertext)
    - Polyalphabetic ciphers (multiple occurance of same character be replaced with different characters)
  - transposition ciphers (Replace the position)
- modern ciphers (bit-oriented ciphers)
- Block ciphers
  - Data encryption standard (DES)
  - Advance encryption standard (AES)

SARAA