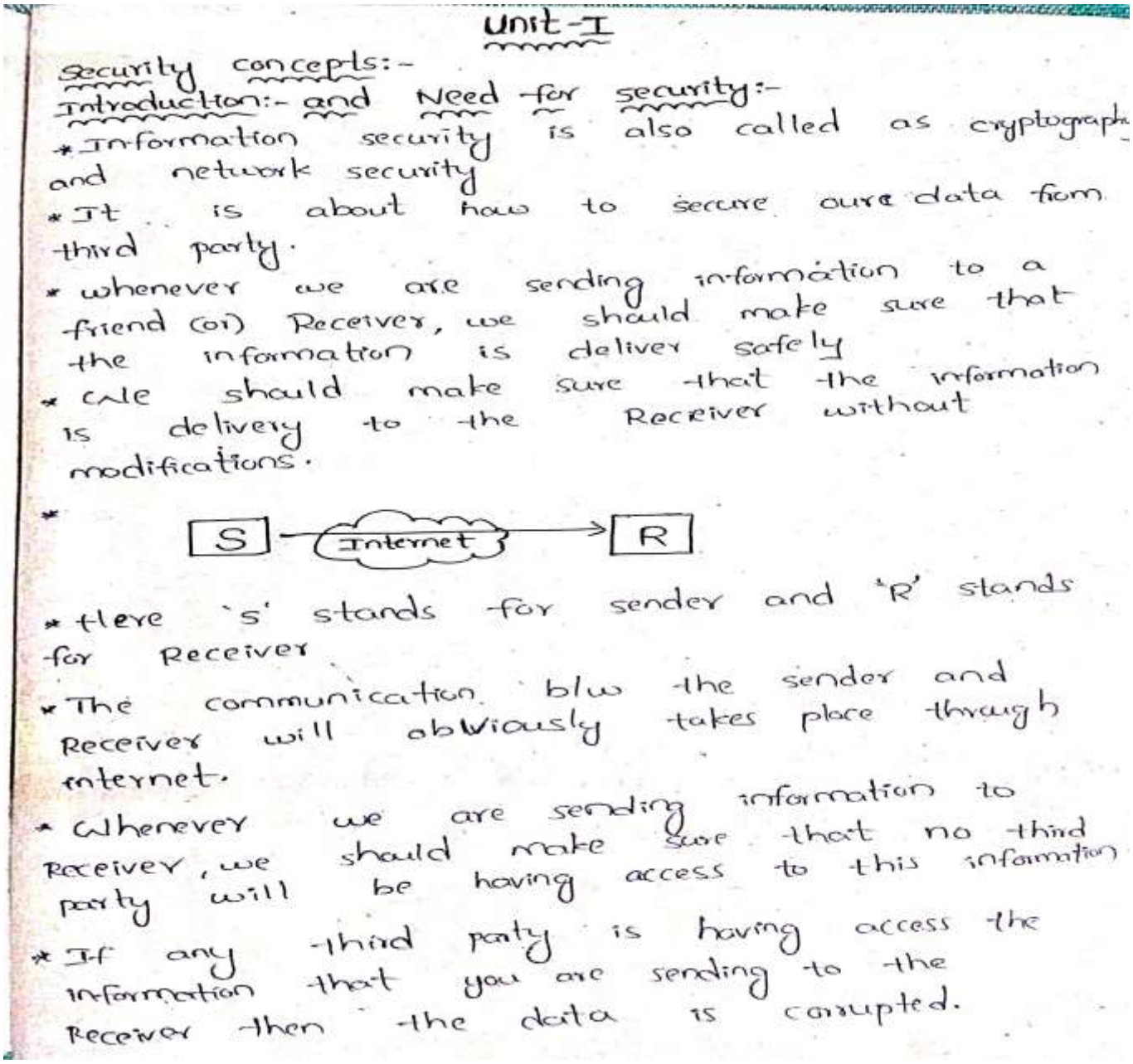
UNIT - I

Security Concepts: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security Cryptography Concepts and Techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.



Unit-I

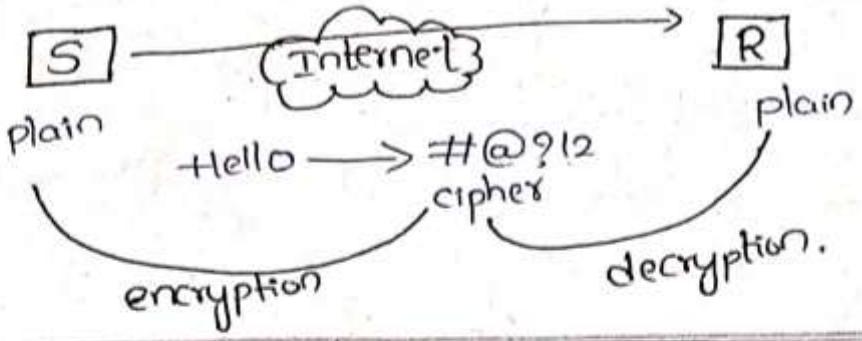
Security concepts:-

Introduction:- and Need for security:-

* Information security is also called as cryptograph and network security
* It is about how to secure our data from third party.
* whenever we are sending information to a friend (or) Receiver, we should make sure that the information is deliver safely
* We should make sure that the information is delivery to the Receiver without modifications.

* Here 's' stands for sender and 'R' stands for Receiver
* The communication blw the sender and Receiver will obviously takes place through internet.
* Whenever we are sending information to Receiver, we should make sure that no third party will be having access to this information
* If any third party is having access the information that you are sending to the Receiver then the data is corrupted.

* The corrupted data is nothing but, the data may be change (or) confidentiality of the data may be lost.
* If you don't maintain the security, there is a chance that your data may be hacked.
* For example:- If you and your friend wants to meet at 2.00pm. You send a text message to your friend that to meet at 2.00pm.
* If that data being read by third person and he modify the data, that to meet at 4:00pm.
* Instead of 2:00pm, he made it 4:00pm. and it is delivery to the Receiver at 4:00pm.
* Here miscommunication takes place and you both didn't meet.
* Whenever the sender we are sending information from sender to the Receiver, two process will takes place i.e.,
  i) encryption
  ii) decryption.
* Encryption:- It converting plain text (Hello) to cipher text (#@?12) (unreadable text).
* decryption:- It converts cipher text to plain text.



Security Approaches:-

* There are three ways that we can approach the security.
  1) prevention
  2) protection
  3) Resilience

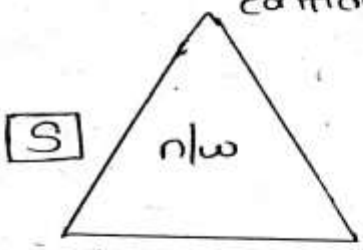
1) prevention:- It will prevent the threats by identifying the underlying causes before they occur.
* It happens before the occurance of threats.

2) protection:- It takes places, when the threats are ready to occur.

3) Resilience:- Here, the threat will already occur. (When we are not in a position to control a threat then we have to adopt a mechanism (or) method (or) write a program through which the threat can be solved.
* This is about security approaches.

4) principles of security:-

* we need security to satisfy the confidentiality integrity and availability.
* It is also called as CIA Triad (three things).
* whenever we are sending information from sender to Receiver, we have to maintain this CIA Traid. for a proper and reliable communication
*

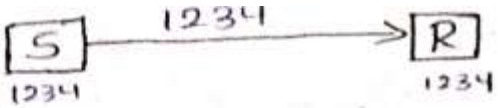


Confidentiality:-

* confidentiality is nothing but confidential data (or) confidential message. should be kept in secret
* ~~The data~~ whenever we are sending information from sender to Receiver, should be known only to the sender and Receiver not to any other third party

Integrity:-

Integrity is nothing but whatever the data we are sending from sender to Receiver, it should send to the Receiver without any modifications.
It take place
* The data should be send from sender side to Receiver-side without any modifications

ex:- 

(without any modifications)

Availability:-

* Availability is nothing but whatever the data we are sending from sender to the receiver, it should be avaliable in all forms.
* The Receiver should be able to read the data and write the data, execute the data, modify the data.
* Receiver should be able to do each & every function.
* These are known as pricriples of security (or) goals of security. (or) maintaining the security to acheive CIA Triad.

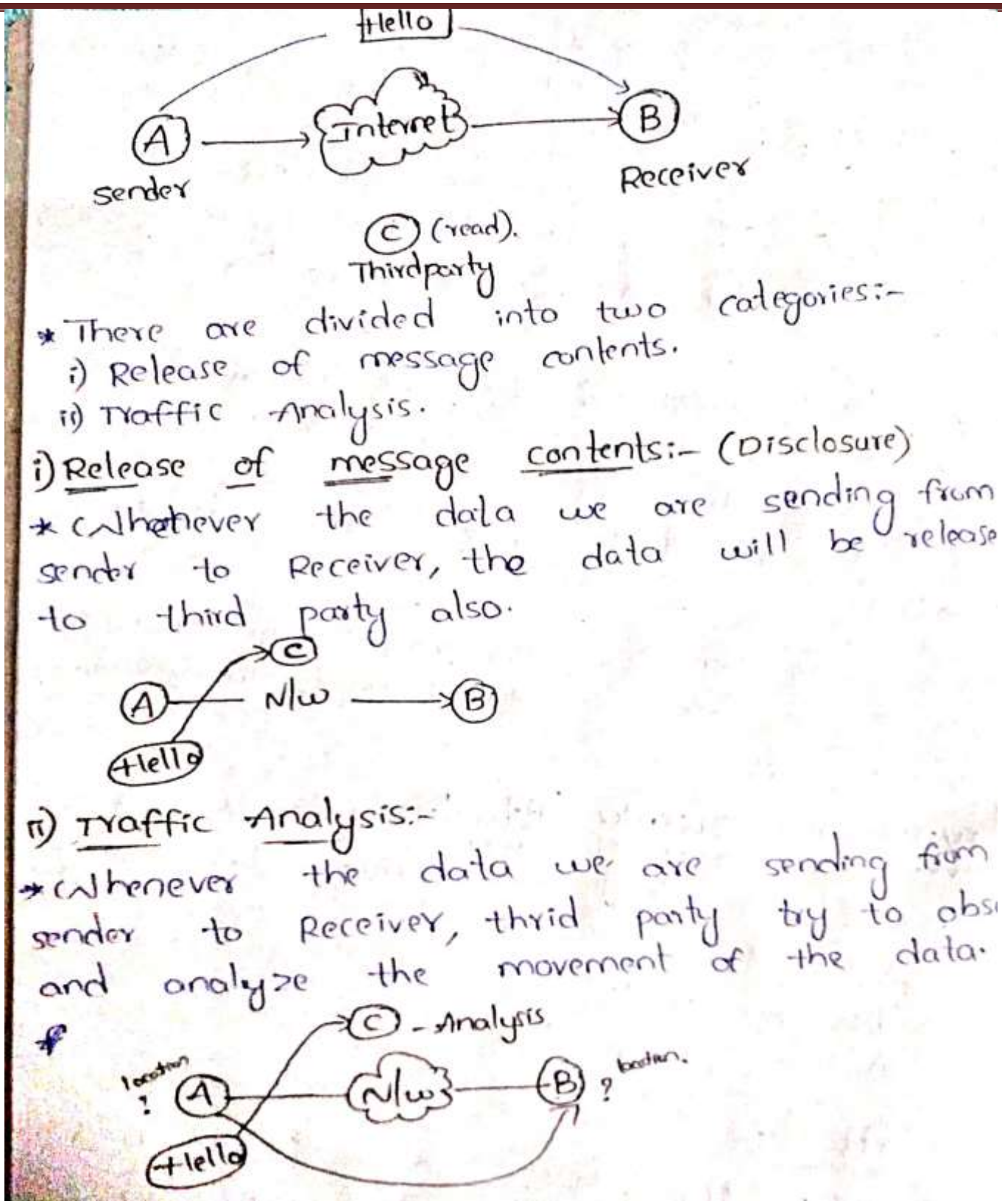
5) Types of security Attacks:- (Possible ways of Attac

* Any action that compromises the security of information.

Types :- i) passive atlack (read)
ii) Active attack. (read, write, modify etc)

Passive attack:-

Whenever the data sending from the sender to Receiver, the third party can only read the data and observe the data. without any modifications.



* There are divided into two categories:-
  i) Release of message contents.
  ii) Traffic Analysis.

i) Release of message contents:- (Disclosure)

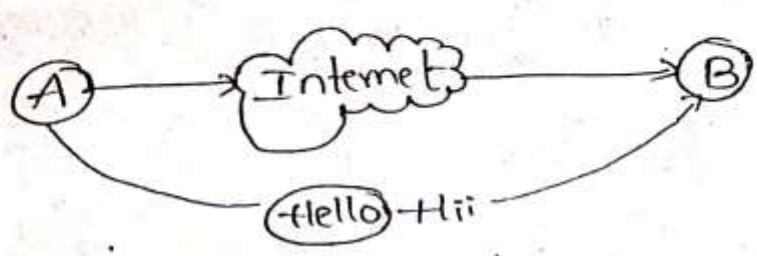
* Whenever the data we are sending from sender to Receiver, the data will be release to third party also.

ii) Traffic Analysis:-

* Whenever the data we are sending from sender to Receiver, thrid party try to obs and analyze the movement of the data.

Active Attack:-

* Whenever the data, we are sending from sender to Receiver, the third party can read, write, modify the data.



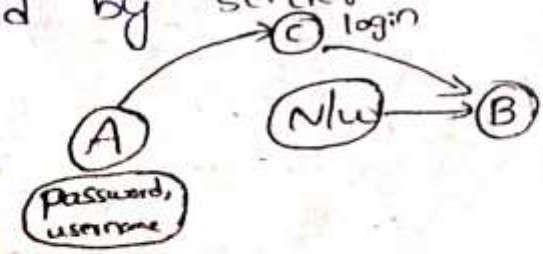
It can be divided into three categories:-

i) Masquerade
ii) Relay
iii) Denial of service

i) Masquerade:-

Whenever the data, we are sending from sender to receiver, the third party will stolen the data and it modify the data and sends to the Receiver.

* But Receiver thought that, the data is send by sender.



ii) Relay:-

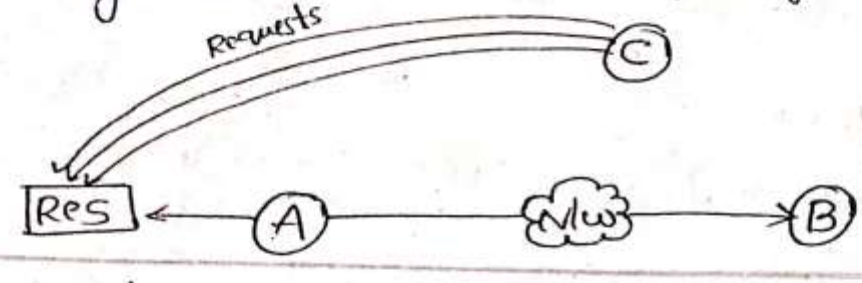
Whenever the data, we are sending from sender to Receiver, through network the third party can read, write, modify the data.

(Same as active attack).

iii) Denial of service:-

whenever sender wanted to access some Resource, third party wantedly send multiple Requests to the Resource.

* In that case, Running capacity of Resource will be slow down.
* Then sender has to wait and suffer.
* Finally sender will be getting loss.



6] Security Services:-

The services provided by security are:-

1) Authentication (user, password) (phone, otp) → server
2) Authorization (access control)
3) Non-Repudiation 

4) Auditing. - Analyse

1) Authentication:-

* Getting an official permission to get into the website. and get into the server to access it.
* There are many ways to check the authetication by checking whether (they are ~~matching~~ with ~~their~~ data) the username and password which you are ~~using~~ giving as an input is correct (or) not.
* If the data is matched then you will be authenticated to use to the services.

2) Authorization:-

* After you are allowed to the enter into the website, upto what extent you can use this services of the server.
* It is also called as access control.
* It has some limitations that upto what extent you can use this services of the server.

3) Non Repudiation:-

* once the message is transmitted from sender to Receiver
* Sender can't say that "No, i didn't send the message" as well as Receiver also
* This is also called as Non Repudiation.

Ex:- Money Transactions.

4) Auditing:-

* It will analyse the data, it will have entire information about the data
* If ony unauthorization permissions happens then the Auditing will track the hacker.

7) Security Mechanisms:-

To ensure the security we have some mechanism

i) Encipherment
ii) Digital signature
iii) Access control
iv) Authentication Exchange
v) Traffic padding
vi) Routing control.

i) Encipherment:- (hide).

* The data will be hidden by cipher
* The sender will convert the data into a unreadable format means sender hides the data
* When the Receiver, Receives the data which is in unreadable that is converted into readable format.

ii) Digital signature:-

* Some special identity which is used for authentication.
* It is like a thumbnail and stamp
* It is also used for to integrity of data.

iii) Access control:-

* Restricting the permissions to several levels.
* In any organization, upto what extent of permissions can be given to a particular person.

Ex:- college management.

iv) Authentication exchange:-

* Declaring the user as an authenticated user by comparing the username and password with the data that we are having in database.

Ex:- login instagram.

v) Traffic padding:-

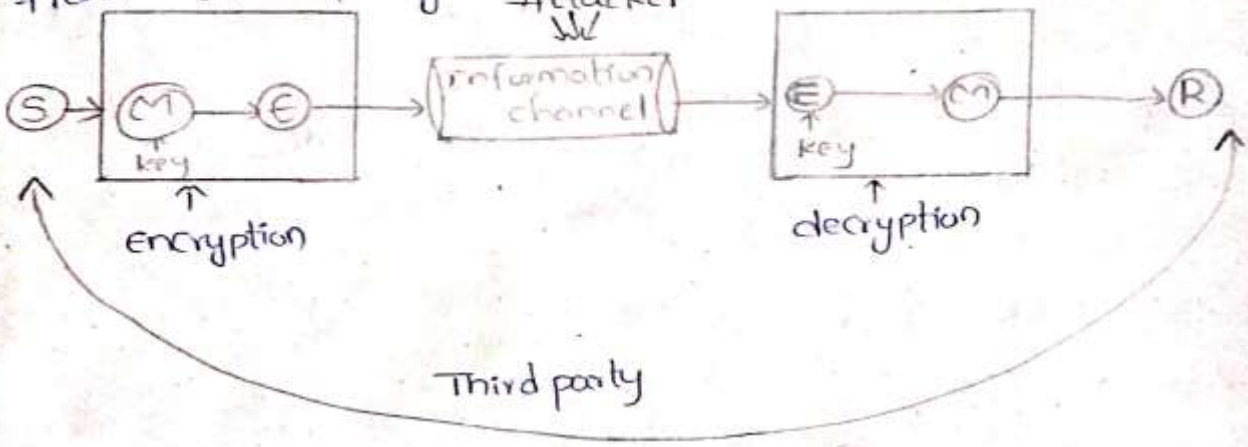
* We have to add extra bits in the beginning (or) in the middle (or) in the ending in order to confuse the observer. (or) hacker.

vi) Routing control:-

* We have 'n' number of paths, we can go with any path, that is our wish.
* We can go with a mixture of path in order to confuse the hacker

8) Model for Network security:-

* This is about, whereever the data is sending from sender to Receiver without any attacks from third party.



* The sender will generate a message, that message will be converted into a encrypted message. by using a key, this process is called encryption.
* After encryption, the encrypted message will be passed into information channel.
* The Information channel acts the medium for both sender and receiver.

* Through this medium only the sender and Receiver will sharing the data
* In this area, there are many attackers ~~are~~ to hack the data. So, we should be careful in that area.
* After crossing the information channel, the encrypted message will come out of the informatic channel.
* The encrypted message is converted into original message by using a key, this process is called as decryption
* The converted message will be read by Receiver
* The tile have a trusted third party which provides a key for encryption and decryption ~~party~~ process.
* This is about network security model.

Part-B

Plain text and cipher text:-

plain text:-

* It refers to anything which humans can understand.
* This is may be as simple as English sentences (Hello), a script (or) Java code.
* If you can make sense of what is writt then it is in plain text.

cipher text:-

* cipher text (or) encrypted text, is a series of randomized letter (hanklmn) and numbers which humans cannot make any sense.
* An encryption algorithm takes in a plaintext message, runs the algorithm on the plaintext and produces a ciphertext.
* The ciphertext can be reversed through the process of decryption, to produce the original plaintext.

Ex:-

* we will encrypt a sentence using caesar cipher
* plaintext : This is srija
* ciphertext : Aopz pz wshpuale.

2) Substitution Techniques and Transposition Techniques [classical encryption Techniques]

Substitution Techniques:-

* Replacing the plain text alphabets (or) digits (or) symbols with some other alphabets (or) digits.
* This is also called as Replacement.

Ex:- FREE → XYZA

* There are six techniques
  i) caesar cipher
  ii) monoalphabetic
  iii) playfair cipher
  iv) Hill cipher
  v) one time pad
  vi) polyalphabetic

ii) ~~Monoalphabetic cipher~~

i) Caesar cipher :-

* converting the plain text into cipher text by using formula.

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

* converting the cipher text into plain text by using formula

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

* 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
PT→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.
CT→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

Ex:- TROUBLE FREE [PT→CT]
wurxeoh ruhh

Ex:- wurxeoh ruhh [CT→PT]
TROUBLE FREE

ii) Monoalphabetic cipher:-

* Monoalphabetic means only one alphabet
* It has one-one relationship.
* there single ciphertext for each plaintext

Ex:- ALWAYS [Pt→ct]
VxAVk

Note:- We have to use only one alphabet for the same alphabet in plain text.

* The disadvantage is; the hacker can easily decode it.

vi) polyalphabetic cipher:-

* polyalphabetic means many alphabets.
* It has many-one relationship.
* Here many ciphertext for a plaintext.

ex:- ALWAYS
KOYTTP

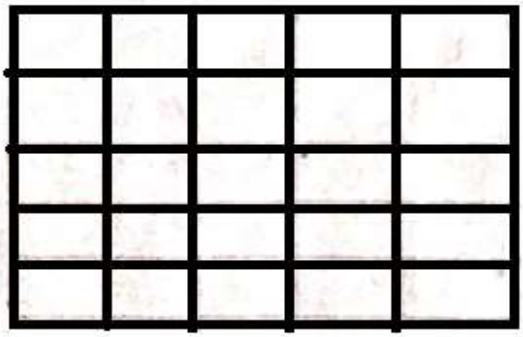
* Cale can use many other alphabels for the same alphabet in plaintext.

iii) playfair cipher:-

*It is also called as multiple letter encryption cipher
* Here we have the plain text of msg & keyword we have to convert it to cipher text
* Cale have some steps:-
  1) construct 5x5 matrix - 25 cells
  2) Fill the matrix
  3) Divide the msg -> 2 letter pairs
  4) Apply rules & encrypt
  (3)

Ex:- plain text = instruments ; key = monarchy

step 1:-



* We have to do mod 26 for simple calculation

$$K^{-1} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

Now, we will decrypt, cipher = FK MF I O

$$C = \begin{bmatrix} F \\ K \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}$$

* plain text :- $P = K^{-1}C \bmod 26$, $P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \bmod 26$

$$P = \begin{bmatrix} 260 \\ 305 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

similarly, $C = \begin{bmatrix} M \\ F \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$

so, corresponding plain text is;

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 149 \\ 396 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$$

Again, $C = \begin{bmatrix} I \\ O \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 366 \\ 452 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

Finally, the plain text is ATTACK.

---

v) one-time pad :- / verman cipher

* The condition is here;

The length of key should be equal to the length of plain text

* key length = length of PT.

Ex:- PT = security, key = ACMTKYIV

PT → security → 18 4 2 20 17 8 19 24

key → Acmtkyiv → 0 2 12 19 10 24 8 21

18	6	14	39	27	32	27	45	add
			-26	-26	-26	-26	-26	
18	6	14	13	1	6	1	19	sub
S	G	O	N	B	G	B	T	

* SGIONBGIB is cipher text for security
* This is encryption.
* For decryption, do the same process in reverse.

Transposition Techniques:-

* This is also called as Rearrangement.
* Rearrange the plain text alphabets (or) digits (or) symbols with the same plain text alphabet (or) digits (or) symbols which are given.
* We shouldn't add any other alphabets.
* Ex:- FREE → EREF
  REEF
  FEER etc...

* There are four techniques
  i) RailFence Transposition ii) columnar Transposition
  iii) Improved Transposition iv) Book cipher

i) RailFence Transposition:-

* We can Rearrange the plain text into cipher text by using the depth which is equal is 2.

Ex:- TROUBLE FREE

T	O	B	E	R	E
R	U	L	F	E	E

CT → TOBERERULFE PT → diagonal, CT → Row.

* It is useful for short messages.
* It is not so efficient.

ii) Columnar Transposition:-

* We have to arrange the plain text into a matrix.
* It is not a mandatory to take a square matrix only.
* We can take any matrix like Rectangle, square etc...
* Fill the matrix with the plain text in a row wise.
* Eg:- Information security → plain text

I	N	F	O	R
M	A	T	I	O
N	S	E	C	U
R	I	T	Y	

* Generate the key, which is in the form of number & which is less than (or) equal to the no. of columns we took.
* Then write the corresponding cipher text column wise

Key = 32514.

* We have to select the key randomly

1	2	3	4	5
I	n	f	o	r
m	a	t	i	o
n	s	e	c	u
r	i	t	y	

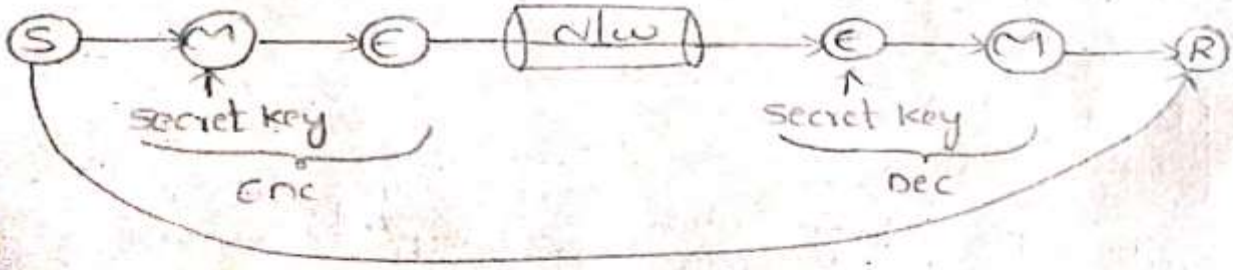
Key = 32514

-ftetn asirouimnroicy ⟶ information security.

4) Symmetric and Asymmetric key cryptograph

Symmetric key cryptography:-

* We have only one key on sender side and Receiver side.
* We are using only one key for encryption and decryption process.

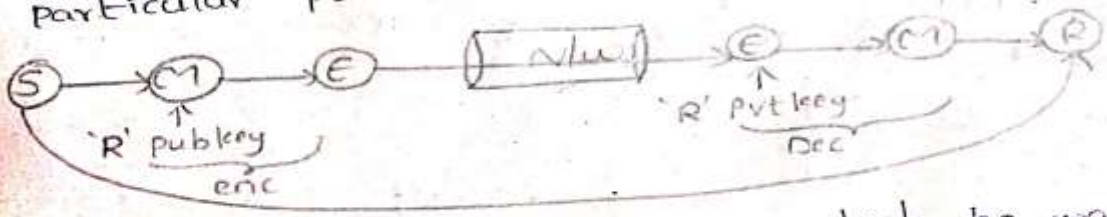


* Sender wants to send a message to Receiver
* Sender generates the message after that, the message has to be encrypted with the help of secret key. This process is known as encryption.
* The encrypted message will be enter into the network
* After that the encrypted message will come out of the network.

* Then, encrypted message is converted into original message with the help of some secret key which is used at the encryption process.
* This process is known as decryption.
* The orginal message is read by the receiver.
* The disadvantage is; it can easily implement because we have only one secret key.
* It is not so efficient.
* It is not at all secure.

Asymmetric key cryptography :-

* We have different keys on senderside and receiver side.
* We have two types of keys:-
  1) public key
  2) private key.
* public key is a key which is known to everyone.
* private key is a key which is known to a particular person

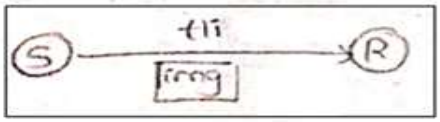


* (Sender generates the message, which he wants to send to a Receiver)
* Sender wants to send a message to receiver.
* sender generates the message after that, the message has to be encrypted with the help of Receiver's public key. This process is

known as encryption.
* The encrypted message will be enter into the network.
* The encrypted message will come out from the network.
* Then, encrypted message will be converted into original message with the help of Receiver's private key.
* This process is known as decryption.
* The original message will be read by Receiver.
* In this, we have more security when compa to symmetric key cryptography.

5] Steganography:—

* Hiding information with in another message.
* Embedding the msg with in an image, (or) video (or) pdf.
* After transferring the msg from sender to Receiver, later msg is extracted from embedded devices by Receiver.



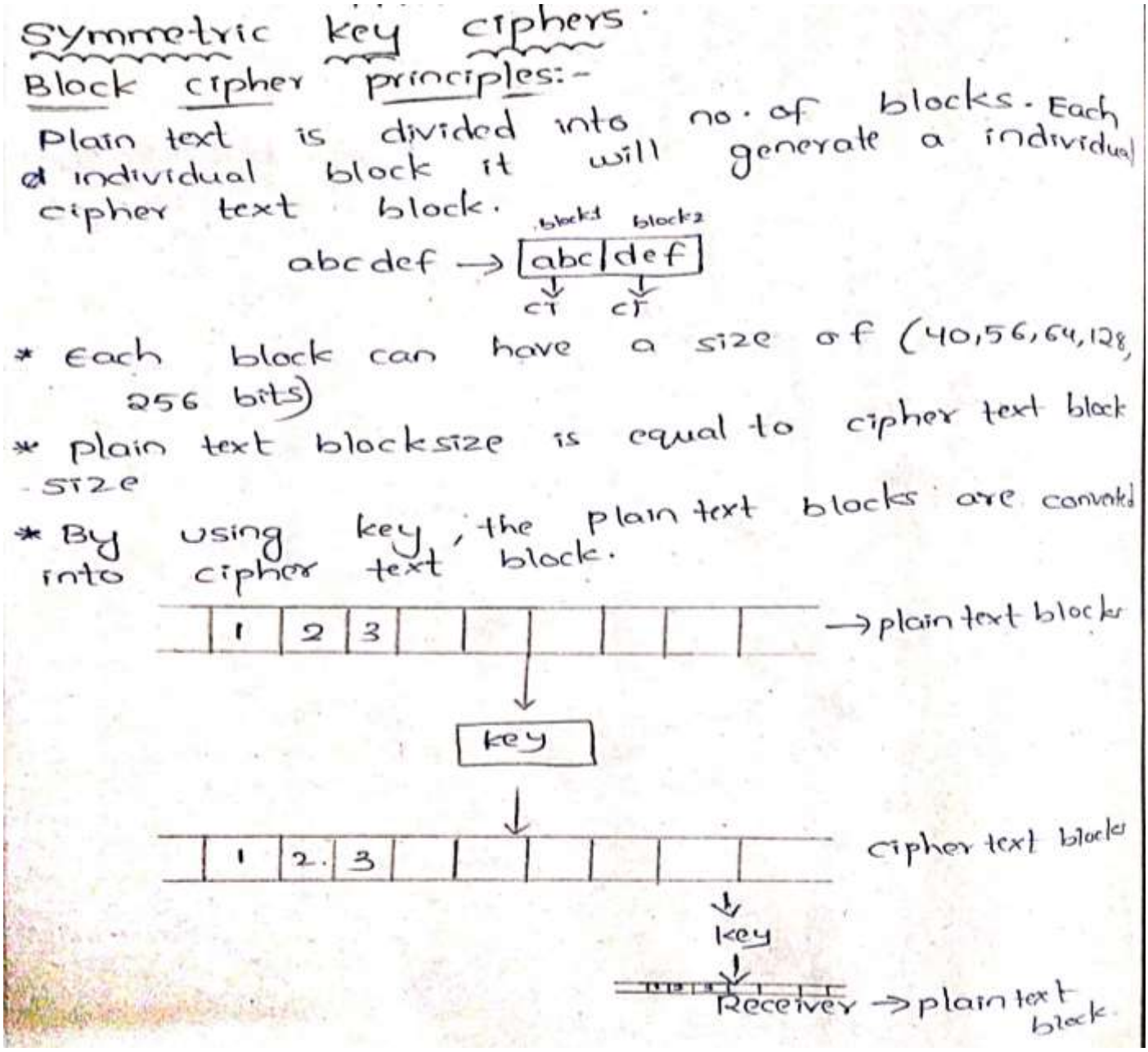
* We have several steganography techniques:-
  1) Least significant bit (LSB)
  2) Audio / video steganography
  3) character marking etc...

* We have some attacks in steganography. like the hacker will observe the data and modifys the data.

6] Key size and key range

UNIT - II

Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4. **Asymmetric key Ciphers**: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm.



Block cipher principles:-

The design principles of Block cipher

1) Number of Rounds
2) Design of function
3) key schedule Algorithm

1) Number of Rounds:-

* Depending (or) Based on the Algorithm, Each and every algorithm will have several rounds.
* Based on the more no. of rounds, that much harder it became to the hacker.
* 10R Algorithm is easy to hack when compare to 20R Algorithm.
* so, No. of Rounds should be more.

2) Design of function F:-

* You should design a function F which will be very much complicated to understand.
* If the function is very much complicated to understand, that much more time hacker will take to decode the data.
* you have to take Non-linear functions, because linear functions are easy.

3) key schedule Algorithm:-

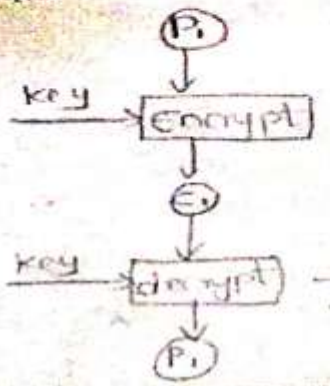
* we should be very careful when we are generating a key, because key is very important.
* Even though a minor change in key, there will be lot of changes in cipher text.

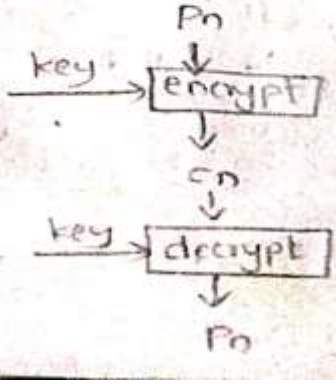
*The modes of operation of Block cipher

1) ECB – Electronic code book
2) CBC – cipher block chaining
3) CFB – cipher feed back
4) OFB – output feed back
5) CTR – counter.

1) Electronic code book (ECB)

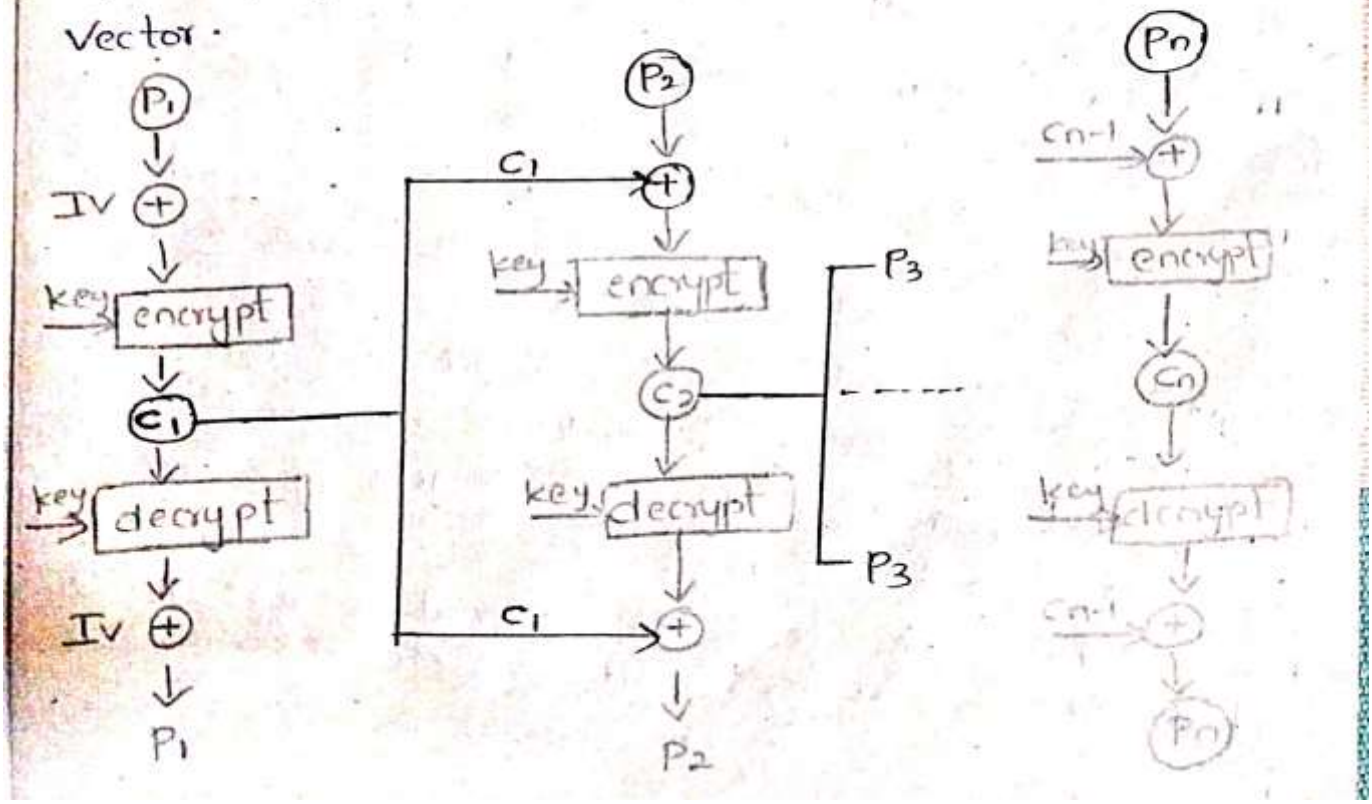
* The plain text is divided into no. of blocks, and encrypt the plain text with the help of the key and we get cipher text. and again by using the key, you can decrypt the cipher text into plain text
* The process will continue upto P_n (plain text n)
* The properties are:-
  i) Block size is equal to 64 bits.
  ii) key is same in everywhere.
  iii) The size of PT and CT should be same
* P is divided into $P_1, P_2, P_3 \ldots P_n$ at the last you will combine the $P_1, P_2, P_3 \ldots P_n$ to get the orginal P.
* This is suitable for only short messages.





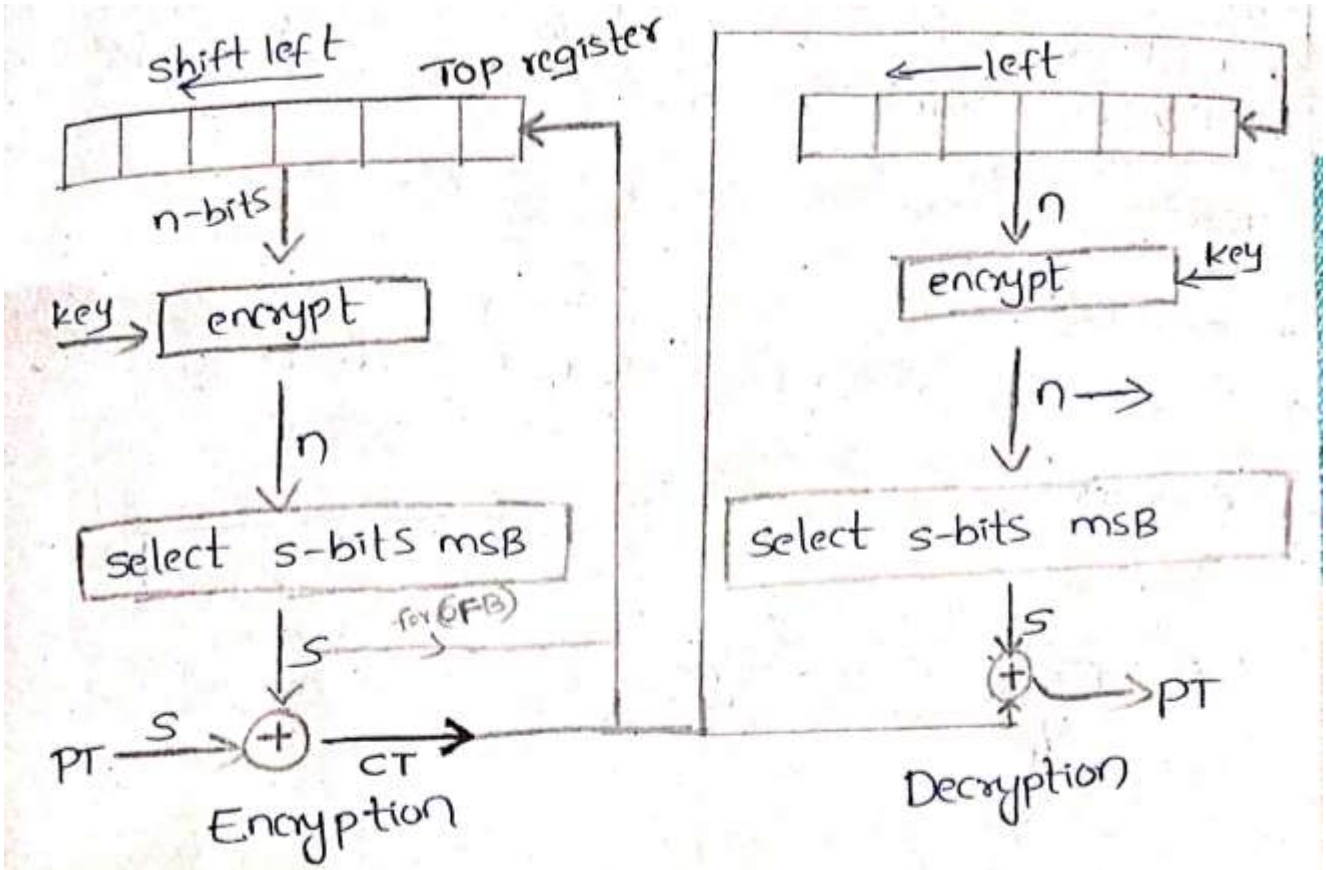
2) cipher block chaining (CBC):-

* The output of the XOR operation blw the plain text and initialization vector, is enters as a input.
* With the help of key and input, the encryption process happens.
* After encryption, the cipher text will get.
* you will decrypt the ~~key~~ ciphertext with the help of key, again that will be XOR with the initialization vector then we get the plain text.
* For the next step, we are using previous cipher text as a initialization vector.
* This process will continue, upto Pn.
* For Pn, the Cn-1 will act as a initialization Vector.



3) cipher feedback (CFB) :- (or) TOP

* In this we have shift Register, the size of the shift (or) TOP register is n bits.
* The size of plaint text is s bits.
* we will encrypt the n bits of TOP register with the help of key then we will get the n bits of cipher text.
* Actually the size of plain text is s bits, so, from that s bits you have to select MSB (most significant bits)
* From the n bits of cipher text, you have to select s-bits as (MSB)
* The s value should be $1<s<n$
* Those s bits are XOR with the plain text then you will get final cipher text.
* The final cipher text will be given to TOP register as a feedback.
* The top register will shifting towards the left side. because in order to accomidate the cipher text inside it.
* Again you will have n bits, n bits will encrypted by using key. Then you will get cipher text, in that cipher text you have to select S-bits as msB.
* The s bits do the XOR operation with the cipher text to get the plain text.



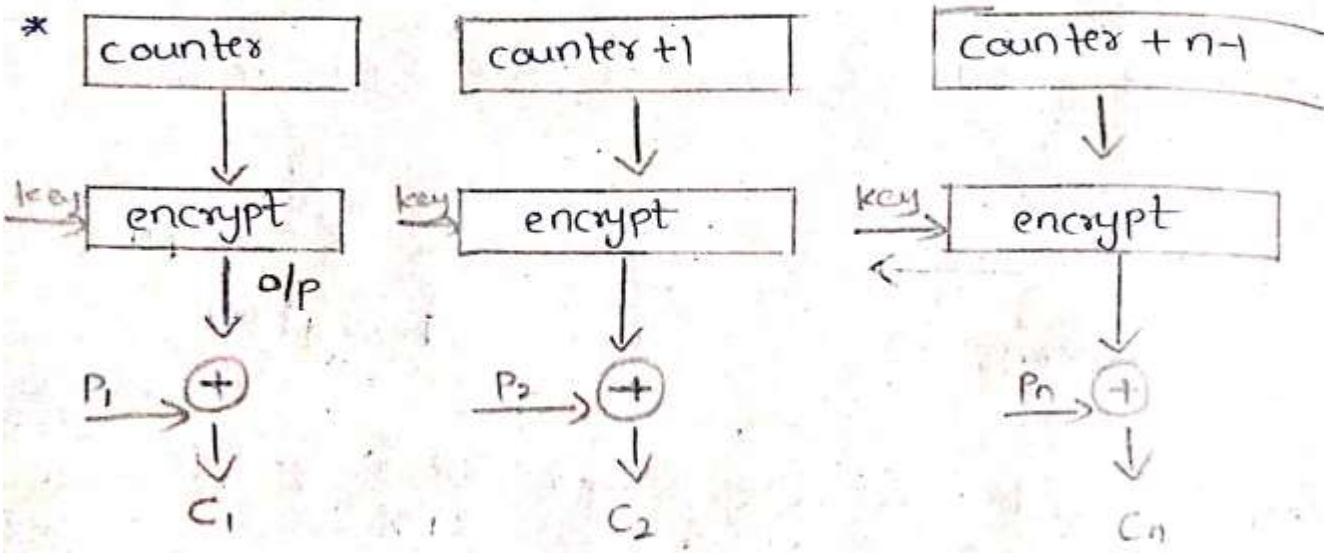
* Both sides, we use encrypt function only
* Top register is filled with IV.

4) output feedback mode : (OFB)

* Same as cipher feed back mode.
* But instead of cipher text, output is given as feed back.

5) counter mode (CTR):-

* Instead of taking plain text directly, we ~~take a~~ are giving it, in the form of counter.
* Taking a counter and giving plain text in the form of counter.
* Counter size is equal to plain text size.
* It is similar to Electonic code book.

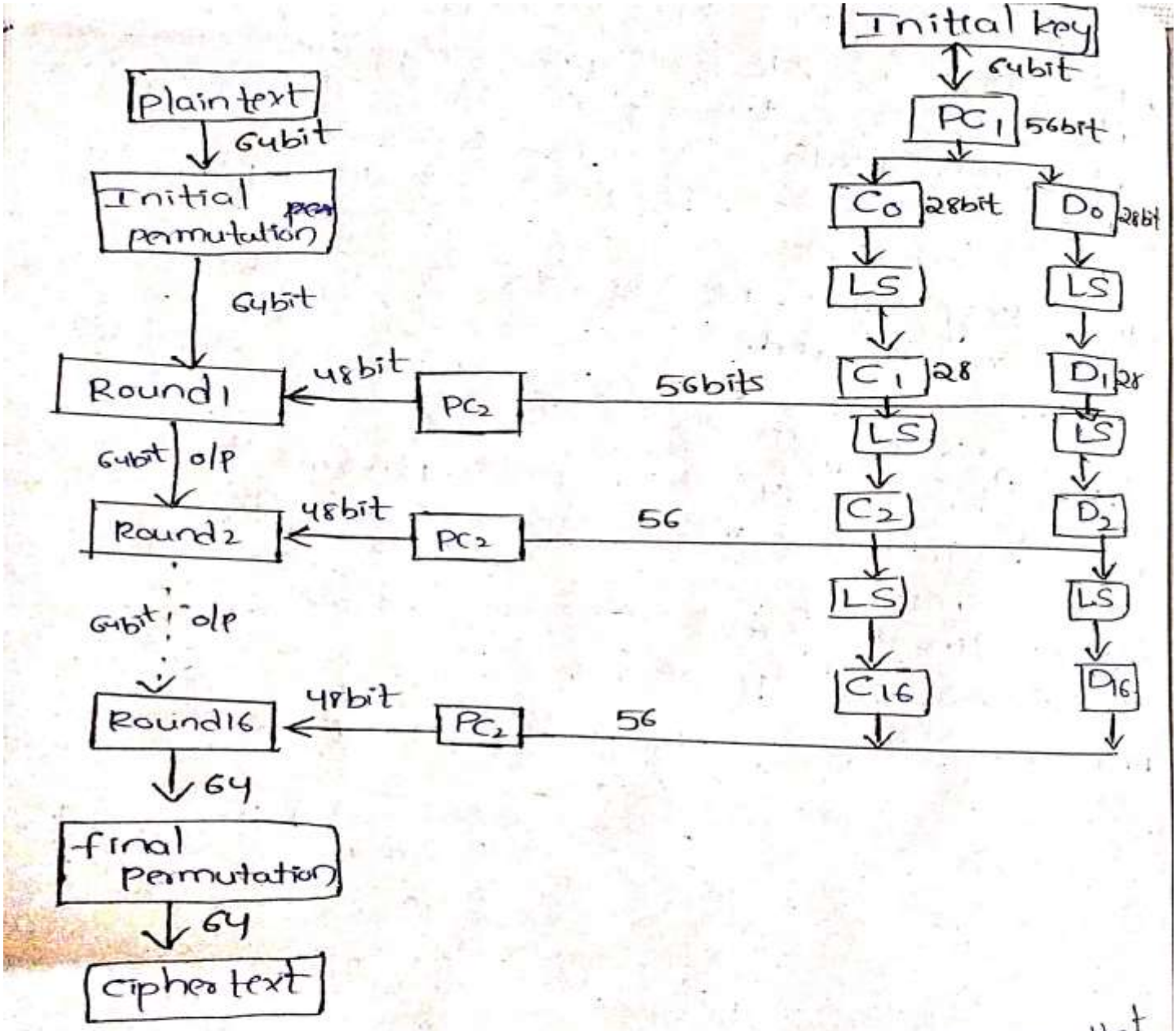


* The counter will encrypted with the help of key, and the XOR operation will done blw the o/p and plain text (P_i) then you will get the cipher text (C_i). Do Reverse proress to get plain text.
* For each next step, the counter will be added on increment with 1
* For nth step, the counter is counter +n-1
* This proress will continue..

2) Data Encryption Standard (DES):-

* It is a block cipher algorithm.
* It converts the plain text into cipher text.
* It has total of 16 Rounds.
* The text size of plain text and cipher text is 64 bits.
* The key size is 48 bits. The remaining 16 bits are removed.
* 8 bits are removed for parity and 8 bits for rearrangement.
* In each round, (4) steps are performed.
  i) Dividing bits into two parts - 32 bits for each
  ii) Bit shuffling
  iii) Non linear substitutions
  iv) Exclusive OR operations.

process:- ~~Initial~~ key



*In PC1, initially, 64 bits are there. In that 8 parity bits are to be removed from every 8th position.

$64 = (8 \times 8)$, i.e., 56bits

$64 - 8 = 56$

* Then apply left circular shift after dividing 56 bits into 2 parts: C_0 and D_0, each having 28 bits.
* D_1 and C_1 are obtained as Result.

left circular shift:-

* Move the bits based on Round number.
* For Rounds 1,2,9,16 – 1 bit shift
  other Rounds – 2 bit shift
* Here in PC2, C_1 and D_1 are combined to form 56bits again. permutted chocie 2 is applied,
* 56 bits are rearranged, permutted and in that 48 bits are selected.
* For Round 1, 48 bits are the key.

Round 1:- i/p – 64bit + 48 bit key
o/p – 64bit

Round 2:- i/p – 64bit + 48 bit key
o/p – 64bit

!

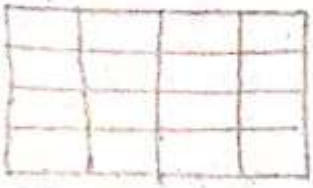
Round 16:- i/p – 64bit + 48 bit key
o/p – 64bit

* At the last, the cipher text is 64bit.

AES (Advanced encryption standard)

* It is a block cipher Algorithm.
* It has i/p array, state array and a key array

Input Array:-



each cell = 1 byte / 8 bits
Total cells = 16 cells
16 x 8 = 128 bits
4 words (32 each) = 128 bits.

PT is represented in the i/p Array.

State Array:-

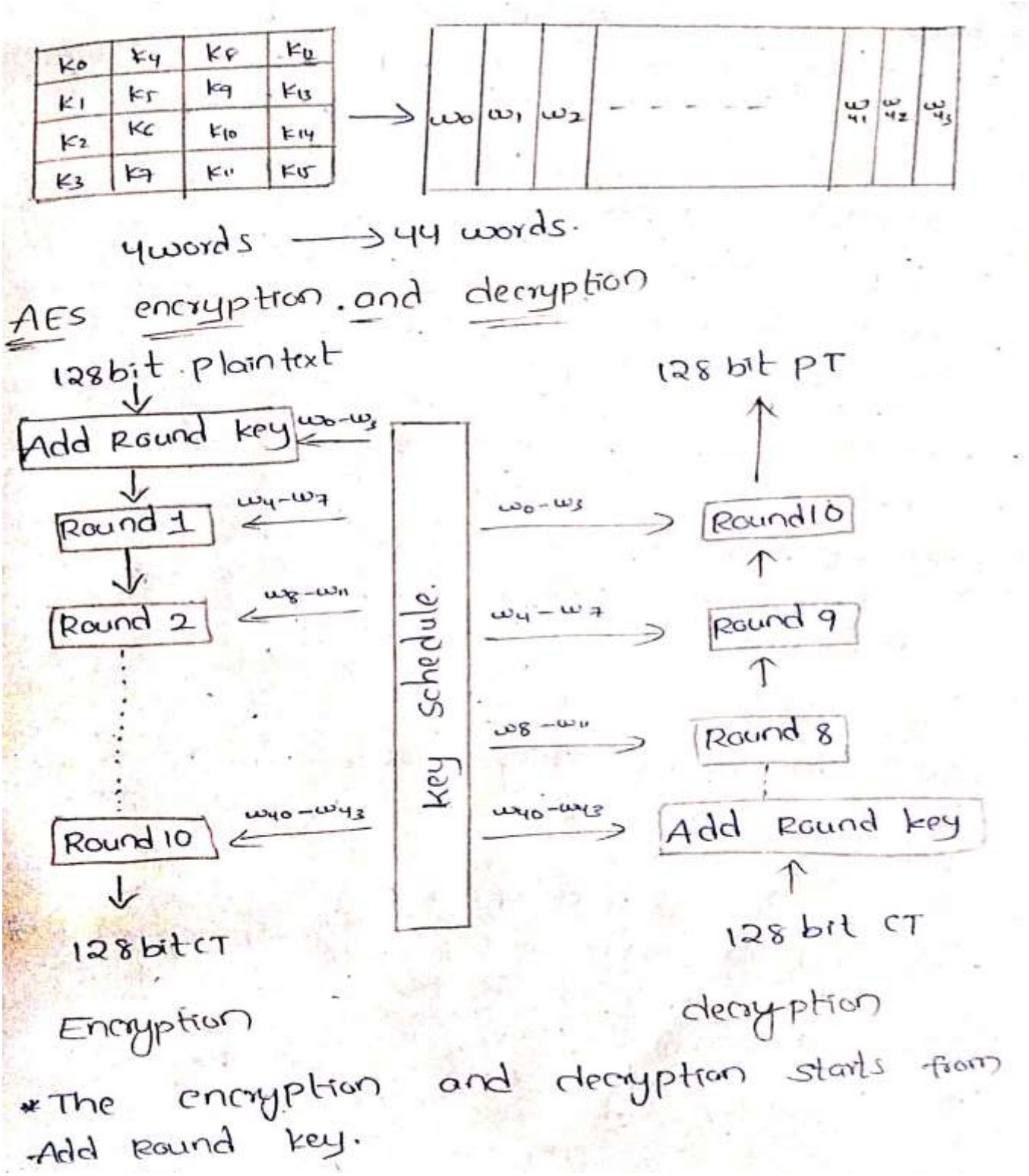
$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$ → 0th bit of 3rd word.
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

* It used to store intermediate results or states within the Rounds.
* The result is stored in the form of four words.

Key Array:-

* Actually we have 4th words. They are expanded into 44 words.
* In AES algorithm, there are 10 Rounds.
* Each round = 4 words

∴ 10 Rounds x 4 words = 40 + 4 (for Add Round key)
= 44 words.


K0 K4 K8 K12
K1 K5 K9 K13
K2 K6 K10 K14
K3 K7 K11 K15
W0 W1 W2 W41 W42 W43
4words → 44 words.
AES encryption and decryption
128bit plaintext
Add Round key
W0-W3
Round 1
W4-W7
Round 2
W8-W11
Round 10
W40-W43
128bit CT
Encryption
key schedule.
128 bit PT
Round10
W0-W3
Round 9
W4-W7
Round 8
W8-W11
Add Round key
W40-W43
128 bit CT
decryption
* The encryption and decryption starts from Add Round key.

* Each process (Encryption & decryption) starts from Round 1 and ends with Round 10.
* We have no-of Rounds = 10 (for encryption & decryption)
* In each Round we have four steps.
  1) substitute Bytes
  2) shift Rows (LCS)
  3) Mix columns – Not in Round 10
  4) Add Round key

  ↓

  In this XOR operation performed b/w the PT and key.
* 128 bit plain text is sending into the Add Round key along with the words w_0, w_1, w_2 & w_3. Total four words.
* For each and every round we have four words.
* Total 44 words along with add round key.
* Then we will get the 128 bit cipher text.
* This is the process of encryption.
* In decryption process the 128 bit cipher text is sending into add Round key along with the words $w_{40}, w_{41}, w_{42}, w_{43}$.
* This process will continue util the 128 bit plain text is obtained.

1) Blowfish:-

- It is a block cipher Algorithm
- It is a symmetric key cryptography.
- The input size is 64 bits.
- The key size is variable length key i.e., you can take any bit from 32 to 448 bits.
- so, it is more secure.

Properties:-

- It is very fast.
- It takes less memory
- It is simple to understand and implement
- It is more secure

* Blowfish Algorithm has 2 parts:
  1) key generation
  2) Data encryption.

* key generation:-
  * keys are stored in an array
    $k_1, k_2, k_3 \ldots k_n \; [1 \le n \le 14]$
  * Length of each block is 32 bits
    $(32 \times 14 = 448$ bits)

2) Initialise an array (P)

$P_1, P_2, P_3 \ldots P_{18}$

length of each word is 32 bits.

3) Initialse S-boxes (4) (substitution boxes).

$S_1 \rightarrow S_0, S_1, \ldots\ldots S_{255}$

$S_2 \Rightarrow S_0, S_1, \ldots\ldots S_{255}$

$S_3 \Longrightarrow$ "

$S_4 \Longrightarrow$ "

4) Initialise each element of p-array and S-boxes with hexadecimal values.

5. XOR operations are performed

$P_1 = P_1 \text{ XOR } K_1$

$P_2 = P_2 \text{ XOR } K_2$

$\vdots$

$P_{14} = P_{14} \text{ XOR } K_{14}$ [bcoz only 14 keys]

$P_{15} = P_{15} \text{ XOR } K_{15}$

$\vdots$

$P_{18} = P_{18} \text{ XOR } K_4$

6. Take 64 bit PT (Initially all bits are 0)

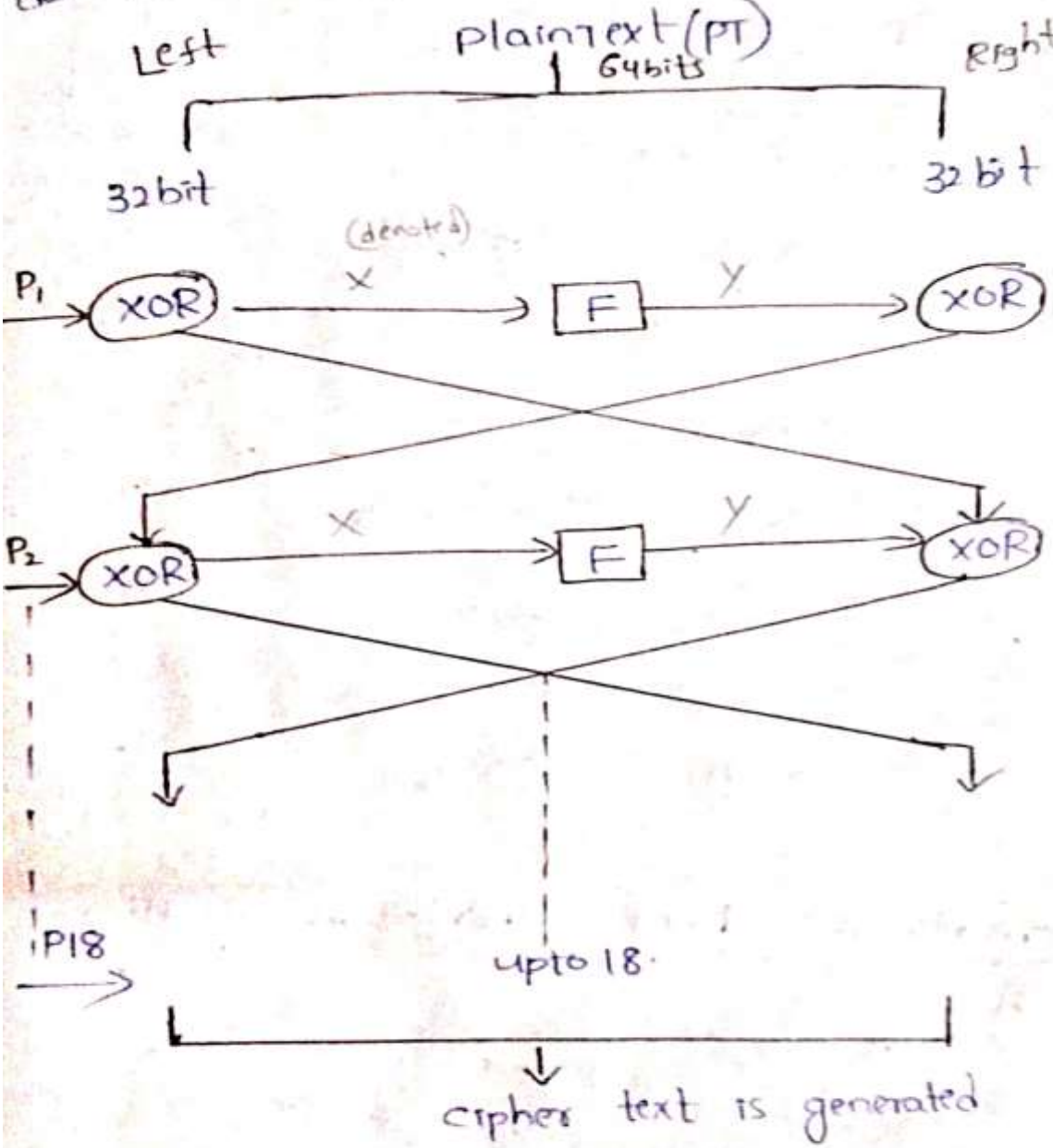
(0,0,0 ..... 0)

Subkey is generated.

Data encryption:-

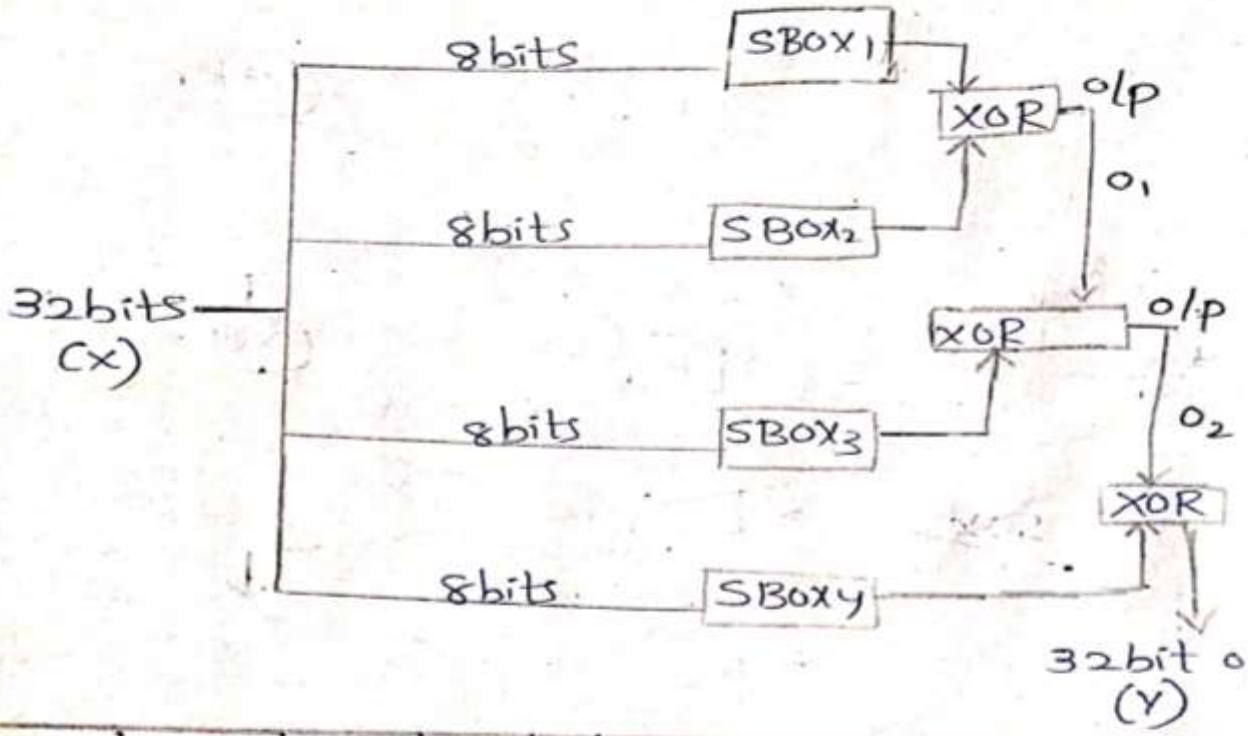
* Divide the plain text into two parts.
* Later the left 32 bit do the XOR operation with P_1. Then we get the output X.
* This o/p will sent into a function and Do function, then we get the output Y.

- The output Y and 32 bit of Right side will do the XOR operation.



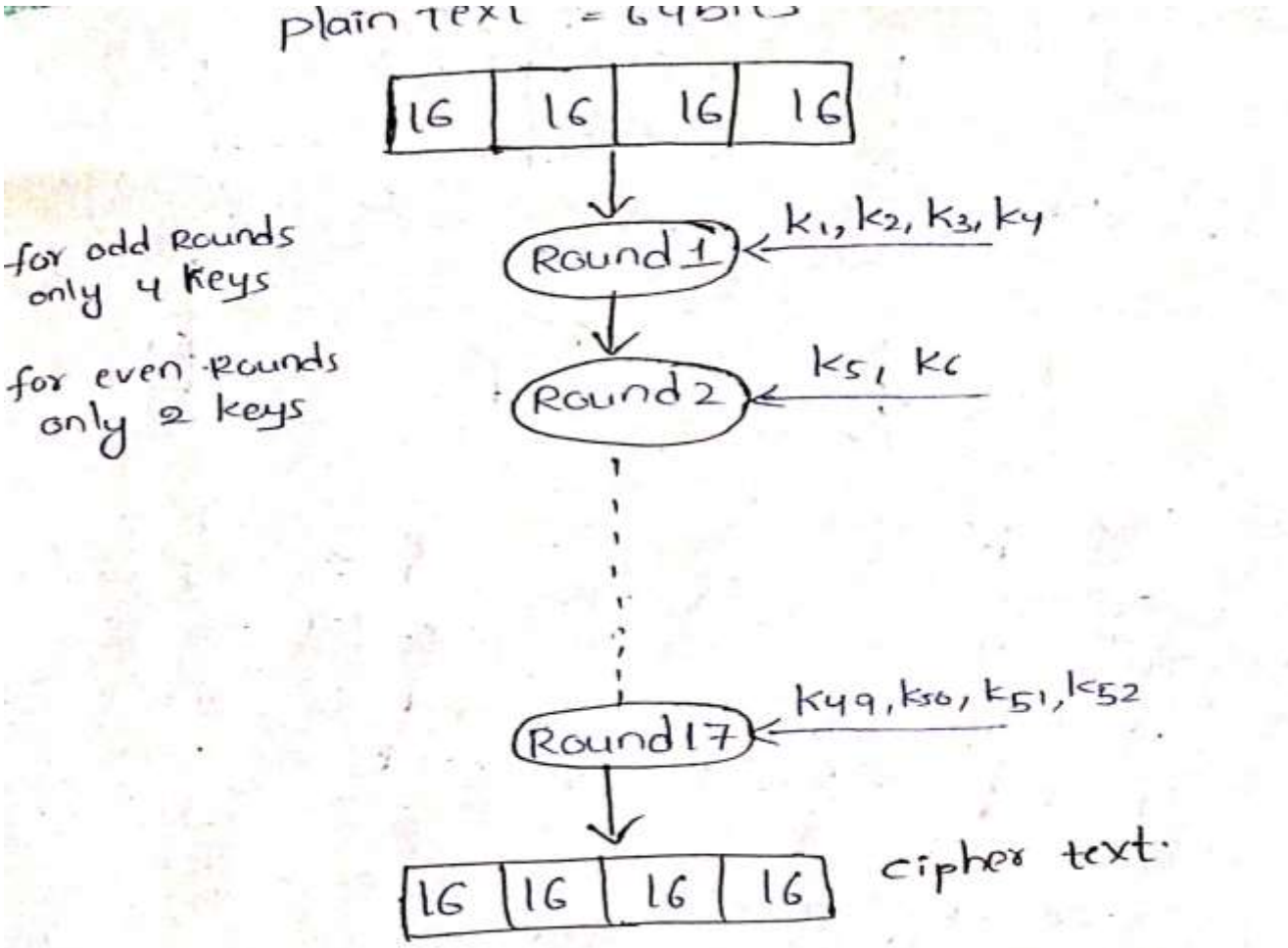
* The o/p of XOR operation of left side will send to Right side.
* The o/p of XOR operation of Right side will send to left side.

* This process continue upto P18.
* After that we have merge the 32 bits of left side and right side to get the cipher text of 64 bits.
* The diagrametic representation of function is:-



5) International data encryption Algorithm (IDEA):-

* It is a block cipher Algorithm
* symmetric key cryptography.
* It follows feistel ciphers (dividing PT into 4 parts).
* The input size is 64 bits i.e., (16,16,16,16)
* The key size is 128 bits and divided into 52 sub keys.
* We have 17 no. of rounds.



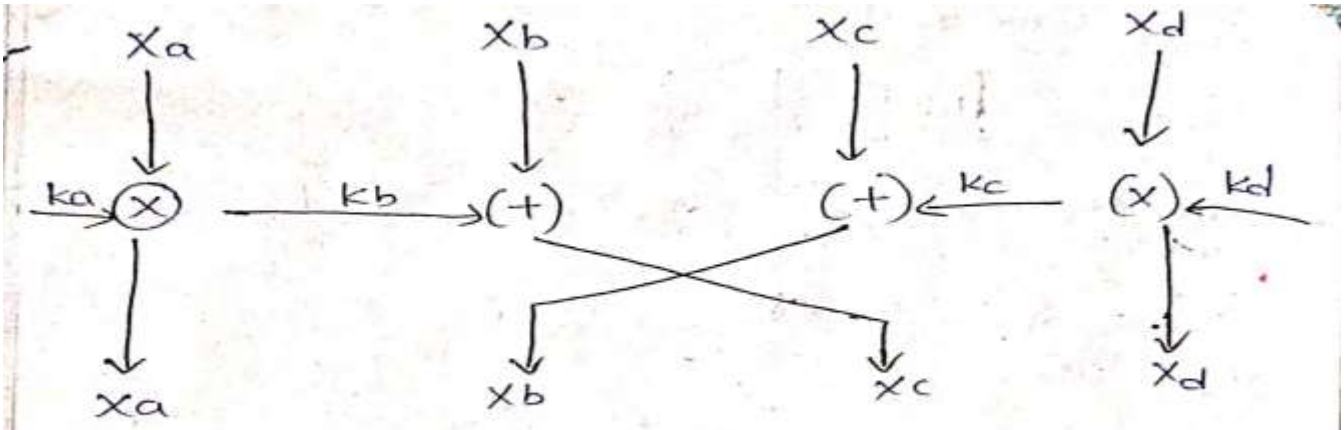
Rounds:-

odd Rounds:-

Input is divided in four parts

keys are four

16	16	16	16
x_a	x_b	x_c	x_d → input
k_a	k_b	k_c	k_d → key



* Here Xa and ka are the inputs and new Xa is generated as o/p. As well as Xd and kd are inputs, the new Xd is generated as o/p.
* But in the cases of Xb and Xc, the o/p's of Xb, kb and Xc, kc are swapped each other. In order to ensure security.
* The outer parts will be same and the inner parts will be swapped.

Even Rounds:-

* We have 4 no. of parts but no. of keys are two only.

Xa Xb Xc Xd

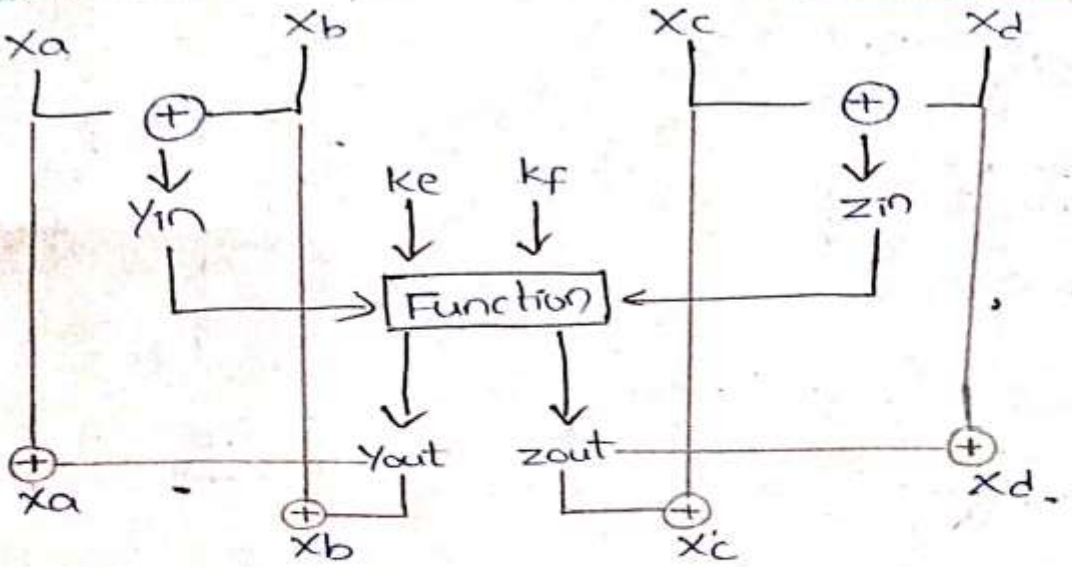
Ke, Kf

i/p = 4 but key = 2 so, Take ② parameters and perform XOR operation.

$Y_{in} = X_a \oplus X_b$

$Z_{in} = X_c \oplus X_d$

Now i/p = 2 & key = 2



$X_a = X_a \oplus Y_{out}$

$X_b = X_b \oplus Y_{out}$

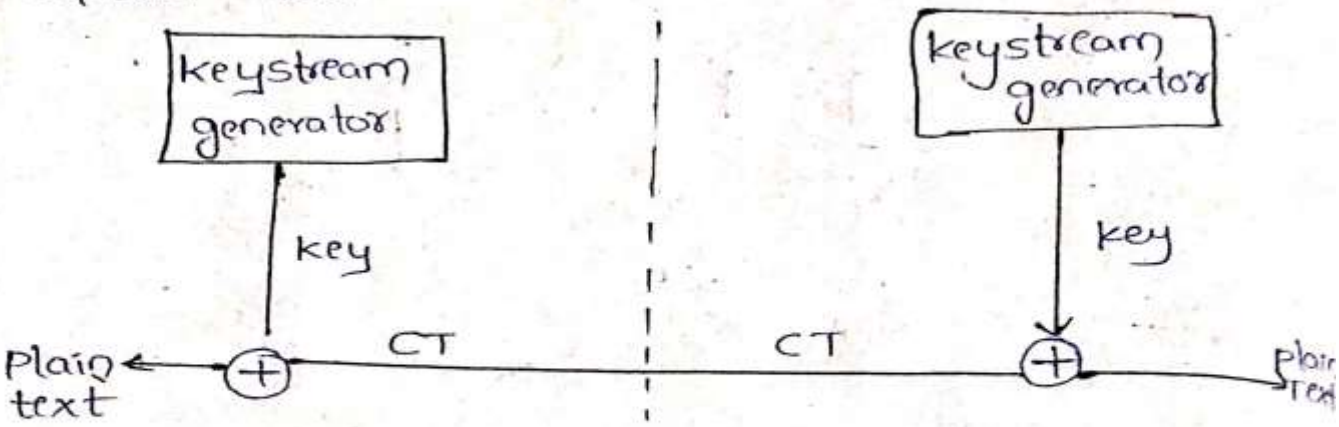
$X_c = X_c \oplus z_{out}$

$X_d = X_d \oplus z_{out}$

* X_a and X_b do XOR operation to get Y_{in}. And Y_{in} along ke are the inputs to do the function. After functioning we get the Yout as o/p.
* X_c and X_d do XOR operation to get z_{in}. And z_{in} along with kf are the inputs given to the function to generate the zout as o/p.
* Then X_a and Yout will do XOR operation to get the X_a as o/p.
* X_b and Yout will do XOR operation to get the X_b as o/p.
* X_c and zout will do XOR operation to get the X_c as o/p.
* X_d and zout will do XOR operation to get the X_d as o/p.

7] Stream ciphers:-

* plain text is divided into number of stream



* (Bitwise) Keys are generated from keystream generator
* Bitwise XOR operation is performed blw the key and plain text. As the result we get the CT.
* In decryption, with the help of key and CT, we will perform a bitwise XOR operation to get plain text.
* Bitwise XOR means it will consider each bit one by one.

Explanation:-

m_1 m_2 m_3 .... m_i → plain text

$\oplus$ k_1 k_2 k_3 .... k_i → keys

c_1 c_2 c_3 .... c_i → cipher text

(ciphertext $\oplus$ key ⟹ plain text) decryption

$$\begin{array}{cccccc} C_1 & C_2 & C_3 & \cdots & C_i \\ k_1 & k_2 & k_3 & \cdots & k_q \\ \hline P_1 & P_2 & P_3 & \cdots & P_i \end{array} \quad (\oplus)$$

Eg:-

PT : 1100
key : 1011
0111 → CT

(bitwise XOR :- same = 0, diff = 1)

CT : 0111
key : 1011
1100 → PT

8) RC4:-

*It is a stream cipher Algorithm.

Procedure:-

1) uses an array (S) - state vector of length 256 bits (0-255)
2) It has a key encoded with ASCII
3) It has a key array of length 256 (0-255)

*RC4 algorithm has three steps:-

1) key scheduling
2) key stream generation
3) Encryption & decryption

1) Key scheduling:-

*No. of iterations is equal to size of S-array.

initialize j=0

for i=0 to 255 do

$j = [j + S[i] + T(i)] \bmod 256$ (depends on size give the mod value)

swap(S[i], S[j]);

Here,

S[i] → state vector

T[i] → key array (temporary vector).

Example:-

S-array = [0 1 2 3 4 5 6 7] (assume)

key array = [1 2 3 6]

Plain text = [1 2 2 2]

Initialise T-array with key

T = [1 2 3 6 1 2 3 6]

i) j = 0

for i = 0 to 7

$j = [0 + 0 + 1] \bmod 8$

$j = 1 \bmod 8$

$j = 1$

swap S(0) and S(1)

S = [1 0 2 3 4 5 6 7]

ii) For i = 1

$j = (1 + 0 + 2) \bmod 8$

$j = 3 \bmod 8$

$j = 3$

swap S(1) & S(3)

S = [1 3 2 0 4 5 6 7]

iii) For i = 2

$j = [3 + 2 + 3] \bmod 8$

$j = 8 \bmod 8$

$\therefore j = 0$

swap S(2) & S(0)

S = [2 3 1 0 4 5 6 7]

* we have to do like this upto 8th iteration.

Stream generation:-

*No. of iterations is equal to size of key (4)

```
i,j = 0;
while (true)
i = (i+1) mod 256;
j = (j+S[i]) mod 256;
swap (S(i), S(j));
t = (S[i] + S[j]) mod 256
K = S[t];
```

* Like this we will get the key array.
  for 1st iteration we get K(0)
  for 2nd iteration we get K(1)
  :
  " " " K(n)

* New key is obtained is used for encryption and decryption.

Encryption and decryption:-

Encryption :- PT XOR New key.

*In this first we have to convert the PT and new key into binary.

PT = 1 2 2 2

Then,

PT :- 0001 0010 0010 0010

key :- ( ) ( ) ( ) ( )

CT :-

decryption:- CT XOR New key

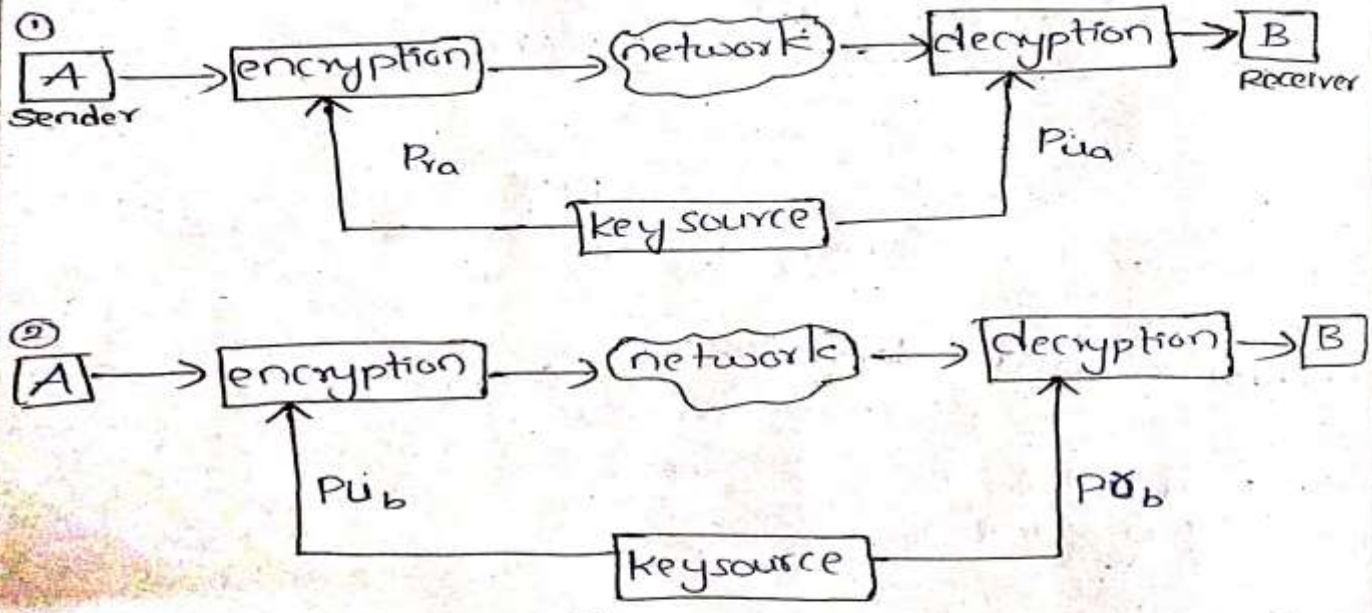
PART-B

Asymmetric key ciphers:-

Principles of public key cryptosystems:-

* For Asymmetric key cryptography we have different key for encryption and decryption.
* There are two principles:
  1) Authentication
  2) confidentiality.

1) Authentication:-

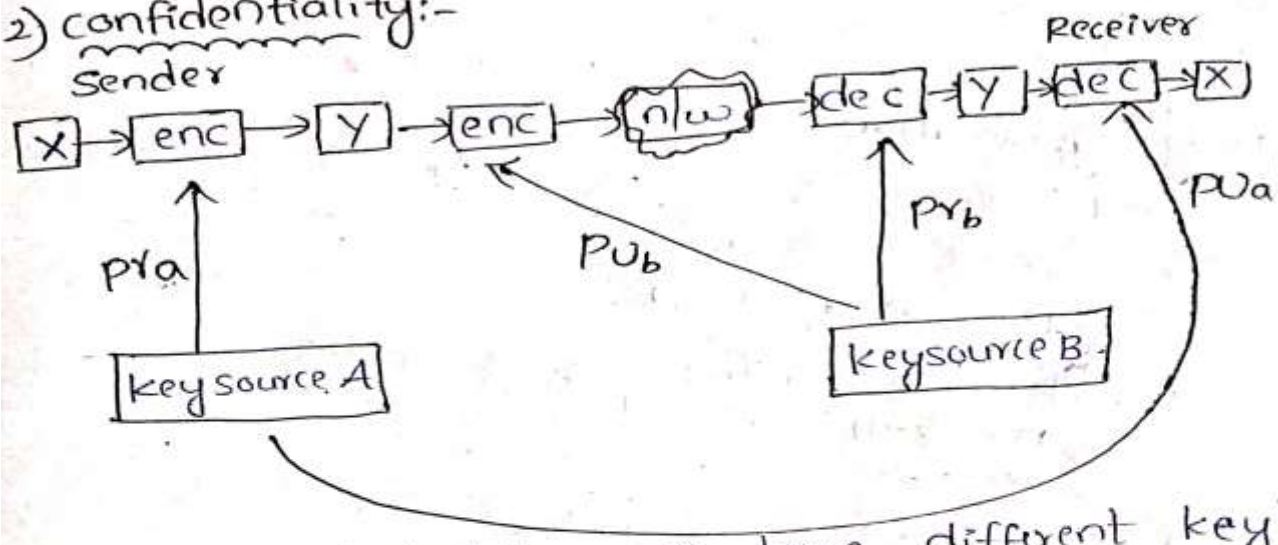


* Here the sender sends the PT and it will encrypted with the help of key which is named as private, taken from key source.
* Then the encrypted msg will enter into a network and come out of this network then to decrypt the msg we are using public A key from

the key source. At last the cipher text is reconverted into plain text which is received by the receiver.

* Here the key source provided the different keys ie, privateA and publicA. but the same source.
* This is known as Authentication.

2) confidentiality:-



* In confidentiality we have different key sources (key source A & key source B).
* The keysource A will genirate the public A & privateA keys which is provided to X (sender)
* The keysource B will generate the privateB, & public B keys which is provided to Y (receiver).
* In this, the privateA key of keysource A is provided to sender and publicA key of keysource A is provided to receiver.
* The privateB key of key source B provided to Receiver and public B key of key source B is provided to sender.

2] RSA Algorithm:-

* Rivest - Shamir - Adleman (RSA)
* It is a asymmetric key algorithm and block cipher algorithm.
* There are three steps involved:-
  1) key generation
  2) Encryption
  3) Decryption.

1) key generation:-

1. Select two large prime numbers p and q for more security
   p=3 and q=11
2. calculate the value of n = p * q
   n = 3x11
   n = 33
3. calculate $\phi(n) = (p-1)(q-1)$
   $\phi(n) = (3-1)(11-1)$
   $= 2 \times 10$
   $= 20$
4. choose the value of 'e' such that $(1 < e < \phi(n)$ and gcd $(\phi(n), e) = 1$
   $(1 < e < 20)$ and gcd $(20, e) = 1$
   e = 7 gcd $(20, 7) = 1$
5. calculate $d = e^{-1} \bmod \phi(n)$
   $ed = 1 \bmod \phi(n)$
   $ed \bmod \phi(n) = 1$

   $ed \bmod \phi(n) = 1$
   $7 \times d \bmod 20 = 1$
   $7 \times 3 \bmod 20 \longrightarrow 21 \bmod 20 = 1$ $\therefore \boxed{d = 3}$

6) public key = {e,n} =
= {7,33}

7) private key = {d,n}
{3,33}

2) Encryption:-

The formula of encryption is:

$$C = m^e \bmod n$$

M = no. of digits in PT
C = cipher text
e = encryption
m should $m < n$ i.e., $m < 33$

⇒ Let $m = 31$

$C = (31)^7 \bmod 33$
$= 4$
$\therefore C = 4$

3) Decryption:-

$$m = c^d \bmod n$$

⇒ $m = 4^3 \bmod 33$
$m = 64 \bmod 33$
$m = 31$

3) Elgamal cryptography:-

* It follows the principles of Asymmetric key cryptography.
* It has three steps:- 1) key generation
2) encryption
3) decryption

1) key generation:-

1) select large prime number (P) P = 11

2) select a dec. key also called private key d = 3

3) select second part of encryption key (e_1) $e_1 = 2$

4) calculate third part of encryption key (e_2)

$$e_2 = e_1^d \bmod p$$

$$e_2 = (2)^3 \bmod 11$$

$$= 8 \bmod 11$$

$e_2 = 8$

5) public key = $(\epsilon_1, \epsilon_2, P)$ and private key = d.

pub key = (2, 8, 11)

2) Encryption:-

1) select random integer (R)

R = 4

2) calculate $c_1 = \epsilon_1^r \bmod p$

$$c_1 = 2^4 \bmod 11$$

$$= 16 \bmod 11$$

$c_1 = 5$

3) calculate $c_2 = (PT \times e_2^R) \bmod P$

$= (7 \times 8^4) \bmod 11$ PT = Assume (7)

$= 28672 \bmod 11$

$c_2 = 6$

4) cipher text = (c_1, c_2)

$c_1, c_2 = (5, 6)$

3) Decryption:-

i) $PT = [C_2 \times ((C_1)^D)^{-1}] \bmod p$

$= 6 \times ((5)^3)^{-1} \bmod 11$

$= 6(5^3)^{-1} \bmod 11$

$= 6(125)^{-1} \bmod 11$

$= 125 \times x \bmod 11 = 1$

If $x = 3$, $125 \times 3 \bmod 11 = 375 \bmod 11$

$= 1$

$\therefore \boxed{x = 3}$

$6 \times 3 \bmod 11 = 18 \bmod 11 = 7$

$\boxed{PT = 7}$

4) DIFFIE - Hellman key Exchange Algorithm:-

* It is a Asymmetric key cryptography.
* It is used to exchange keys blw sender and Receiver.
* It just exchange the key, didn't perform the encryption /decryption Algorithm.

Procedure:-

1) consider a prime number q

let $q = 7$.

2) select α such that $\alpha < q$ and α is primitive root of q.

Primitive root?

$\alpha^1 \bmod q$

$\alpha^2 \bmod q$

$\alpha^3 \bmod q$

$\alpha^{q-1} \bmod q$,

Ex:- $\alpha = 3$ and $q = 7$

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$ = {7, 3, 2, 6, 4, 5, 1}

$3^3 \bmod 7 = 6$ {1, 2, 3, 4, 5, 6, 7}

$3^4 \bmod 7 = 4$

$3^5 \bmod 7 = 5$ $\therefore$ 3 is primitive root of 7.

$3^6 \bmod 7 = 1$

3. Assume X_A (private key of A) and $\boxed{X_A < q}$

Calculate $Y_A = \alpha^{X_A} \bmod q$

Y_A = public key of A

Ex:- $q = 7$ and $\alpha = 5$ and let $X_A = 3$ ($\because$ X = private, Y = public)

$Y_A = (5)^3 \bmod 7 = 125 \bmod 7 = 6$

$\boxed{Y_A = 6}$

4. Assume X_B and $X_B < q$

Calculate $Y_B = \alpha^{X_B} \bmod q$

Let $\boxed{X_B = 4}$

$Y_B = (5)^4 \bmod 7 = 625 \bmod 7 = 2$

$\boxed{Y_B = 2}$

5. Calculate secret keys k_1 and k_2 for exchanging

$k_1 \rightarrow$ person A and

$k_2 \rightarrow$ person B

$k_1 = (Y_B)^{X_A} \bmod q$ $\quad k_2 = (Y_A)^{X_B} \bmod q$.

After calculating, if $k_1 = k_2$ then success

$k_1 = (2)^3 \bmod 7 = 8 \bmod 7 = 1 \longrightarrow \boxed{k_1 = 1}$

$k_2 = (6)^4 \bmod 7 = 1296 \bmod 7 = 1 \longrightarrow \boxed{k_2 = 1}$

$\boxed{k_1 = k_2}$ $\therefore$ success.

keys exchanged successfully.

5) knapsack problem:-

* It was proposed by Hellman.
* It is a Asymmetric key cryptography.

Ex:-

weights = (1,6,8,15 and 24)

In general knapsack, we select weights to acheive a sum

* If we want sum = 30 then, we select 1, 6, 8, 15.

Let plain text

PT:- 1 0 0 1 1
wt:- 1 6 8 15 24
CT:- 1 + 15 + 24 = 40

PT:- 1 1 0 1 0
wt:- 1 6 8 15 24
1 + 6 + 15 = 22

∴ CT = 40 & 22

* key generation:-

1) public key (Hard knapsack)
2) private key (easy knapsack)

↓ we find private key first.

Ex:-

{1,2,4,9,20,40}

weights are always in increasing order

1. first, find private key (Assume)

D = {1,2,4,10,20,40} — pvt key.

select ② numbers "n" and "m"

m > sum of all no.s in sequence.

Sum = 77 ∴ let m = 110 (select no. which is more than 79)

n - select so that it has no common factor with m

∴ let n = 31

Now (D * n) mod M ∀ elements in D

(1 x 31) mod 110 = 31

(2 x 31) mod 110 = 62

(4 x 31) mod 110 = 14

(10 x 31) mod 110 = 90

(20 x 31) mod 110 = 70

(40 x 31) mod 110 = 30

{31, 62, 14, 90, 70, 30} ⇓ public key.

* Encryption:-

Now, assume PT

let PT = 10010 | 111100 | 101110

divide into 6-6 parts (no. of elements in sequence = 6).

1st part ⟹ 100100 = 1x31 + 0x62 + 0x14 + 1x90 + 0x70 + 0x30

= 31 + 90

= 121.

2nd part ⟹ 111100 = 1x31 + 0x62 + 1x14 + 1x90 + 0x70 + 0x30

= 197.

3rd part ⟹ 101110 = 1x31 + 0x62 + 1x14 + 1x90 + 1x70 + 0x30

= 205

∴ CT = [121 197 205].

*Decryption:-

Calculate $n^{-1} = 31^{-1}$

$31x \bmod 110 = 1$ then we get $x = 71$

$(CT \times x) \bmod m$ from seq D = {1, 2, 4, 10, 20, 40} - pvt key

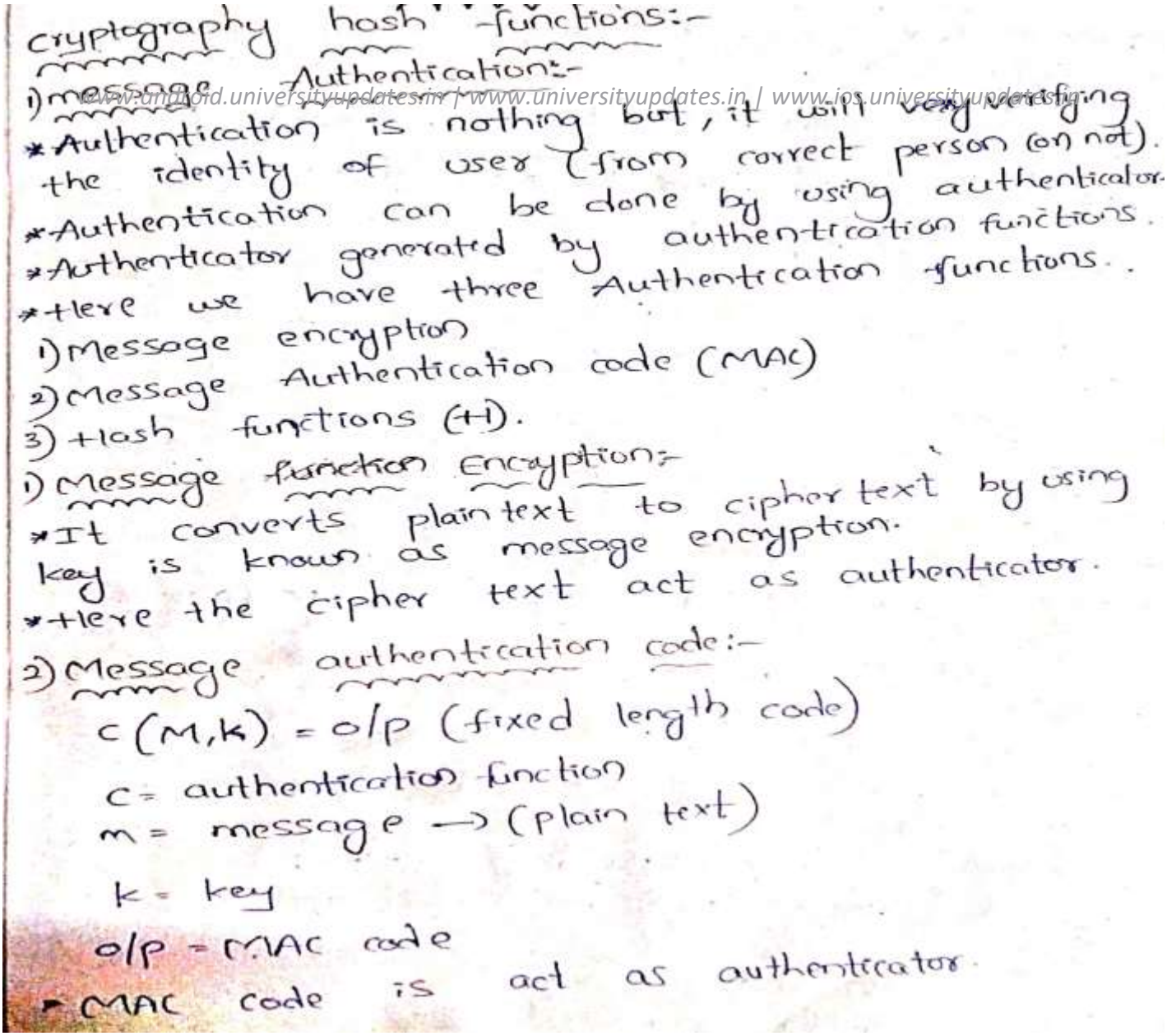
$(121 \times 71) \bmod 110 = 11 = 100100$ (1+10 = 11)

$(197 \times 71) \bmod 110 = 17 = 111100$ (1+2+4+10 = 17)

$(205 \times 71) \bmod 110 = 35 = 101110$ (1+4+10+20 = 35)

UNIT – III

Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA-512), Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme. **Key Management and Distribution:** Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure



cryptography hash functions:-

1) message Authentication:-

* Authentication is nothing but, it will verifying the identity of user (from correct person (or) not).
* Authentication can be done by using authenticator.
* Authenticator generated by authentication functions.
* Here we have three Authentication functions..
  1) Message encryption
  2) Message Authentication code (MAC)
  3) Hash functions (H).

1) Message function Encryption:-

* It converts plain text to cipher text by using key is known as message encryption.
* Here the cipher text act as authenticator.

2) Message authentication code:-

c(M,k) = o/p (fixed length code)

c = authentication function

m = message → (plain text)

k = key

o/p = MAC code

* MAC code is act as authenticator.

3) Hash function (H):-

* Here in case of key, we will be using Hash function.
* key is replaced with hash function.
  H(m) = fixed length code (Hash code h)
  H = hash function
  h = hash code
* This hash code will act as authenticator.

2) secure hash algorithm (SHA):-

* It is a modified version of MD5 (Message digest)
* In MD5 the length of the o/p is 128 bits.
* In SHA the length of the o/p is 160 bits.

Working:-

1) padding:-

* In this, we have to add extrabits to the orginal message.

original message + (padding) → extrabits.

so, that total length is 64 bit, less than exact multiple of 512.

Example:- orginal msg = 1000 bits

512 x 1 = 512 bits
512 x 2 = 1024 bits
512 x 3 = 1536 bits

1536
- 64
1472

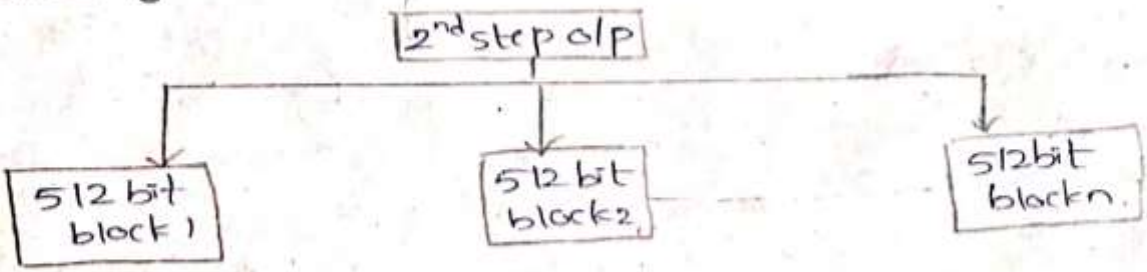
∴ add 472 bits

1000 bits + 472 bits = 1472 bits.

2) Appending :-

* Append the original length before padding
  calculate length mod 64
* Most of the cases, 64 bits is obtained as answer
  (∴ append 64 bits)
* so, it again becomes multiple of 512.
  Means 1472 bits + 64 bits = 1536 bits.

3) Dividing :- (each 512 bits)



4) Initialising :- (5 chaining variables)

* Here we have consider 5 chaining variables, the values are predefined.
  each = 32 bit
  (A) (B), (C), (D) & (E) → values predefined.

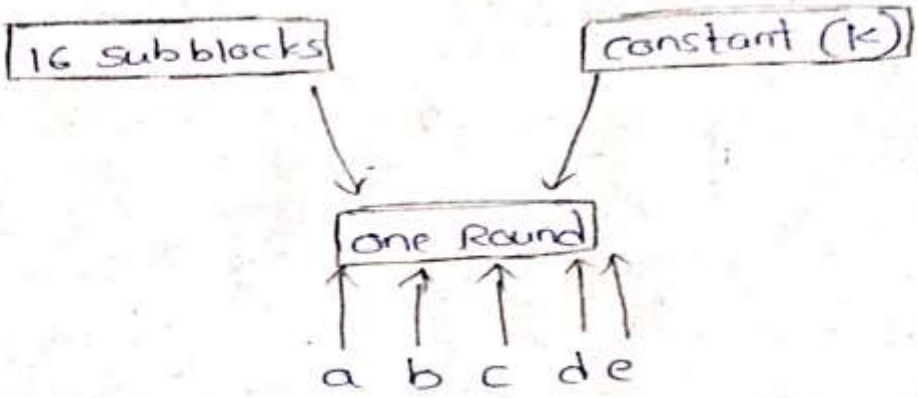
5) Process Blocks :- 5 chaining variables into

i) copy ↑ corresponding variables
   A = a, B = b, C = c, D = d, E = e.

ii) divide into no. of 512 bit blocks
   (16 – 32) → each 32 bits.
   subblocks

iii) Four Rounds (each round = 20 steps)

16 subblocks and a constant (K)



$a = b + ((a + process, p(b,c,d,e) + m[r] + T[k]))$

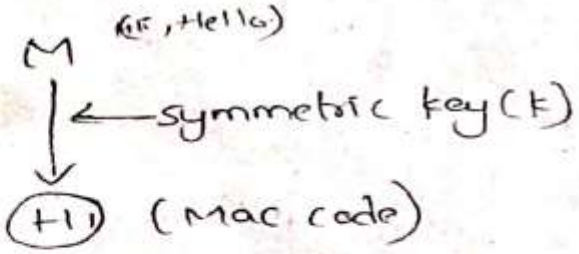
PART-B

Message Authentication code (MAC):-

* It is similar to message digest 5
* In this, symmetric key cryptography is used.

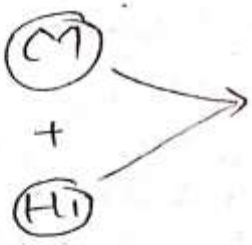
Working:-

* If a sender wants to send a message M by using symmetric key (K), then we get the H1 (MAC code) i.e., cipher text



* Now, the message and Hash code (H1) combined together sent to the Receiver.
* The Receiver calculate his own MAC (H2) by using key (K) i.e., same key that is used at

the sender side.



Now, on Receivers side, H_1 and H_2 are compared.

$H_1 = H_2$ → no change in message

$H_1 \neq H_2$ → message is changed.

Significance of MAC:-

1. Receiver can know if message is changed / not.
2. Receiver has assurance that message is from correct Sender. (because same key for ⑤ and ⑥)

2) Message Authentication Requirements:-

*There are seven message Authentication Requirements.

1) Disclosure (Release of msg content)
2) Traffic Analysis
3) Masquerade

→ [which is same in attacks of security]

4) content modification
5) sequence modification
6) Timing modification
7) Repudiation

) Content modification:- changes to the contents of a message, including insertion, deletion, transposition, or modification.

5) Sequence modification:- Any modification to a sequence of messages blw parties, including insertion, deletion and reordering.

6) Timing modification:- Delay (or) replay of messages. In a connection orented application, individual messages in the sequence could be delayed (or) replyed.

7) Repudiation:-
Denial of receipt of message by destination (or) Denial of transmission of message by source.

3) Hash based MAC (HMAC)

* It is used in secure sochet layer. algorithm.

Working of HMAC:-

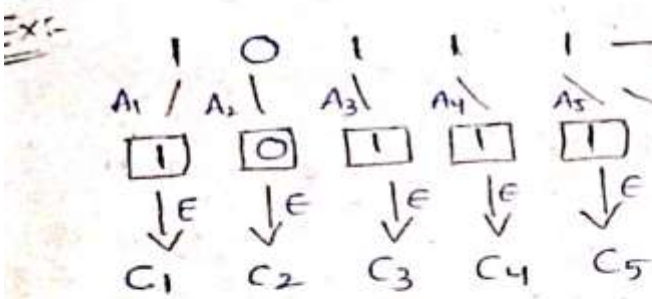
original msg(m) → message digest is generated
↓ MD5/SHA
↓ ← key(K)
encryption
↓
MAC (CT)

* By using MD5/SHA, the original message (M) is generated the message digest.
* The message digest is encrypted by using the key (K). Then MAC is obtained which is known as cipher text.
* In MAC - direct MAC is generated
* In HMAC - MAC is generated with the help of msg digest.

1) Cipher Based MAC (CMAC):-

* It has message size limit.
* It is based on block cipher algorithm.
* The given message is divided into equal number of blocks and each block is encrypted separately.

Ex:-



* Here the last cipher text (C5) act as a MAC. Because we have 5 cipher texts from that we have choose last one.

* Theoretically:-

$C_1 = E(k, A_1)$

$C_2 = E(k, (A_2 \oplus C_1))$

$C_3 = E(k, (A_3 \oplus C_2))$

$C_4 = E(k, (A_4 \oplus C_3))$

$\vdots$

$C_n = E(k, (A_n \oplus C_{n-1}))$

C_n ↓ Act as MAC.

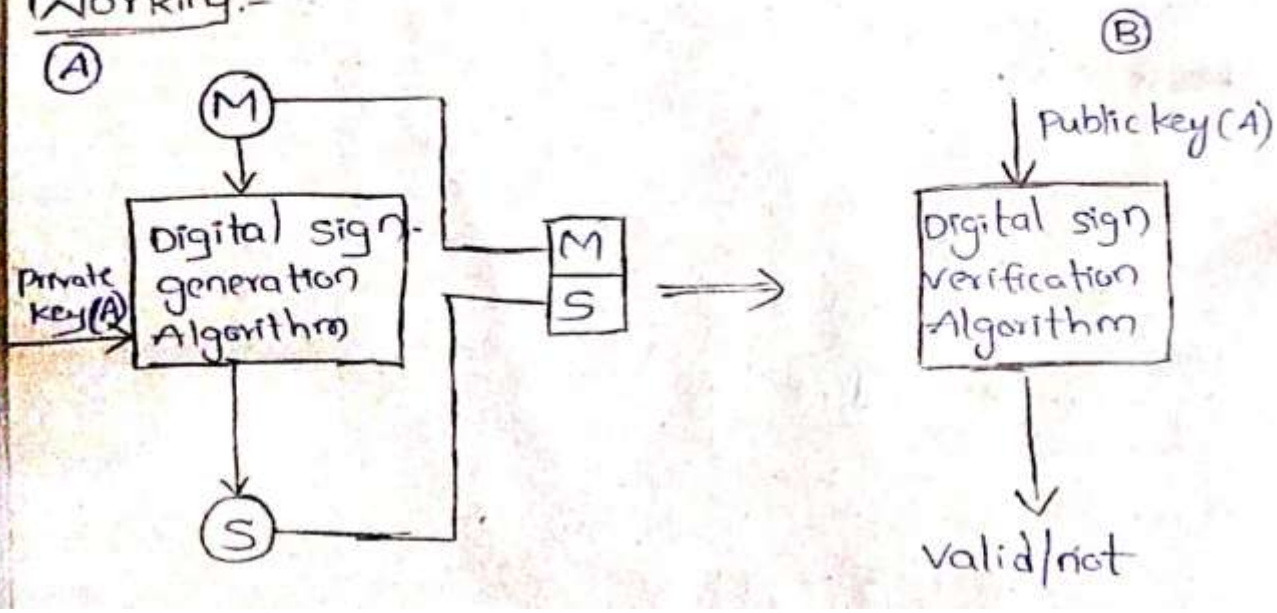
5) Digital signature:-

* It is Asymmetric key cryptography.
* It uses both private and public key.
* For encryption, private key is used.
* For decryption, public key is used.
* It is used for both authentication and Non-Repudiation.
* **authentication:-** sending the message to the correct person.
* **Non-Repudiation:-** The person who receives the msg, he cannot deny (like phone, gpay)

Signature:-

It is a proof of identity. That is it from correct sender / not.

Working:-



* The message and private key (A) are as the inputs of digital signature generation Algorithm.
* And It generates the signature.
* Again the message and generated signature combined together and sent to the Receiver
* The public key (A) of Receiver side and the combination of message and signature are as the inputs for digital signature verification Algorithm
* Then it checks wheather it is valid (or) not.
* If message matches then it is valid.
* If message is not matching then it is not valid.

6) Elgamal digital signature:-

* It is one of the digital signature scheme.
* For encryption we are using public key
* For decryption we are using private key

Working:-

1) select a prime number (q)
2) select a primitive root (α) of q
3) generate a random integer (X_A)
   $1 < X_A < q-1$
4) compute $Y_A = (\alpha)^{X_A} \bmod q$
5) Generate keys for user (A)
   private key $\Longrightarrow X_A$
   public key $\Longrightarrow \{q, \alpha, Y_A\}$
6) generate hashcode (m) for the plain text (M)
   $m = H(M) \quad 0 \leq m \leq q-1$

7) Generate a random Integer K
$1 \le K \le q-1$ and gcd $(K, q-1) = 1$

8) Now calculate S_1 and S_2 ; $S_1 = \alpha^K \bmod q$

$S_2 = K^{-1} (m - X_A S_1) \bmod q-1$

9) Now we got the signature pair (S_1, S_2)

Note, at user's B's side

Calculate V_1 and V_2

$V_1 = \alpha^m \bmod q$

$V_2 = (Y_A)^{S_1} \cdot (S_1)^{S_2} \bmod q$

if $V_1 = V_2$
signature is valid

if $V_1 \neq V_2$
signature is not valid.

Example:-

Let $q = 19$ and $\alpha = 10$

Now, Random integer X_A $(1 < X_A < q-1)$

$\Rightarrow 1 < X_A < 18$

$\Rightarrow \boxed{X_A = 16}$

$Y_A = \alpha^{X_A} \bmod q$

$= (10)^{16} \bmod 19$

$\boxed{Y_A = 4}$

A) keys:- private key $X_A = 16$

public key $\{q, \alpha, Y_A\} = (19, 10, 4)$

Now, generate hash code (m)

$m = H(M)$ $\quad 0 \le m \le q-1$

$0 \le m \le 18$

$\therefore \boxed{m = 14}$

generate (k), $0 \le k \le q-1$ and gcd $(k, q-1) = 1$

$0 \le k \le 18$ and gcd $(k, 18) = 1$

$\therefore \boxed{k = 5}$

calculate $S_1 = \alpha^k \bmod q$

$= (10)^5 \bmod 19$

$\boxed{S_1 = 3}$

$S_2 = k^{-1}(m - x_A S_1) \bmod q-1$

$k^{-1} \Longrightarrow k^{-1} \bmod q-1$

$5^1 \bmod q-1$

$5 \times ? = 1 \pmod{18}$

$\boxed{k^{-1} = 11}$

$\left[\begin{array}{l} \frac{5 \times ?}{18} = 1 \\ \frac{5 \times 11}{18} = 1 \\ \therefore \frac{55}{18} = 1 \end{array}\right]$

$S_2 = 11(14 - 16 \times 3) \bmod 18$

$= 374 \bmod 18$

$\boxed{S_2 = 4}$

At B's end:-

$V_1 = \alpha^m \bmod q$

$= 10^{14} \bmod 19$

$\boxed{V_1 = 16}$

$V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q$

$= 4^3 \times 3^4 \bmod 19$

$= 5184 \bmod 19; \boxed{V_2 = 16}$

Now, $V_1 = V_2$
∴ signature is valid.

PART-C

Key Management and distribution:-

key management:-

* The main aim of key management is to generate a secret key blw two parties and store it to prove the authenticity blw communicating users.
* key management is the techniques which support key generation, storage and maintainance of the key blw authorized users.
* key management plays an important role for securing cryptographic goals like confidentiality, authentication, data integrity and digital signatures.
* Basic purpose of key management is key generation, key distribution, controlling the uses of keys, updating destruction of keys and key backup/recovery.

The points to be executed in KM:-

1) user registration
2) user initialization
3) key generation
4) key installation
5) key registration
6) Normal use
7) key backup
8) key update
9) key Recovery
10) key de-registration and revocation.

2] Key distribution in symmetric key:-

* There are four ways:-

1) physical delivery
2) key distribution center (KDC)
3) using previous keys.
4) using third party

1) Physical delivery:-

* The sender and receiver will meet physically and exchanging the key.
* It is most secure way to exchange key
* The disadvantage is, it takes more time.

2) Key distribution center:-

* It will generate the key and it will distribute the key for both sender and Receiver
* It takes less time.
* It is authentic, but you have to relay on (or) depend third party (KDC).

3) Using previous key:-

* By encrypting the previous key, we generate the new key.
* We didn't generate the new key directly, by using some hint of previous key, we generate new key.

4) Using third party:-

* The sender send the msg to third party, that third party will send the msg to Receiver. Here we have trusted third party.

* The sender and receiver will communicate with each other indirectly.

3] key distribution [in Asymmetric key]

* There are four ways:-
  1) Public Announcement
  2) public key directory
  3) public key Authority
  4) certificate Authority.

Public Announcement:-

* The particular user will announce the key to all other users in that network.
* So, they can do encryption (or) decryption. They will broadcast.

2) Public key directory:-

* It is like telephone directory.
* All users will put (or) store their keys in public key directory.
* User can come and search for it's required key and takes the key
* changes should reflect in the directory also. like updation, adding new keys etc.--

3) public key Authority:-

* It is similar to the directory but, improves a security by tightening control over the distribution of keys from the directory.

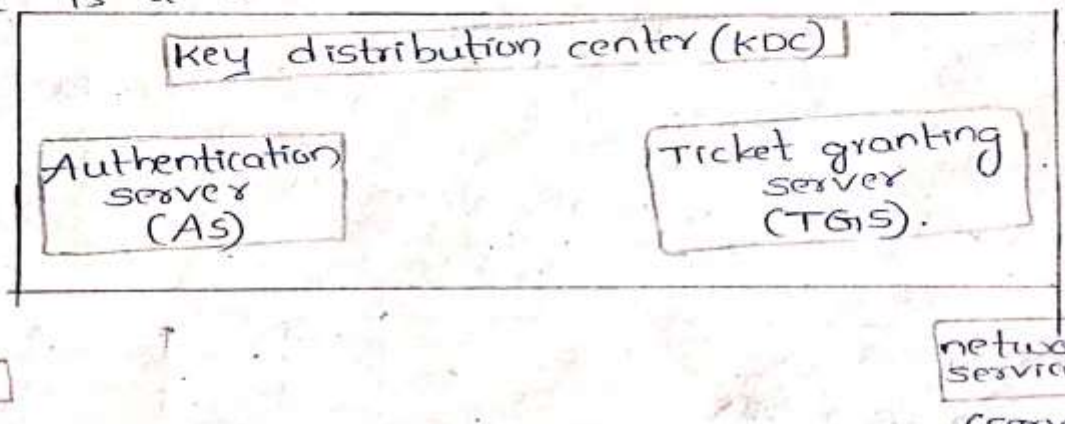
4) Certificate Authority:-

* A trusted third party organization that issues public key certificates is known as a ceritificate Authority (CA).
* The CA can be likened to a notary public.

4) Distribution of public keys:-

5] Kerberos:-

* It is a networky authentical protocol.
* It follows a client server Architecture
* It follows a symmetric key algorithm.
* It Requires a third party for key
* KDC is a database of all secret keys.



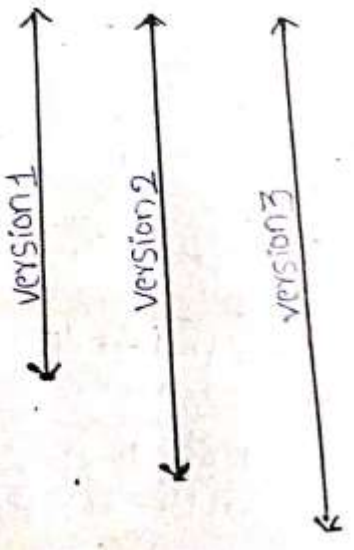
* user sends a request to key distribution center for keys.
* Then Authentication server will respond, and sends a ticket to the user.
* The ticket is in the encrypted form. Then user will decrypt the ticket to get the Hash code.

* The hash code again will send to the authentication server.
* Then authentication server checks that authenticity i.e., if the user will able to decrypt the ticket correctly then it declare that he is a cerifited user. (or) authorbed user.
* Then Authentication server gives service ticket to the ticket granting server (TGS)
* The TGS will gives the service ticket (secret key) to the user.
* By using this service ticket, the user will communicate with network services.

6] X-509 Authentication Service:-

* It is a digital cerificate which is accepted by internationally.
* It does not generate any keys. but it provides a way to access public keys.
* There are several elements in x509 certificate.
* It has three versions.

Versions
serial number
signature Algorithm Identifier
Issuer Name
validity period
subject Name
public key Information
Issue unique ID
subject unique ID
Extentions.



Versions:-

* we have 3 versions:-
* version 1 is from version to public key information.
* version 2 is from version to subject unique ID.
* version 3 is from version to extentions.

Serial number:-

* It is a serial number of certificates.

Signature Algorithm identifier:-

* In order to sign on the cerificate, which algorithm the user used. The algorithm may be a RSA, IDEA etc...

Issuer name:- (organization name):

The name of the person who issued the certificate.

Validity period:-

* Validity period means from which date to date and time to time it will have. validity of certificate.

Subject name:-

* It is name of the person to whom you are giving the certificates.

Public key information:-

In order to encrypt (or) decrypt the msg, the user (subject) will be using the public key information.

Issue unique ID & subject unique id:-

Every issuer have a unique id and every subject have unique id.

Extensions:-

* If you want to add any descriptions, These extensions are optional
* This may (or) may not be included.

7] public key infrastructure:-

* It is standard which is followed for managing, storing and revoking the digital certificate
* It follows asymmetric key cryptography.
* It includes the:-
  message digests (Integrity)
  Digital signature (Authentication, Non-Repudiation)
  encryption services (confidentiality).

Architecture of PKI:-

* There are four parts.
  1) Certificate Repository
  2) Entity
  3) Registration Authority (RA)
  4) certificate Authority (CA).

1) certificate Repository:-

* storing the certificates and information of certificates.
* certificates ID, the name, owner all the information stored in certificate Repository.

2) entity:-

It is the user of PKI, it can be a single person, organization, Router etc...

3) Registration Authority:-

* It is used for Registration and verification
* It is a function for certificate enrollment used in public key infrastructures.

4) certificate Authority:-

* A trusted organization that issues public key certificates is known as certificate Authority.
* It can be likened to a notary public.

UNIT – IV

Transport-level Security: Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH) **Wireless Network Security**: Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN, IEEE 802.11i Wireless LAN Security

Transport layer security:-
* It is refined in RFC 2246 (request for comments).
* TLS is needed for providing security in Transport layer.
* When the data is travelling from transport layer to next layer, we need to provide a security to the data.
* It is derived from SSL.
* It provides a secured connection blw client & server (i.e., no hacker (or) third party can interfrer in blw server and client).
* It is used by http, smtp.

Working:-
* It uses client server handshake mechanism. (i.e., handshake blw the client and server).
* First, we have to establish the connection after that the key exchange blw client and server (By diffie hellman key exchange algorithm).
* once the key exchange is successful after TLS protocol will open an encryption channel (by RC4/IDEA/DES algorithm).
* It also ensures that the messages are not altered. It can be done by any of the hashing algorithm (changed) like MD5/SHA Algorithm
* RFC 2246 is similar to SSL V3 (SSL version 3)

9] Web security Considerations:-

* whenever we are sending the data from one user to another user, always attacks will be there.
* In order to escape from the attacker we need security.
* security is required for websites.
* There are six security considerations:-
  1) updated softwares
  2) Beware of SQL injections
  3) cross site scripting (xss)
  4) Error message
  5] Data validation
  6] passwords.

1) updated software :-

* Let us you need always update your softwares for example:- once you joining the office, if you wont to access the some of the office websites on your mobile, they will ask you that the phone should be updated time to time.

2] Beware of SQL injections:-

* SQL injections is nothing but that the data is inserting in tables (i.e., rows (or) columns).
* The hacker will inserting the data in the form of rows and columns to disturb the integrity of the data.

3] cross site scripting (xss):-

* It is also called as xss.
* Attacker will send site scripting to your website, like any data is related into the client.

ex:- Forms.

4) Error Message:-

* when we are giving the password & username to the any website. Sometimes we are forget the password. In that case we will get error message like your password and username is wrong.
* In that cases the attacker will not have clarity wheather the attacker will enter the wrong password (or) wrong username.

5] Data validation:-

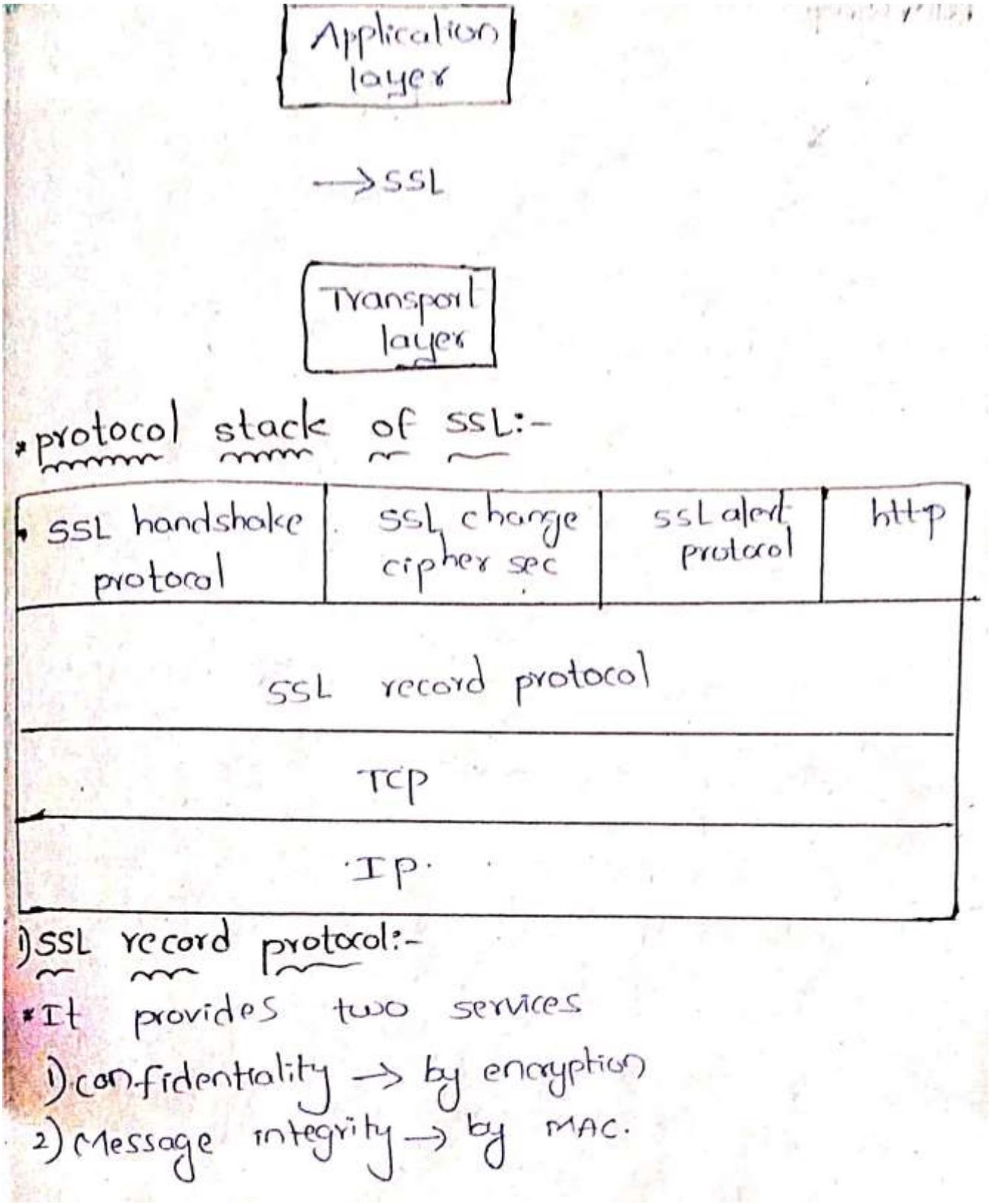
* Data validation should be done in both client side and server side.

6] passwords:-

* The passwords are always should be strong (minimum 8 letters should be there).
* so, the attacker will not be able to get the password.

3] Secure Socket Layer:-

* It is used to provide security for communication blw two users.
* It ensures integrity, authentication and confidentiality.
* It lies blw application layer and transport layer of TCP/IP protocol.



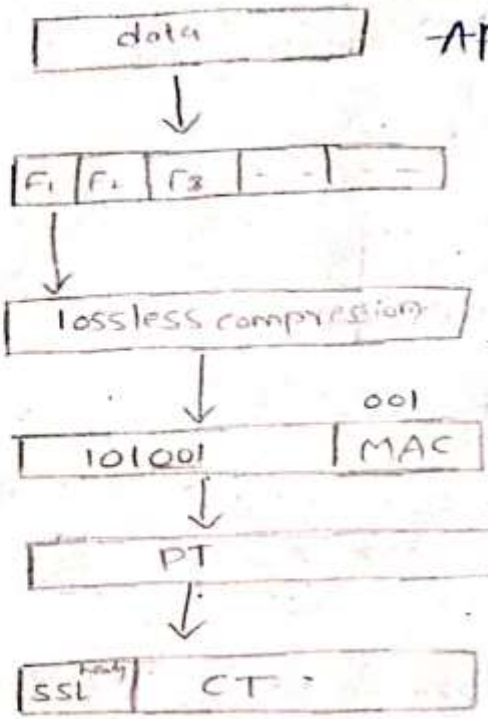
* protocol stack of SSL:-

SSL handshake protocol	SSL change cipher spec	SSL alert protocol	http
SSL record protocol			
TCP			
IP			

1) SSL record protocol:-

* It provides two services
  1) confidentiality → by encryption
  2) Message integrity → by MAC.

Working:-



* The data in the application layer is divided into no. of fragments based on the size of the data. This process is known as fragmentation.
* The size of the each fragment is 2^{14} byte block.
* For each and every fragment there is a separate process.
* Take one fragment and do that data compression means you have to reduce the size of data.
* This compression has to be lossless compression
* Cale have to calculate the MAC code of the data and add this MAC code at the end of the data
* For the complete data block do the encryption.

* Encryption is done ~~for~~ to ensure the confidentiality.
* Before the encryption, the data can be called as plain text.
* After encryption, we will get the corresponding cipher text.
* We have to add SSL Header at the beginning of the cipher text.

SSL Handshake protocol:-

* SSL handshake protocol is used to ensure Authentication
* Most complicated part in SSL
* It will do key exchange blw client and server.

Working:-

1. Connection establishment with server
2. key exchange from server to client } authentication
3. key exchange from client to server
4. Handshake done from server.

SSL change cipher protocol:-

* It has only one message and size of the one message is 1 byte.
* It will copy the pending state into current state.

SSL Alert protocol:-

* whatever alerts related to SSL are sent to clients.
* Alerts is nthg but notifications.

*It has two bytes :- i) byte 1 & ii) byte 2.

* Byte 1 can have the value as ① or ②
value ① indicates the warning, if we ignore the warning then value ② becomes the fatal error. Then you need to stop it completely.

* Byte 2 specifies the type of error.

+Http:-

* +Hypertext transfer protocol is an application layer protocol
* +HTTP is a synchronous protocol, which in this case means that after a client sends a request to a server.
*It waits for a single response.
* The server can only respond to requests.

TCP:-
Transmission control protocol works with the internet protcol (IP) which defines how computers send packets of data to each other.

IP:-
* Internet protocol is the set of rules (ruling) governing the format of data sent via the internet (or) local network.

HTTPS (Hyper text transfer protocol secure):-

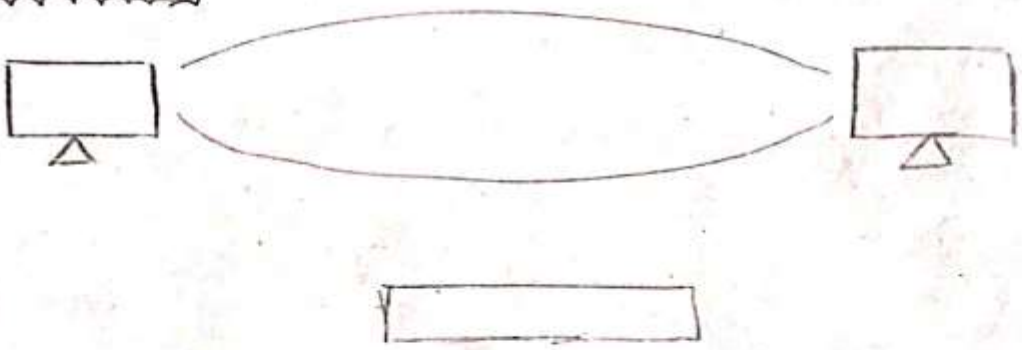
*It is a combination of http and ssL.
*It has an additional layer of security provided by TLS/SSL
* It is more secured compared to http
Eg:- websites starting with (https://)
*In http data is in the form of plaintext only.
*In https data is in the form of plaintext and cipher text. (i.e., encryption and decryption takes place).
*It belongs to transport layer protocol.
* It is heavier that http because it has an additional layer of security.
* It runs on port number 443 of server. and http runs on port number 80 of server
*It uses a certificate Authority (CA).
*It works on asymmetric key pkI and it uses (2) different keys
1) private key:- It is avaliable on the web server and managed by owner of the server.
2) public key:- It is avaliable to everyone (client and server can access)

* HTTPS is slower than http.
* The main usage of https are Banking websites, login credentials.

5) SSH protocol (secure shell):-

*It is a protocol for operating network services over an unsecured network.
*It is alternative to Telnet, FTP etc... (unsecured Protocols)
*It uses client server Architecture.
*It follows asymmetric key cryptography.
Two keys:- Encryption => public key
decryption => Private key.
*It provides confidentiality and Integrity.

Working:-



*client sends the request to the server.
*server will check the authentication of client with the public key.
*If public is matched then it will generate random string.
*The random string will send to the client, before sending to the client, the random string is encrypted and server sends the cipher text to

the client.
* The client will decrypt the cipher text with the help of private key.
* Again the decrypted data is sent back to the server.
* If client sent the correct decrypted data to the server, then server will believe that, the client is a trusted client.
* The authentication of client is conformed at the server side then SSTL Tunnel is created.
* SSTL Tunnel is a channel for communication blw client and server.
* No body can enter into the SSTL Tunnel to steal the data. means it is very secure.

PART-B

Wireless security:-
* protecting wireless n/w from unauthorised users
Ex:- Wifi, bluetooth etc...
* It is very complex in working.

factors contributing to risks in wireless n/w:-
- channel
- mobility
- Resources
- Accessibility.

*wireless n/w Threats:-
1) Malicious Association:- A wireless devices is configured in such a way that, to the user it will appears as a trusted device. But actually it is not a trusted device.

* The user will connect to it and all the data will be stolen by third party.

2) Adhoc network:-

* It is a wireless device which is not having the common access point (x) to communicate.

* For security purpose there is no chance.

3) Non-Traditional network:-

It is nothing but bluetooth, barcode, PDAs

* These are the wireless networks, so don't have much security.

4) Identity Theft:-

* For everything there is need of identity. that means everything have a unique barcode.

* The attacker will observe the network traffic, he will steal (or) findout the MAC address of the computer.

5) network injection:-

* Without the user notice, the data will be injected and this network injection mainly happens in the systems are exposed to non filtered network traffic.

Measures for wireless security:-

1. signal hiding Techniques. SSID → encryptions → protocols → firewalls
2. Encryption and authentication protocols.
3. use antivirus sw and firewalls
4. change Routers pre-set password
5. Allow only specific computers to access to your wireless n/w

UNIT – V

E-Mail Security: Pretty Good Privacy, S/MIME IP Security: IP Security overview, IP Security architecture, Authentication Header, Encapsulating security payload, Combining security associations, Internet Key Exchange **Case Studies on Cryptography and security**: Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability.

* What is e-Mail Security :-

as a platform for delivering viruses, spam and phishing attacks, email is prominent with attackers.

To manipulate users into disclosing personal information they use misleading texts, culminating in identity fraud. they tempt users to user register files or click URL's on users computer that allows like email malware.

for threats anyone wants to penetrate network architecture. and hack sensitive customer information. e-mail is often a key entry point.

the characteristics of email security are often flexible and according to the user requirements

* pretty good privacy: (PGP)

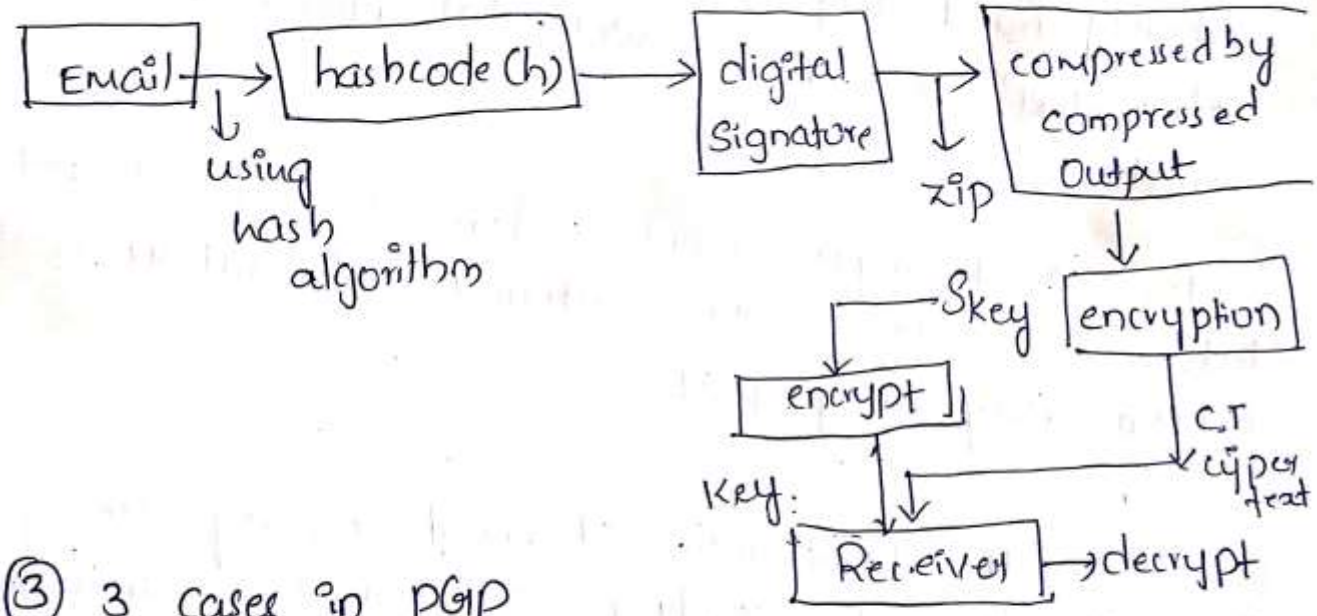
- provide email security.
- used for siging, encryption, decryption ... of texts, files, directories -- (data in emails)

* Techniques used in PGP :-

1. Hashing :- MD5, SHA
2. Data compression
3. Symmetric key cryptography
4. Asymmetric key cryptography

* Services of PGP :-

(i) Authentication
(ii) Confidentiality

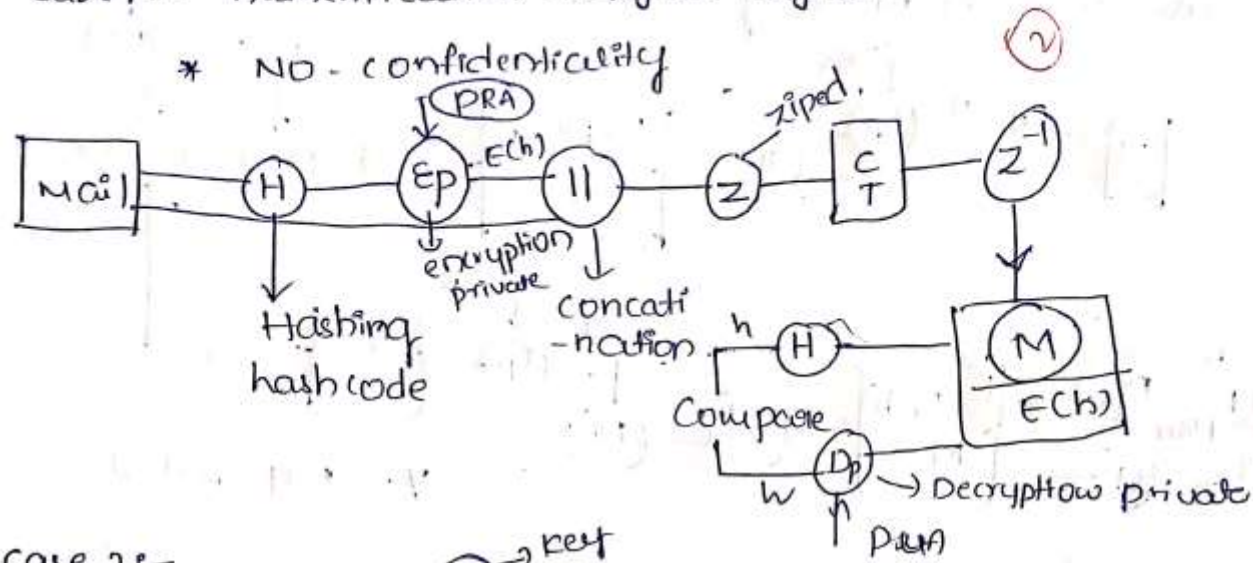


(3) 3 cases in PGP

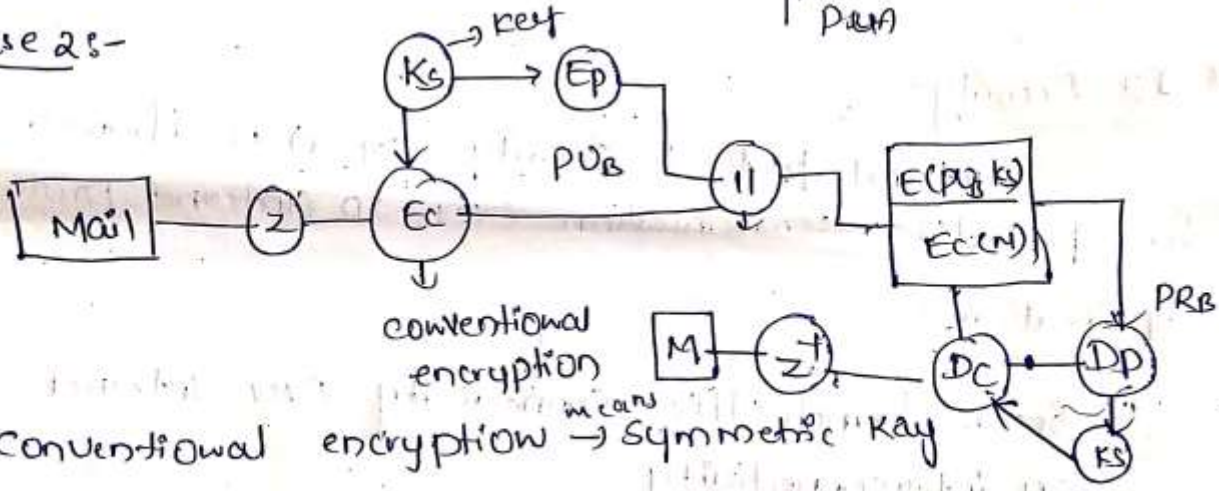
(i) Authentication - only
2 confidentiality -
3. Authentication + confidentiality

Case 1:- Authentication + digital Signature.

* NO - confidentiality



Case 2:-



* Conventional encryption means Symmetric Key

Z - zip u r information

EC - conventional encryption

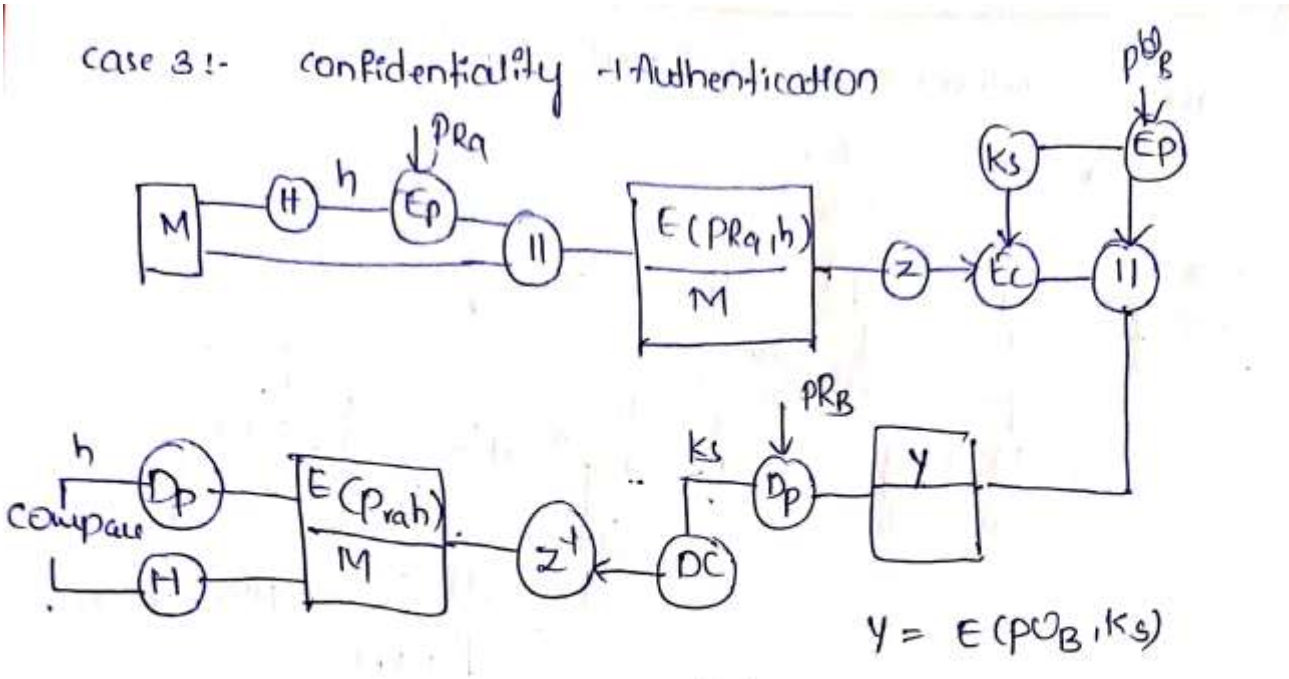
Ks - Key for encryption with Ep using PU_B. (public key of B)

(||) - concatination

Z^{-1} decompression of your data

In second case both data and key are encrypted.

Dc - conventional Decryption.



* Ip Security :-

Internet protocol Security (ipsec) is a framework for protecting communication over Ip (internet protocol)

Applications :-

1. Secure branch offic connecticity over internet. (or) interconnecticity

   Eg :- banks Sectors.

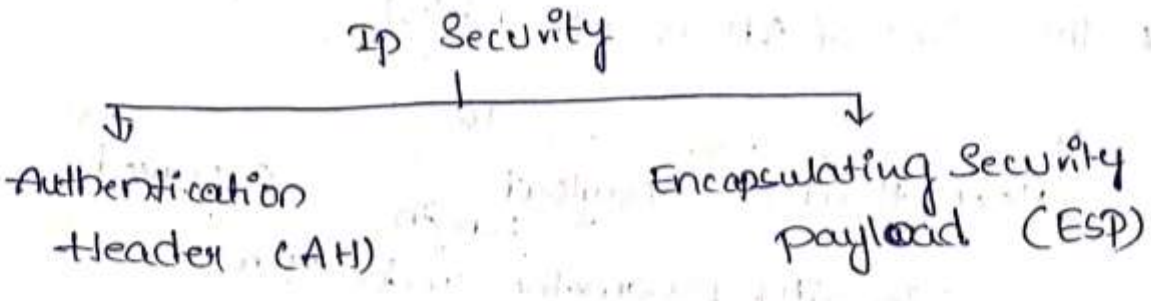
2. Secure remote access over internet

3. enchancing electronic commerce Security

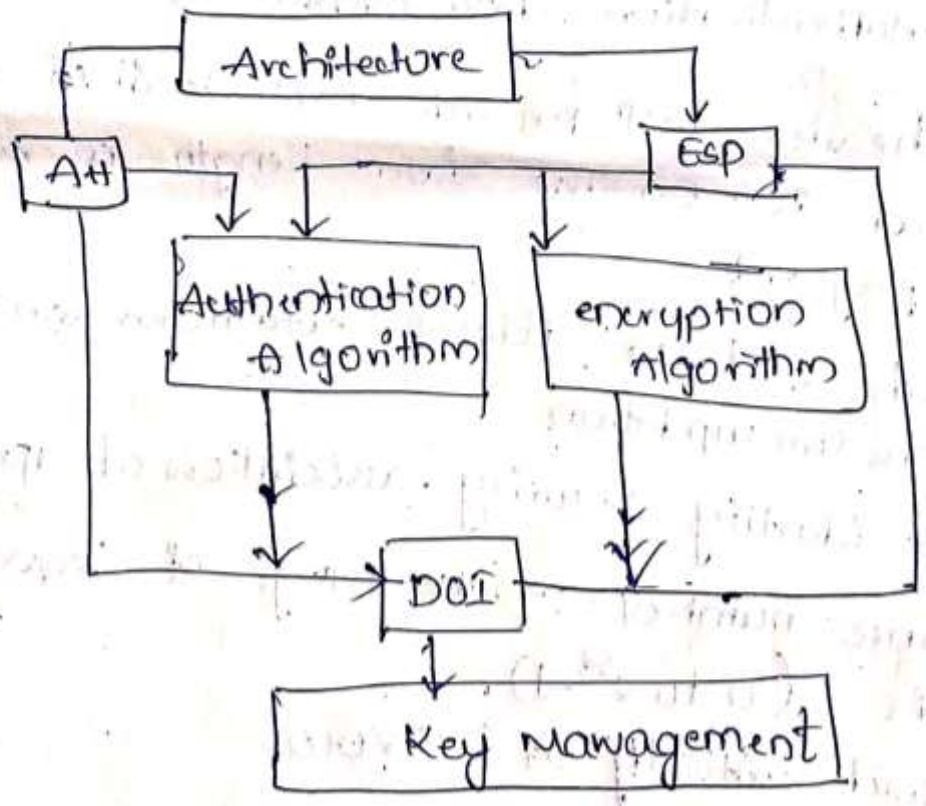
   Eg :- e-commerce Secure transactions

Ip Security architecture :- (5)

Ip security architecture is combination of two protocols



Architecture :-

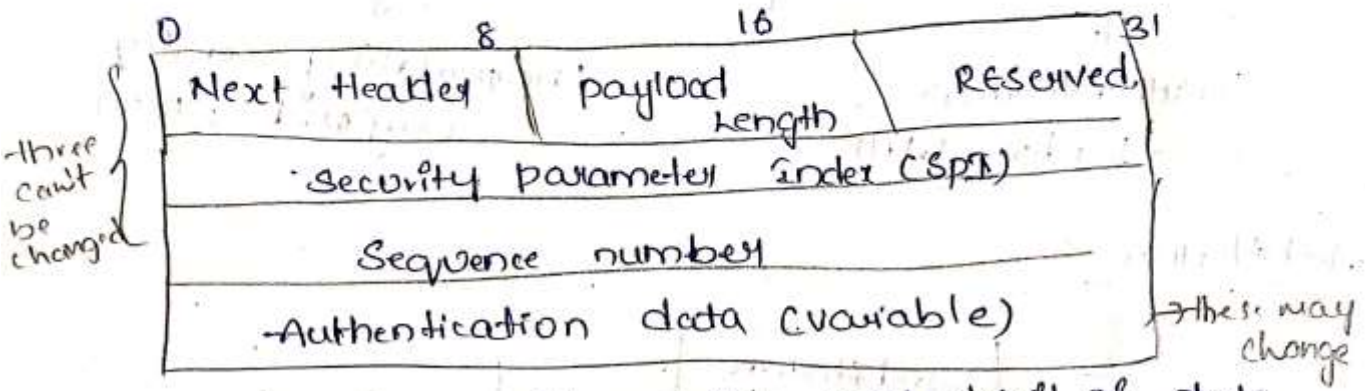


* DOI :- Domain of interpretation
  ↳ it will have id's of all the approved authentication and encryption Algorithms

* Authentication Header :- (AH)

authentication Header for Integrity and authentication

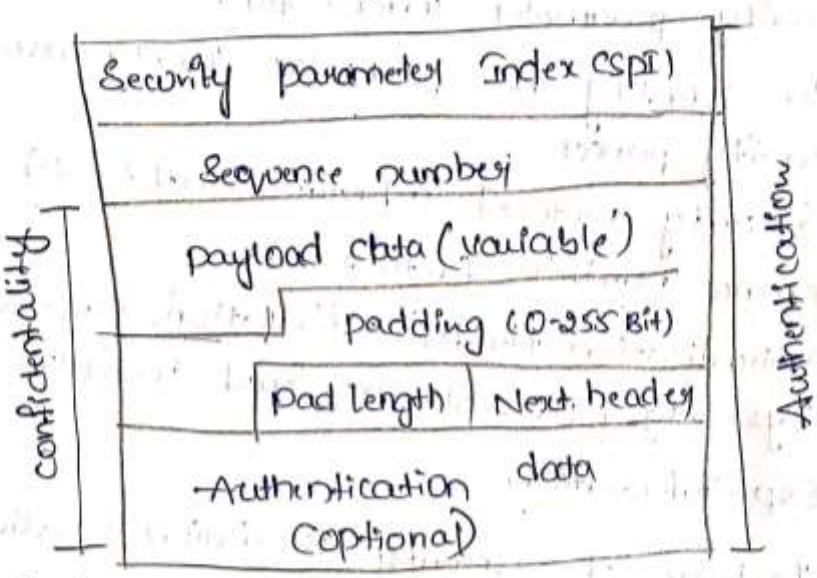
* the size of AH is (0-31 bits)



* Next header will provide next detail of data
* payload is original data length is measured by payload
* Reserved used for future extentions or new versions or updation
* SPI → identify security association of packet
* Sequence number :- the range of sequence number is (0 to $2^{32}-1$). and initially it is zero.
* Authentication (data) :- it contain ICV (or) MAC of packet
* ICV -! (Integrity check value) :- if there are any unwanted modification are changes done to data that determined.

* Encapsulating Security payload :-

(4)



* payload data → original data.
* padding means adding extra bit to original data
* pad length :- no. of bits at the end. how many bits are added.
* Authentication data is (Optional)

* Combining Security associations :-

* Security Associations :- (SA)

1. Security association is a contract shared between all the entities before the start of communication
2. SA specifies the protocols to be used in Ipsec to ensure security.

1 Parameters of Security associations:-

i. Security parameter Index (SPI) :-

↳ to identify the particular security association of security packet

2. ↳ Security protocol Identifier (AH & ESP)

3. Sequence number (0 to $2^{32}-1$)

4. Authentication Header informations : means what are Keys, Alg's, protocols are used in (AHI)

5. Esp information

6. life time of security association → validity on life time of security.

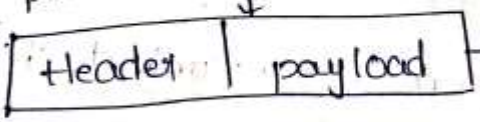
7. Ipsec protocol modes :- 2 modes

Transport mode, tunnel mode

① Transport mode :-

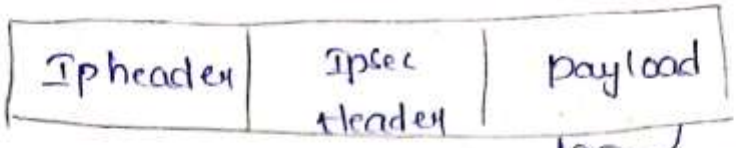
payload → encrypted
Header → not encrypted

* initially packets are



* a packet will have both Header not encrypted payload is encrypted

later in transport mode we insert Ipsec header in b/w



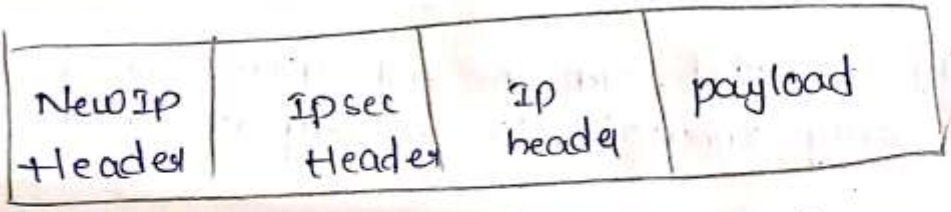
⑤

* direct host to host communication

* Tunnel Mode:-

payload } both are encrypted
Header

(ie: entire packet is encrypted as a result, new ip header is generated)



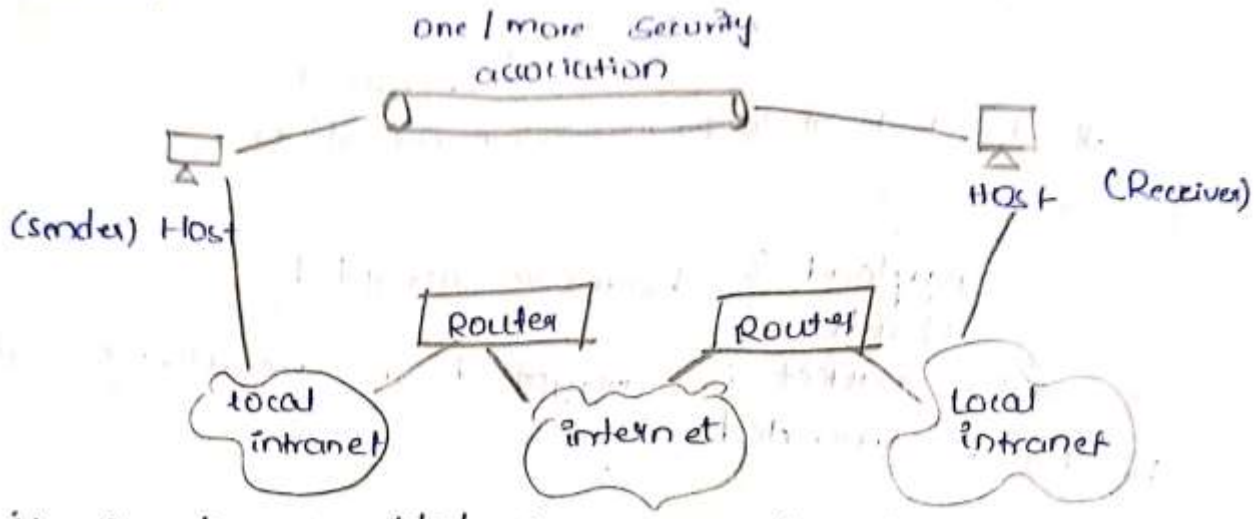
- Gateway to gateway communication is done
  - for sender
  - Receiver.

* Combining Security associations:-

with an individual SA's we can implements either (AH/ESP) but not both.

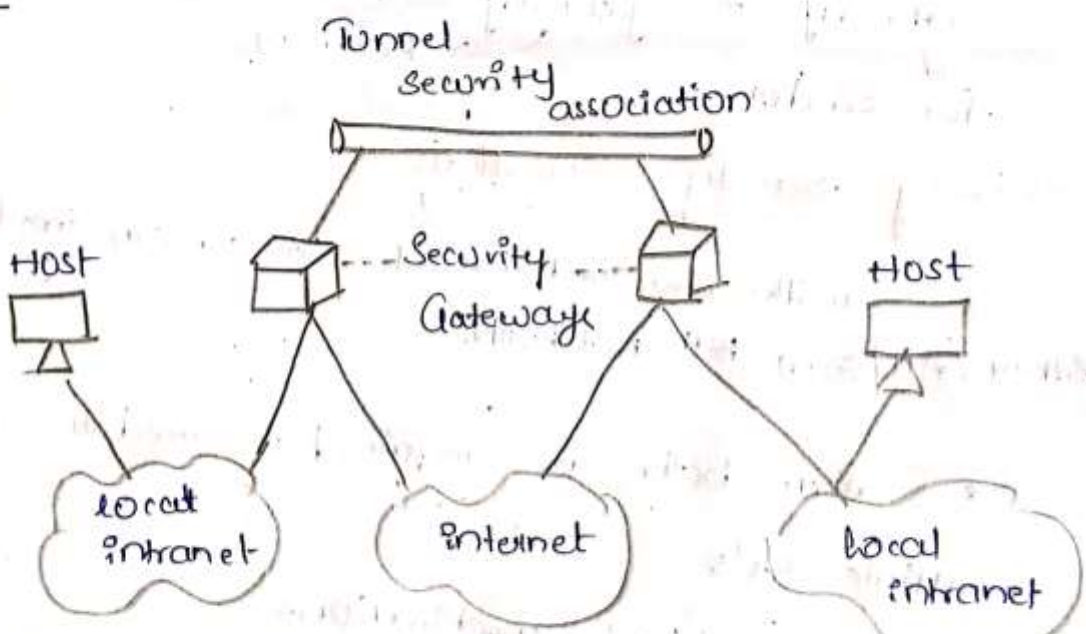
* when both are required we need to combine multiple SA's.
* we have '4' combinations

case 1 :-



i) Security provided bleb the end systems, because host is directly connected to security association.

case 2 :-

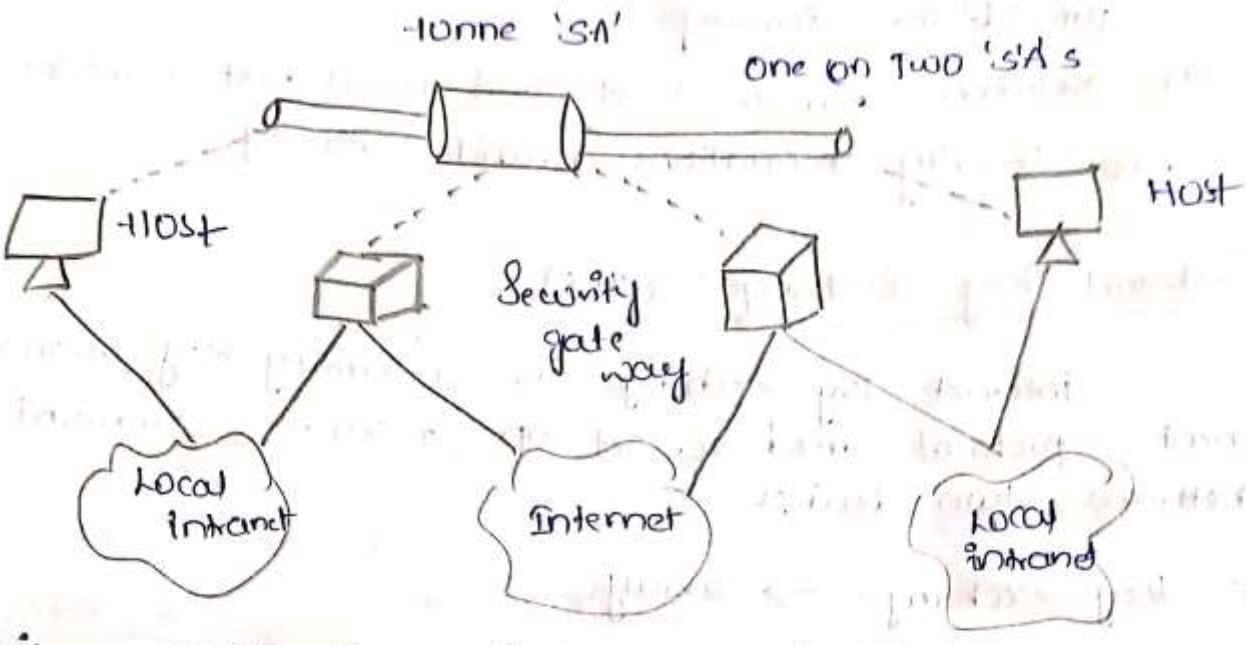


i) Here we use single tunnel Security association

But here 'SA' connected to the gateways connected to host local (intranet)

(iii) mostly used in VPN. VPN

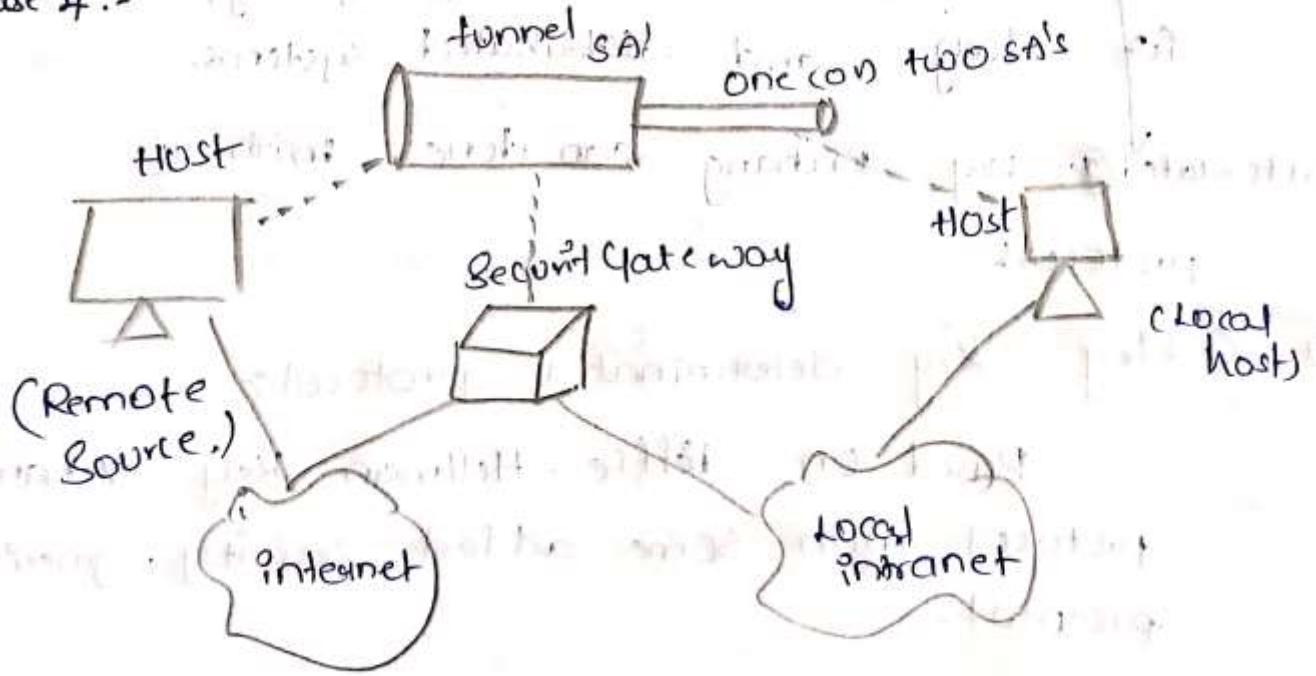
Case 3 :-



(i) combination of case 1 and case 2

(ii) tunnel - security for Gateways + Security association to end to end systems also

Case 4 :-



(i) used in remote sensors

(ii) between remote host and Gateway → tunnel mode provide the security

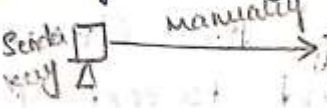
(iii) between remote host and local host → one on two security associations provide security.

* Internet Key Exchange :- (IKE)

Internet key exchange is a security key management protocol used to set up a secure communication between two devices

* Key exchange → 2ways

(i) Manual :- manually configure each system, small, and static.



→ system admins can do

(ii) Automated :-

for large and distributed systems.

on demand creation of keys

automated key Exchang can done with: (2)

protocols

(i) Oakley key determination protocol :-

Based on diffie-Hellman key exchange protocol with some added security, generic protocol.

② ISAKMP :- (Internet Security association Key management protocol) :- ④

- provide a framework for key exchange and provides protocols specific support

* ISAKmp is done in two phases

phase 1 :-

(i) exchange of proposals for security services. (encryption algorithm, authentication alg^n etc)

- when both ends of the tunnel agree to accept a set of security parameter then phase ①

* In phase ① we have two modes those are

(i) main mode
(ii) aggressive mode

phase ②

once participants established a secured channel in phase ① they move to phase ② - here security association are negotiated

- decided to use 'AH'/Esp and also select with algorithm. to use
- phase ② always operates in ② quick mode.

* S/MIME protocol:-

* Mime protocol:- "multipurpose internet mail extention"
* previously, emails could be sent only in NVT - 7 bit ascii format.
  eg: audio, / video / images etc could not be sent)
  -! mime is introduced.
  ↓
  add on which allows us to transfer non-Ascii data over mail (other type of data)

Smime: Secure mime, extention to mime protocol.

1) encrypts emails and provide security
2) allows us to digitally sign on our email
3) Uses asymmetric key cryptography

functions of S/mime

(i) Authentication (ii) message integrity
(iii) non-Repudiation - can't deny the message
(iv) privacy
(v) data security

(8)

* Security services of S/Mime :-

1) Security of services of S/mime are

i) Digital Signature

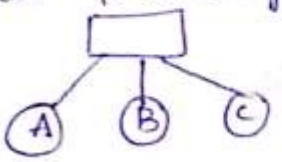
ii) Message encryption. → (write in detail about both for exam)

* Case Studies On Cryptography and Security :-

i) Secure Multiparty calculation →

when data is distributed in network, it provides a protocol : so that no individual can see other parties data

In General it enable data scientists and analysis to compute data privately without exposing it.



Example :- if we want calculate the average salary of (3) employees then

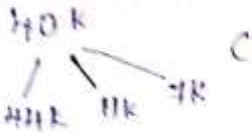
without - this protocol - data should be revealed

with this protocol - data need not be reveled

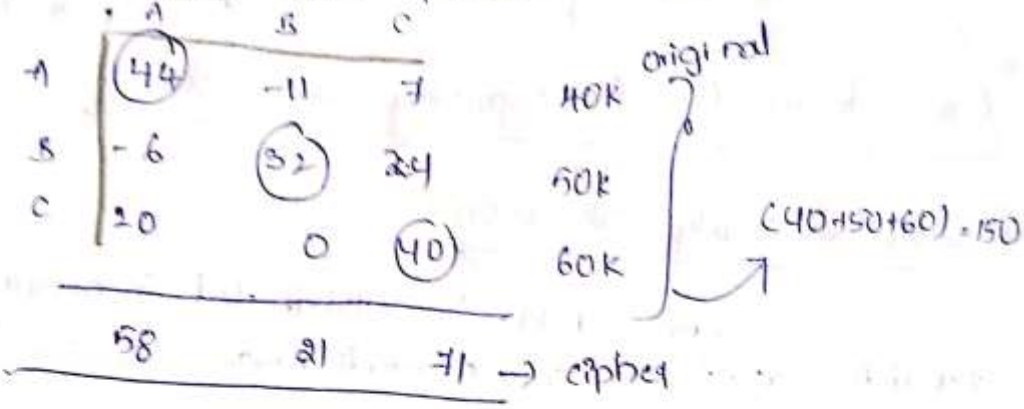
functionality F(A,B,C) = Average (A,B,C)

We have calculate average salary of A,B,C without divided into three parts.

If A's Salary is 40K then using additive sharing 40K is divided into (3) parts



and B & C also same process



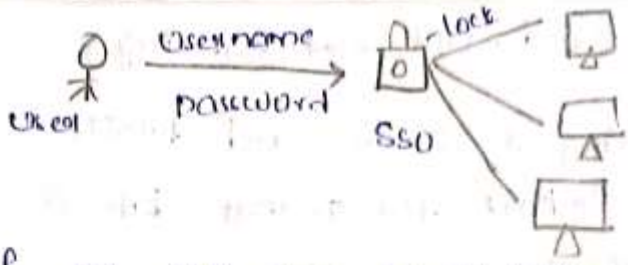
total salary = 58 + 21 + 71 = 150

average = 150/3 = 50.

* Single Sign On :- (SSO)

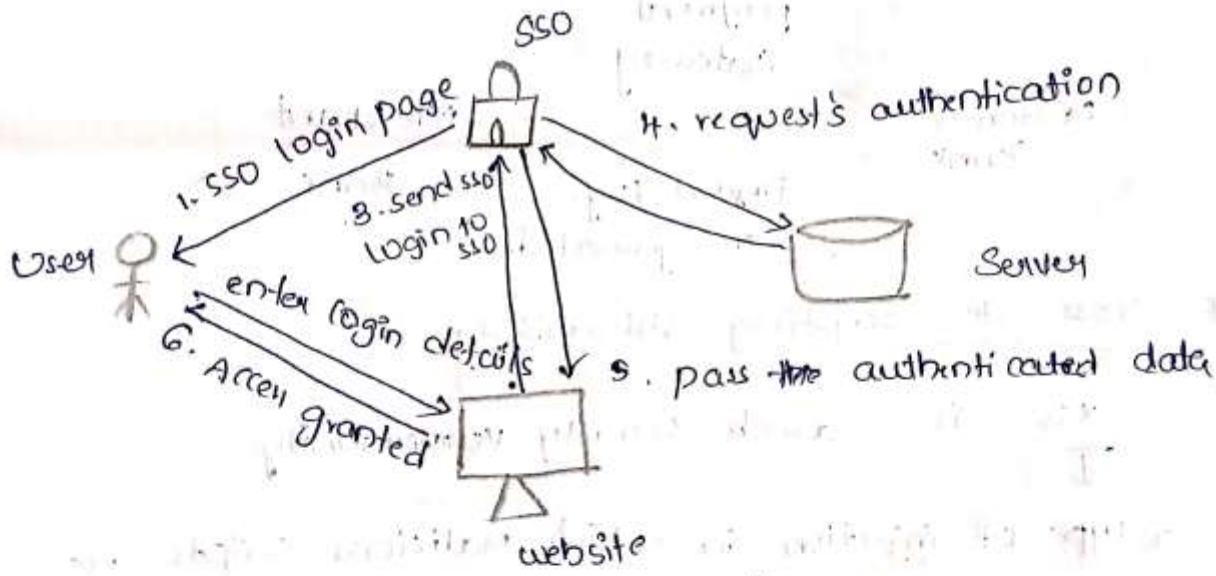
- SSO in an authentication Scheme where users can securely gain access to multiple applications and website only with single user name and password.

Example :- One Google account it provide services like Gmail, docs, drives etc.



(9)

* If no SSO then every time you enter User id, and password every-time
* With SSO we no need to give (or enter id & password different web sites
- It is very important to protect SSO. for that we we used MFA (multifactor authentication)



* Secure inter branch payment transactions :-

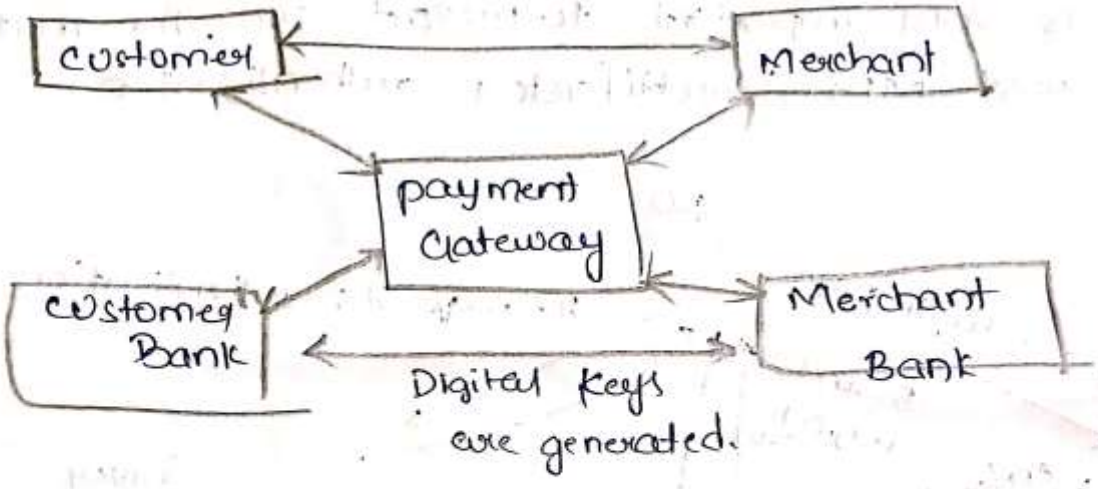
done with the help of Secure electronic transaction (SET)

SET protocol :- this protocol ensures security and integrity of electronic transactions

(credit and debit card, UPI, Net banking)

* SET restricts revealing of credit card details to merchants (amazon, flipkart etc) so that data is protected from hackers.

- implemented with help of digital signature.



* Cross site Scripting Vulnerability:-

XSS is a web security vulnerability

↓

a type of injection in which malicious scripts are injected into trusted websites

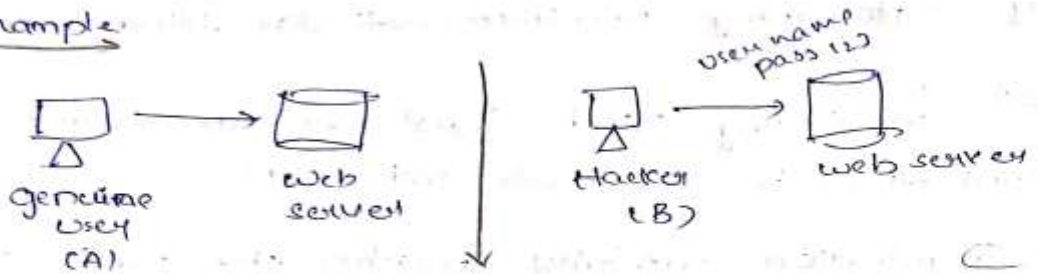
examples:- Data enters into website / application through an untrusted sources - (in form of a web request)

↓

(javascript, html, etc)

- XSS vulnerabilities are easy to spot and they have high impact on your website.

Example:



* Electronic voting :-

An electronic voting system work as follows before voting a voter must first communicate with a registration authority. who provides the voter with a token. this token is used to vote.

Goals of electronic voting

3) correctness :-

1. only authorized parties can vote ie; register voters.
2. no voters vote more than once
3. no voter can replace other votes
4. the party in charge of tabulation cannot change the outcome

(ii) Verifiability :- Universal (or) private

(iii) Uses anonymity (iv) Receipt Freeness

using cryptography primitive particulars, blind, signatures

Method 1 → (using Blind Signatures) We assume that communication is anonymous and secure.

(i) registration authority publishes the public key 'pk'

(ii) voter picks a random number that become their ID, and append the candidate.

(iii) voter sends their personal information along with blinded versions of the tokens.

(iv) the voter unblinds all the signatures.

* Method (2) cryptography counters

If A and B are cryptographic counters consists of three algorithms

(i) Gen: generates $(pk, sk, s_0) \in \{0,1\}^* \times S_0$ is the initial state of the encrypted counter

(ii) Decrypt: $Dec(s, sk)$ outputs one of $0, \ldots, B$ and $Dec(s_0, sk) = 0$

(iii) Increment : Inc (s) satisfies

Dec (Inc(s)) = Dec(s) + 1 (pk, sk) have been omitted for clarity

Definition :- A B-counter is (t, ε)-secure if for all t-time algorithm A.

$$Pr[A(pk, s) = Dec(s, sk) \mid (pk, st, s_0)$$

Method 3 Mix nets:

In this scheme, each user encrypts their vote (using the public key of a decryption authority) and gives the it to a mixer

the mixer then outputs a permutations of the encrypted votes along with a proof that it has been mixed correctly

for extra security, several mixers can be used ie: the first mixer passes its output to a second mixer who, passes its output to a third mixer and so on.

Using a Neff mix, the proof requires about 8n exponentiations, where 'n' is the no. of voters