CRYPTOGRAPHY AND NETWORK SECURITY

Syllabus

1. Attacks on Computer & Computer Security – Introduction, Need for Security, Security Approaches, principles of Security, Types of Attack.

2. Cryptography : Concept and Techniques - Introduction, plain Text, cipher Text, Substitution Techniques, Encryption and Decryption, Symmetric and Assymmetric key, Key Range and Key size.

3. Symmetric key Algorithm - Introduction, Algo. Types and Modes, Overview of Symmetric key Cryptography, DES( ), IDEA, RC5, Algo.

4. Asymmetric Key -Algo, Digital Signature and RSA - Intro, RSA Algo, Basic Concept of Message Digest and Hash fn.

5. Internet Security protocols, User Authentication - Basic Concepts, SSL protocols, Authentication Basic, Password, Token, Certificate Based Authentication, Biometric.

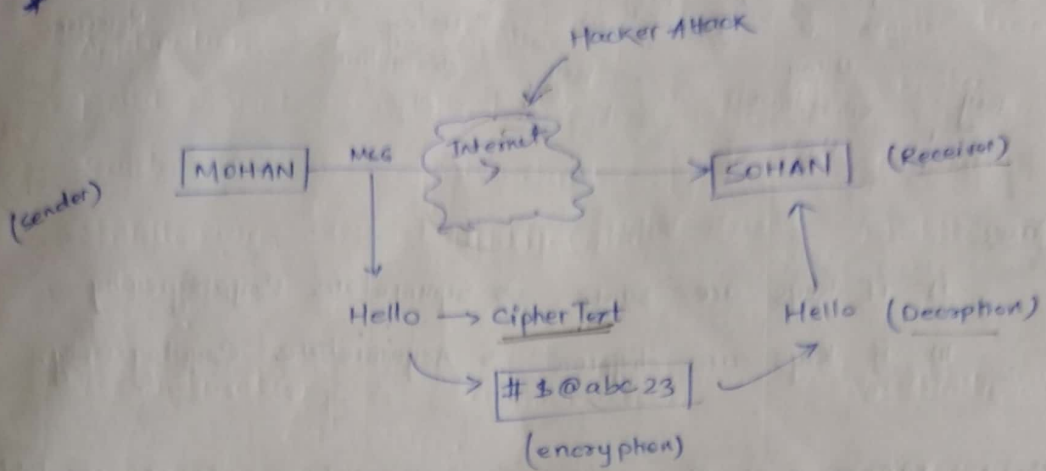
6. Electronic Mail Security - Basics Mail Security, pretty good privacy, S/MIME.

7. Firewall - Introduction, Types of firewall, Firewall configuration, DMZ Network.

08/02/2023

CRYPTOGRAPHY

* Sol



Cryptography : The Art of protecting information by Transforming it into an unreadable format.

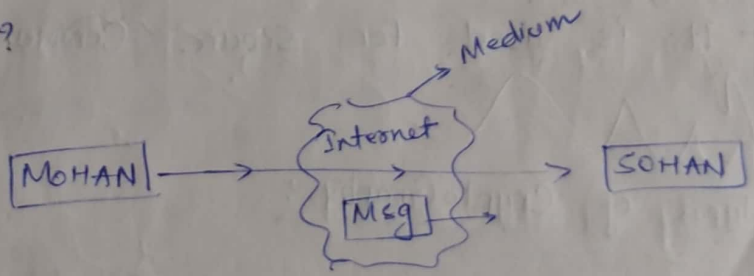
OR

Method of protecting information and communications Through the use of codes so that only those for whom the information is intended can read and process it.

OR

↳ Now Generally Cryptography is About Constructing and Analyzing protocols that prevent third parties or the public for reading private Messages.

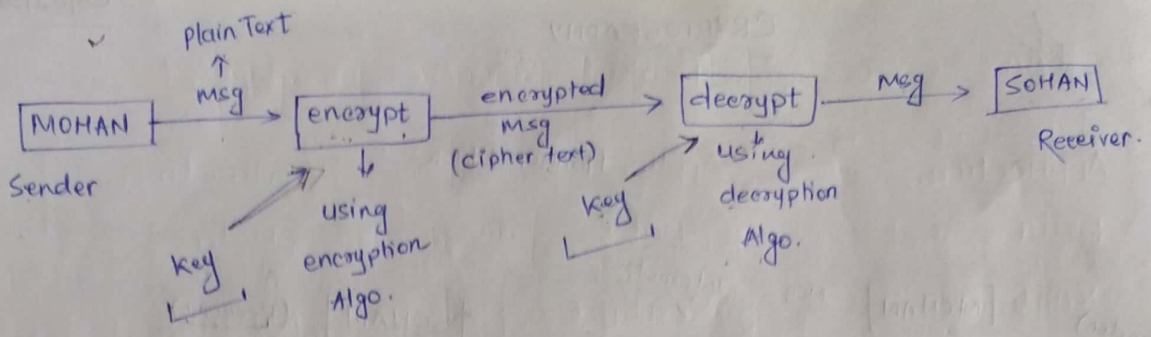
Q. Is it Secure ?



A1. No, Because,

Attackers / 3rd parties May corrupt / change our data and may Misuse it Also.

Thus, To provide Security and protect the Valuable information, We can use CryptoGraphy.



Case:

i) if keys are same → Symmetric Cryptography

ii) if keys are different → Asymmetric Cryptography.

Encryption:- • process of Transforming information from readable to unreadable.

• Encryption Algo. are used to encrypt the information on data.

Decryption:- • Process of Transforming data/info from unreadable to readable format.

• Decryption Algo. are used to decrypt the data.

Key :- String of bits used by Cryptographic Algo. to transform plain-Text to Cipher text and vice versa.

- It is used for Secure Communication.

Types of CryptoGraphy :

1. Symmetric Cryptography : It is the simplest kind of Encryption Technique that involves only [1 Key] to encrypt and decrypt (cipher and decipher) information.

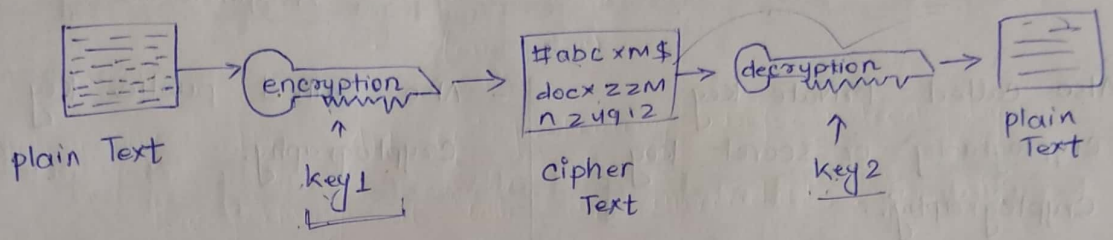
- It is also called secret key / private key Cryptography.
- The Most Popular Symmetric Key Cryptography is DES. (Data Encryption System).

2) Asymmetric key Cryptography :-

- It is also called public key Cryptography.
- It uses [two keys] i.e. A pair of keys for encryption and decryption.

  public key → known for everyone
  private key → known only to that particular person.

eg:



Note → A Message that is encrypted using a public key can only be decrypted using a private key.

Also,
A Message that is encrypted using a private key can only be decrypted using a public key.

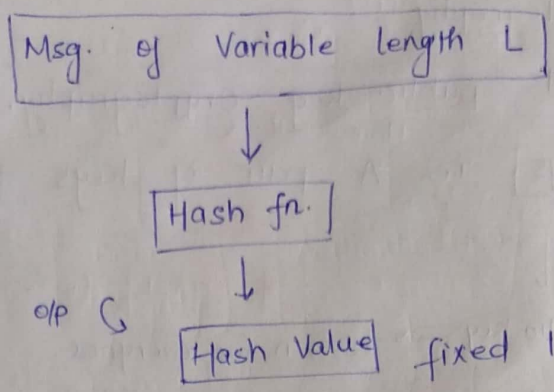
- Popular Asymmetric Key Algo → RSA, DSA, Elliptic curve etc

3) Hash functions :-

- There is no uses of key in the concept/algo.
- Takes in variable length size Message and gives fixed size [output]

  Hash code or
  Hash Value.

- Hash code makes it impossible for the Context of plain text to be recovered.
- Many O.S. use Hash functions to encrypt passwords.



Symmetric

- Also called Private key cryptography or secret key Cryptography.
- Only 1 key is used for encryption and decryption.
- performance → Symmetric key Algo. are faster in execution.
- Less complex and less computational power is required.
- Used for the tranfer of bulk data (because ~~bte~~ executes fast).

Assymmetric

- Also called public key cryptography.
- 2 diff. keys (public & private) is used for encryption & decryption.
- slower in Execution.
- More complex and more computational power needed.
- used for secretly exchanging the secret key.

Security Goals :

1) CONFIDENTIALITY : It is the Most Common Aspect of info security.

- It Allows authorized users to access Sensitive & protected data.
- The data sent over the network shouldnot be accessed by unauthorized users/individuals.

- Attacker will try to capture data. To avoid this, various encryption techniques are used to safeguard our data so that even if attackers gaves access, He/she will not be able to decrypt it.

2) INTEGRITY :- It means that changes need to be done only by the Authorized entities and through authorized mechanism, and nobody else should modify our data.

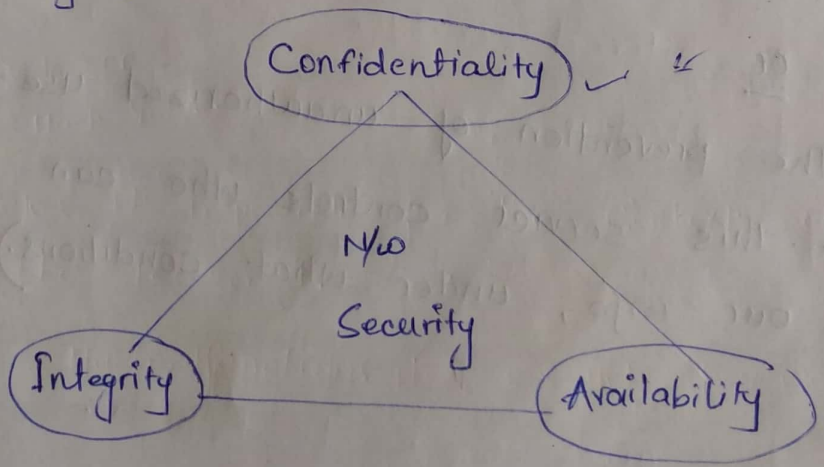
eg:
In a bank, when we deposit/withdraw money, the balance needs to be maintained.

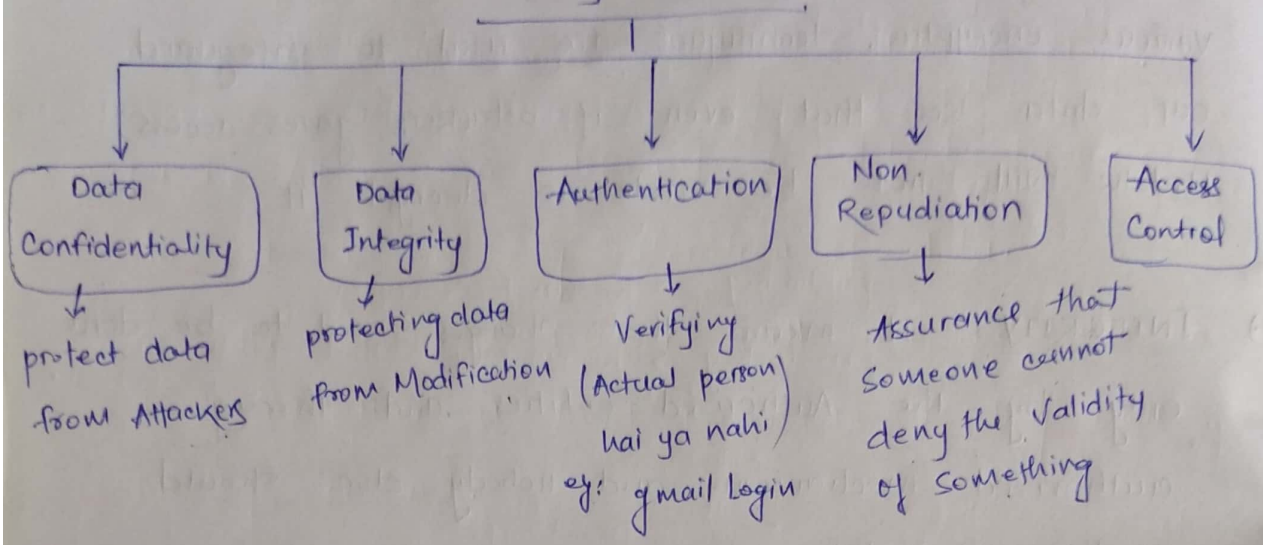
3) Availability: Data must be available to the authorize user.
- Information is useless if we cannot use it.

eg:
What would happen if we cannot access our bank accounts for transaction.

CIA triad in Cryptography

Confidentiality, Integrity, Availability.





Repudiation: denial of truth or validity of something. i.e. act of claiming that something is invalid.

4) Non-Repudiation : It is a service, which provides proof of the origin of data and the integrity of the data.

eg:

A gives ₹100 check to B. and later B deny it. It cannot happen because A will have its proof.

) Access Control :- To whom the Access should be given can be decided.

or

The prevention of unauthorized use of a resource. (i.e. this service controls who can have access to our info, under what conditions.)

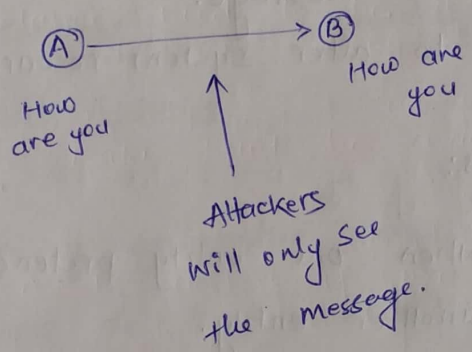
Security Attacks

- Passive Attack
- Active Attack

1) **Passive Attack**: It Attemts to learn or make use of the information from the system, but doesnot affect the system resources.

i.e.
The Attackers will only see the data, but he will not modify it.

eg:



⇒ We can prevent it using better encryption Techniques

Two Types of passive Attack:

1.) **Release of Message Content**:- The Attackers/Hacker will easily be able to understand the data/information

2.) **Traffic Analysis**: If we have encryption protection, an opponent/attacker might still be able to observe the pattern of these message.

- The Attacker could determine the location and identity of communication Host and could observe the frequency and length of the message being exchanged.

- This information might be helpful in guessing the nature of communication that was taking place.

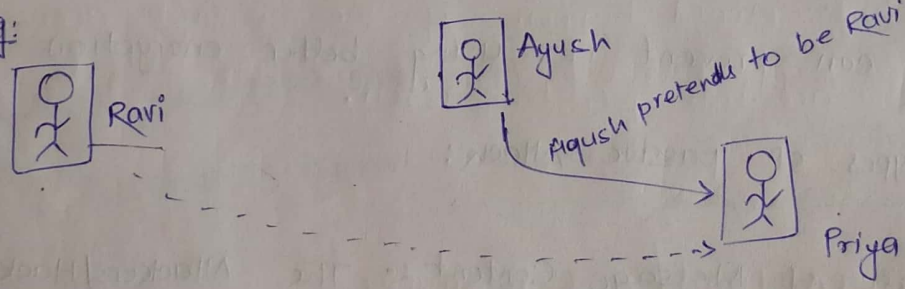
- passive Attacks are difficult ~~to~~ detect because they do-not involve any alteration of data.
  ↳ So, the sender & receiver will not be able to know wheather a third person is reading their message or not.

2) **ACTIVE ATTACK** : Attackers will see the message and modify the message.
It attempts to alter system resources/information.

It is of 4 types:

i) **Masquerade** : When one entity pretends to be another entity.

eg:



(ii) **Modification of Message**:- Some portion of the Message is altered or the message is delayed or reordered to produce an unauthorized ~~attack~~ effect.

eg:

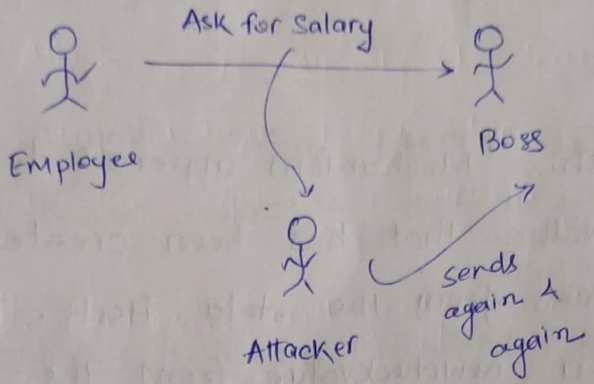
give 100 Rs to John

↓

give 500 Rs to Rakesh.

iii) **Replay** : Involves passive capture of a Message and its subsequent retransmission to produce an unauthorized effect.

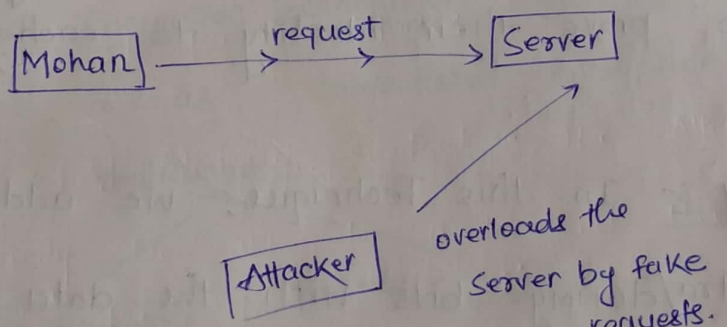
eg:



iv) **Denial of services** :- It prevents normal use of Communication facilities.

eg:

Disruption of an entire network wheather by disabling the network or by overloading it by message so as to degrade performance.



Security Mechanism :-

- Security Mechanism are used to provide security.

1) **Encipherment** :- The use of Mathematical algo. to transform data into a form that is not readily intelligible.

ntext to
er text

2) Digital Signature :- It is means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

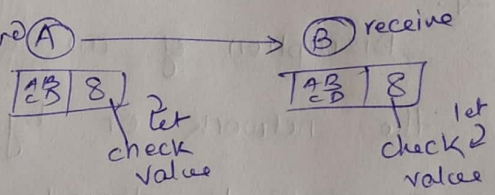
or

we can say it is a mathematical scheme for authentication.

Data Integrity :- This Mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The receiver creates a newcheckvalue from the required data and compares the newly created check-value with the one received.

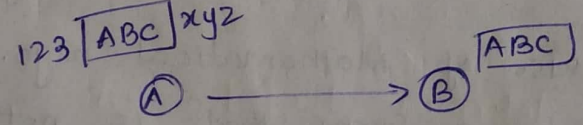
If both the values are same, the integrity of the data has been preserved.

Authentication Exchanged :-



↳ In this Mechanism, Two Entities Exchange some Messages to prove their identity to each other.

Traffic Padding :- In this Technique, we add some extra/dummy bits with the data while encrypting.



6) Routing Control: Means selecting and continuously changing different available ~~roots~~ routes b/w the sender and the receiver. to prevent the attacker from eavesdropping on a particular route.

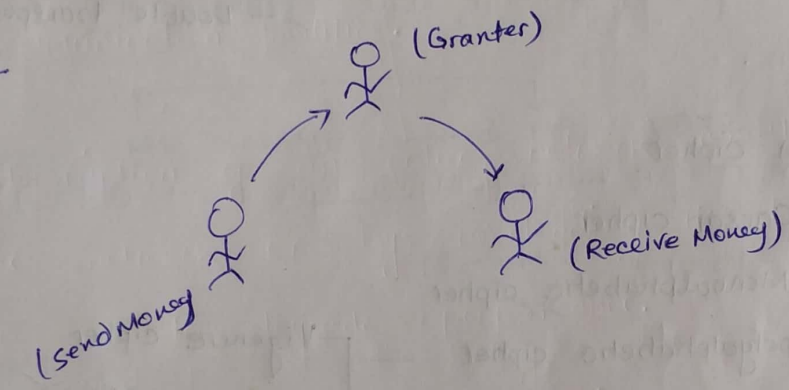
↓

जासुसी

7) Access Control: These Method proves that a user has access right to the data.

8) Notarization :- Means selecting a third trusted party to control the communication b/w two entities. This can be done to prevent repudiation.

eg:



Classical Encryption Techniques :- Symmetric Encryption also reffered to as conventional encryption is of 2 types or 2 techniques.

- Substitution Technique/cipher
- Transposition Technique/cipher

1. Substitution Techniques: It is the one in which the letters of the plain text are replaced by other letters or by numbers or symbols.

eg:

Name → I W P X

2) Transposition Techniques : No Replacement/substitution.

- performing some sort of permutations on the plaintext letters.

i.e. it reorders the symbols.

ie. Rearrangement of the letters of the plain text.

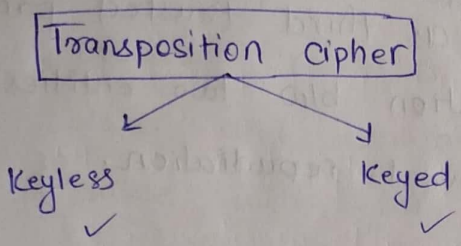
eg:

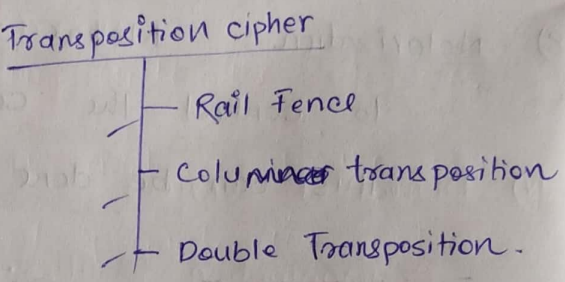
NAME ⟶ EAMN or

MAEN

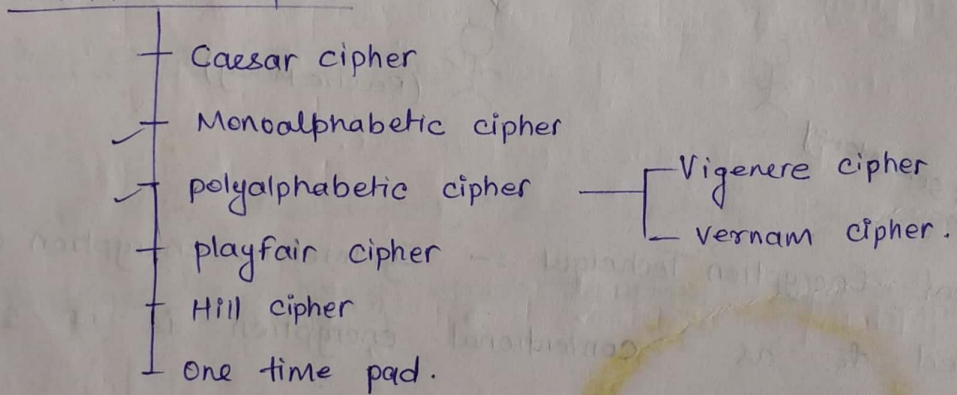
-- — etc.

#





→



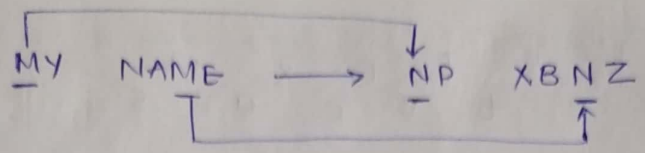
) Monoalphabetic Substitution Ciphers:-

A single cipher Alphabet for each plain text alphabet is used throughout the process.

i.e. fixed substitution

if 'N' ⟶ I will use 'x' then always i will use 'x' only in place of N.

eg:

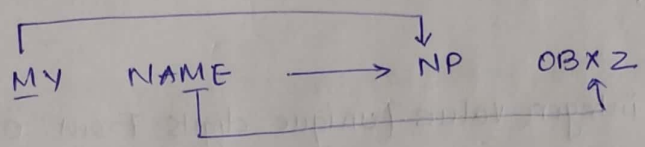


In Monoalphabetic cipher relation b/w a character in the plain text to a symbol in cipher text is always one ~~to~~ one.

2) Polyalphabetic Substitution Cipher:

- There is no fixed substitutions
- Each occurence of a character may have a different substitute.
  i.e. we can use more than 1 substitution for the same letter.

eg:



M → N
  → X
} one to many.

eg:

a → d
  → M.

Transposition Techniques:

1) Rail Fence Technique: In this Technique, the plaintext is written down as a sequence of diagonals and then read off as a sequence of moves.

eg: "all the best for exams" → plain Text

To encrypt this with a rail fence of depth 2, we write the following -

depth 1 → a l h b s f r x m

depth 2 → l t e e t o e a s

encrypted message is :-

ALHBSFRXMLTEETOEAS

Note:

↳ used for short Messages

↳ Easy to break by the attacker.

2) Row Transposition Cipher : we write the Message in a rectangle, row by row, and read the Message off, column by column, but permute the order of column.

key → integer value (unique digits from 0 to 9)

eg: 45312

eg: 4321 etc.

eg: plain → attack postponed until two am

Key

Key →	4	3	1	2	5	6	7
plain text →	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

extra dummy bits

Sometime left blank (Irregular case)

acc to wikipedia

Cipher text : TTNA APTM TSUO AODW COIX KNLY PETZ

↳ Read column by column.

CASE 2

It can be made more secure by performing more than one stage of transposition. so, the result will be a more complex permutation.

Key may be same or different

Key

4	3	1	2	5	6	7
plain text						
t	t	n	a	a	p	t
m	t	s	u	o	a	o
d	w	c	o	i	x	k
n	l	y	p	e	t	z

Ciphertext : NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

Double Transposition :

- Column or transposition/Row transposition cipher applied twice.
- The key in case 2 can be same/different also.
- This Technique was used in World War I by German Military and also in World war II.

Note:

eg: Keyword/Key : STRIPE
it will be use as : 564231

} → decided by the alphabetical order of letters in the key.

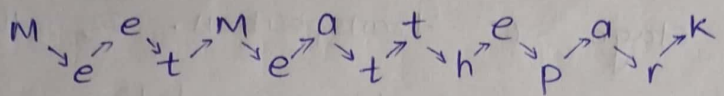
eg: key : Z E B R A

→ 5 3 2 4 1

1) Keyless Transposition Ciphers:

↳ The text is written into a table column by column and then transmitted row by row.

eg:



ciphertext: MEMATEAKETETHPR

↳ The text is written into the table row by row and then transmitted column by column.

M	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

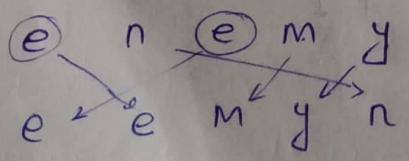
cipher text: MMTAEEHREAEKTTP

2) Keyed Transposition Cipher: In this method we divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

eg: "Enemy attacks tonight"

Cipher →	3	1	4	5	2
plain → ↓ Encryption	1	2	3	4	5

↑ decryption



→ a t t a c k t o n i g h t z

cipher → t a a c t t k o n s h i t z g

Caeser Cipher :

- It is also called shift cipher / additive cipher.
- Each letter in the plain text is replaced by a letter corresponding to a no of shifts in the alphabet.
- It is a monoalphabetic ceaser cipher.
- It is one of the earliest and simplest method of encryption technique.

eg: Key = 3

MEET → PHHW

MNQ

plain → Meet Me Zebra

cipher → PHHW PH CHEUD

cipher text

$$[C = E(K, P) = (P + K) \bmod 26]$$

(K: key, P: plain, message)

↳ for encryption.

for decryption

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

(C: cipher)

// if (c-k) is -ve then add 26 to i

Numerical value is assigned to each other.

a	b	c	d	e	-----	x	y	z
0	1	2	3	4	-----	23	24	25

⇒ If the Crypt Analyst/Attacker knows a cipher text. then He can apply brute-force technique to find the plain text by using all the possible 25 key.

- Since it is a part of Symmetric encryption, same key is used for encryption and decryption.

$$\boxed{1 \leq K \leq 25}$$

eg:

Encryption

Message - "HELLO"

let Key = 4

$C(H) = (P+K) \bmod 26$

$(7+4) \bmod 26 = 11 = L$

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

$= (4+4) \bmod 26 = 8 = I$

$C(L) = (P+K) \bmod 26$

$= (11+4) \bmod 26 = 15 = P$

$C(O) = (P+K) \bmod 26$

$= (14+4) \bmod 26 = 18 \bmod 26 = 18 = S$

$\therefore$ cipher → LIPPS

Decryption

cipher C = LIPPS , Key = 4

Now

$P(L) = (C-K) \bmod 26$

$= (L-4) \bmod 26 = (11-4) \bmod 26 = 7 = H$

$P(I) = (8-4) \bmod 26 = 4 = E$

$P(P) = (15-4) \bmod 26 = 11 = L$

$P(S) = (18-4) \bmod 26 = 14 = O$

$\therefore$ plain text = HELLO

playfair cipher Algorithm :-

1) Create 5×5 Matrix that is called Grid of letters.

2) The Matrix is made by inserting the values of key and remaining alphabets into the matrix (Row wise from left to Right) where letter I and J will be combined together.

3) Convert the text into pair of Alphabet.

eg:

Heya → He ya

a) pair cannot be made with same letters. Break the Letter in single and add 'x' to the previous letter.

eg:

Hello → He lx lo

Helloe → He lx lo ez

e Alone.

b) If the letter is standing alone in the process of pairing, then add 'z' with the letter.

eg:

Helloe → He lx lo ez

e was alone so we added z Here.

Hexxoe → He xz xo ez

↳ x was already there so, We took 'z'.

4) Code will be Formed using 3 rules.

i) If both the Alphabet are in the same row, replace them with alphabets to their immediate right.

ii) if both the Alphabets are in same Column, replace them with alphabets immediately below them.

iii) If not in same row/column, replace them with alphabets in the same row respectively but at other pair of corners.

---

eg:

Key → Abhi

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

eg:

i) plain text

Same col.

B M → E R

R W → W B

Same row

F G → G K

U Q → Q R

Horizontal

Q W → R V

F L → D N

Random

K L → D P

K S → F U

VIGENERE CIPHER

- Designed by Blaise de Vigenere (16th century French Math.)
- It is a polyalphabetic substitution cipher.
- The Encryption is done using a (26×26) matrix
  ↓
  i.e. a table

Method ① → Vigenere table → used to find cipher text.

eg: plain text = GIVE MONEY

KEY = LOCK

Soln:

P →	G	I	V	E	M	O	N	E	Y
(K) Key →	L	O	C	K	L	O	C	K	L

→ Repeat the letters of the key so, that the no° of letters in P and K i.e. plaintext and key becomes equal.

Cipher text: R W X O X C P O J

26×26

Key \ plain text	a	b	c	d	...	x	y	z
a	A	B	C	D	...			
b	B	C	D	E	...			
c	C	D	E	F	...			
⋮								
x								
y								
z								

Method 2 : When the table is not given

1) Encryption:

$$C_i = E_i = (P_i + K_i) \bmod 26$$

E_i = encryption
P_i = plain text
K_i = key value

2) Decryption:

$$D_i = (E_i - K_i) \bmod 26$$

eg: plaintext → "She is Listening"

Key → "PASCAL"

∴ Key Stream → (15, 0, 18, 2, 0, 11)

↳

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Soln

plain	s	h	e	i	s	L	i	s	t	e	n	i	n	g
P's value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Key stream	15	0	18	2	0	11	15	0	18	2	0	11	15	0
(P+K) mod 26 C's value	7	7	22	10	18	22	23	18	11	6	13	19	2	6
Cipher text	H	H	W	K	S	W	X	S	L	G	N	T	C	G
(E-K) mod 26 plain text	S	H	E	I	S	L	I	S	T	E	N	I	N	G

(7-15) mod 26
-8 mod 26
(-8+26) mod 26
18 mod 26
= 18

VERNAM CIPHER

- Used for encrypting alphabetic text.
- Simply a type of Substitution cipher.

eg: plain text — RAMSWARUPK

Key — RANCHOBABA

Soln

P.T.	17	0	12	18	22	0	17	20	15	10
Key	17	0	13	2	7	14	1	0	1	0
(PT+Key) Add	34	0	25	20	29	14	18	20	16	10
Sub >26	(34-26) 8	0	25	20	3	14	18	20	16	10
C cipher	I	A	Z	U	D	O	S	U	Q	K

Now,

For Decryption

cipher	8	0	25	20	3	14	18	20	16	10
Key	17	0	13	2	7	14	1	0	1	0
CT-Key	-9	0	12	18	-4	0	17	20	15	10
plain	17	0	12	18	22	0	17	20	15	10
	(26-9) R	A	M	S	W	A	R	U	P	k

HILL CIPHER

- It is a polyalphabetic cipher.
- encrypts a group of letters called polygraph.
  (like in playfair cipher, we said it was a encrypting a pair of letters which was called as a digraph)
  So, Here it can be a polygraph (digraph, trigraph etc)

- This methods makes use of mathematics.

To encrypt

$$C = KP \bmod 26$$

- Step 1 → Choose a key (key matrix must be a Square Matrix)

We can take any key.

eg:

$$VIEW = \begin{bmatrix} V & I \\ E & W \end{bmatrix}_{2\times2} = \begin{bmatrix} 21 & 8 \\ 4 & 22 \end{bmatrix}_{2\times2}$$

$$Key = QUICKNESS$$

$$= \begin{bmatrix} Q & U & I \\ C & K & N \\ E & S & S \end{bmatrix}_{3\times3} = \begin{bmatrix} 16 & 20 & 8 \\ 2 & 10 & 13 \\ 4 & 18 & 18 \end{bmatrix}_{3\times3}$$

eg: plaintext = ATTACK

Let $Key = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

Since, the key is a 2×2 matrix, text should be converted into vectors of length 2.

So,

$\begin{bmatrix} A \\ T \end{bmatrix}_{2\times1} \begin{bmatrix} T \\ A \end{bmatrix}_{2\times1} \begin{bmatrix} C \\ K \end{bmatrix}_{2\times1}$

Now, Encryption begins

① So, 1st vector → $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$, Key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

$C = KP \bmod 26$

$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2\times0 + 3\times19 \\ 3\times0 + 6\times19 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0 + 57 \\ 0 + 114 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 11 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$

∴ plain text $\begin{bmatrix} A \\ T \end{bmatrix}$ becomes $\begin{bmatrix} F \\ K \end{bmatrix}$ i.e. AT → FK

Now, 2nd vector → $\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$ ~~mod~~.

$C = KP \bmod 26$

$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 38+0 \\ 57+0 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$

∴ plain text $\begin{bmatrix} T \\ A \end{bmatrix}$ becomes $\begin{bmatrix} M \\ F \end{bmatrix}$ i.e. TA → MF

Now 3rd vector → $\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

$C = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4+30 \\ 6+60 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$

CK becomes IO,

∴ plain = ATTACK
cipher = FKMFIO

} polyalphabetic cipher.

For decryption

$$P = K^{-1} C \bmod 26$$

$$K^{-1} = \frac{1}{|K|} adj(K)$$

eg:

plain → ATTACK

cipher → FKMFIO , Key $K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

$C = FK\ MF\ IO$

$$\therefore d = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = 12 - 9$$

$$|d| = 3$$

→ determinant value.

Now, Find the multiplicative inverse of determinant

i.e. $dd^{-1} = 1 \bmod 26$

$\because dd^{-1} \bmod 26 = 1$

$5 \times d^{-1} \bmod 26 = 1$

$5 \times 21 \bmod 26 = 1$

$d^{-1} = 21$

$3 \times d^{-1} \bmod 26 = 1$

$d^{-1} = 9$

$3 \times 9 \bmod 26 = 1$ → true.

$\therefore d^{-1} = 9$

Now, Adjacent

let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ the $adj(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Here, $K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ $adj(K) = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$

+ve outputs 26 add

$$adj(K) = \begin{bmatrix} 6 & -3+26 \\ -3+26 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$d^{-1} = 9$

Now,

$$K^{-1} = \frac{1}{|K|} adj(K) = |K^{-1}|\, adj(K) = d^{-1}\, adj(d)$$

$$K^{-1} = 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix}$$

Now find its modulo 26

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

Now

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

Now,

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

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 10+250 \\ 125+180 \end{bmatrix} \bmod 26$$

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

for

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

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} 24+125 \\ 300+90 \end{bmatrix} \bmod 26 = \begin{bmatrix} 149 \\ 390 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$$

in for

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

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \end{bmatrix} \bmod 26 = \begin{bmatrix} 16+25(14) \\ 25(8)+18(14) \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 366 \\ 452 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

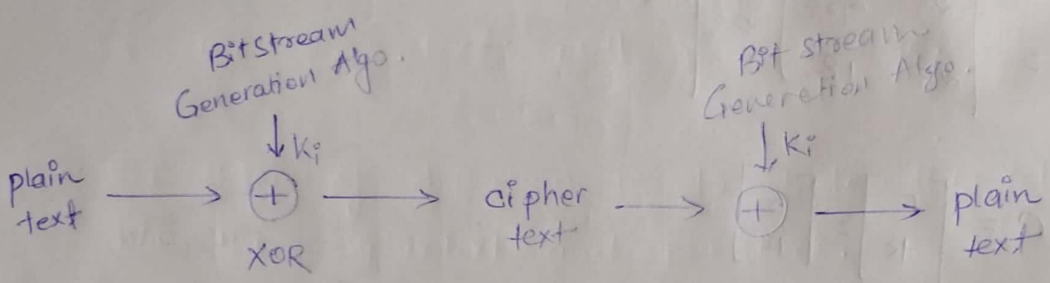
∴ plain text → ATTACK

Stream & Block Cipher

- used to convert plain text → cipher text

1) Stream cipher :-

- It is the one that encrypts a digital (0 or 1) data - stream one bit or 1 byte at a time.
- It is a symmetric key cipher (i.e. 1 key for encry. + decrypt)



eg:

```
  1 0 1 1 0 1 1 0   ← Msg at sender side
⊕ 0 1 0 1 0 1 0 1   ← Key
-----------------
  1 1 1 0 0 0 1 1   ← cipher.
-----------------
```

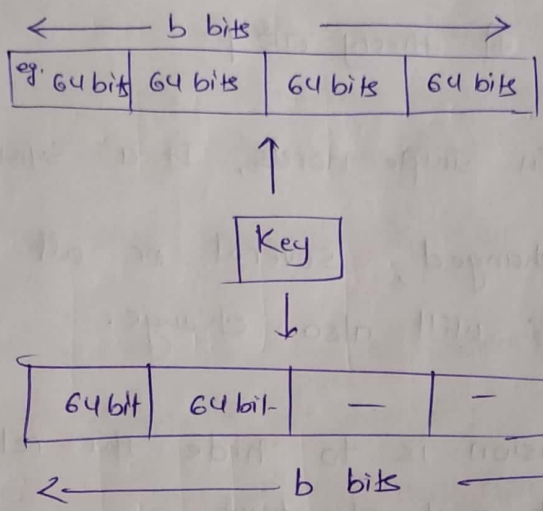
To decrypt

```
  1 1 1 0 0 0 1 1   ← cipher
  0 1 0 1 0 1 0 1   ← key
-----------------
  1 0 1 1 0 1 1 0   ← plain
-----------------
```

2) Block Cipher :-

- In this, A Block of plain text is treated as a whole and used to produce the ciphertext to equal length.

- Typically a block size of 64 and 128 bits is used.
- Symmetric key cipher (1 key used only).
- Key will be Applied on each Block.



BLOCK CIPHER

- plain → cipher text by taking plain text block at a time.
- It uses 64 bits or more.
- Complexity of block cipher is simple.
- Uses Confusion as well as diffusion Concept.
- In this, reverse encrypted text is hard.

STREAM CIPHER

- 1 bit or 1 byte of plain text → cipher text.
- Stream cipher uses 8 bits.
- While stream cipher is more complex.
- Uses only Confusion concept
- Reverse encrypted text is easy.

SHANNON'S Theory of Confusion & Diffusion :

- जब हम plain text को cipher text में change करते हो, तो Attackers may be cipher text को modify कर सकते है, इससे बचने के लिए SHANNON'S ने confusion & Diffusion की theory लाई।

1. **DIFFUSION** :- In simple words, If a symbol in the plaintext is changed, several or all symbols in the ciphertext will also change.

- The Idea of diffusion is to hide the relationship b/w the ciphertext and plaintext.

- If we change 1 bit of ciphertext, then atleast one Half of the plaintext bits should change.

2. **CONFUSION** :-

- It hides the relationship b/w ciphertext and the key.

- If a single bit in the key is changed then most/all bits of the ciphertext will also be changed.

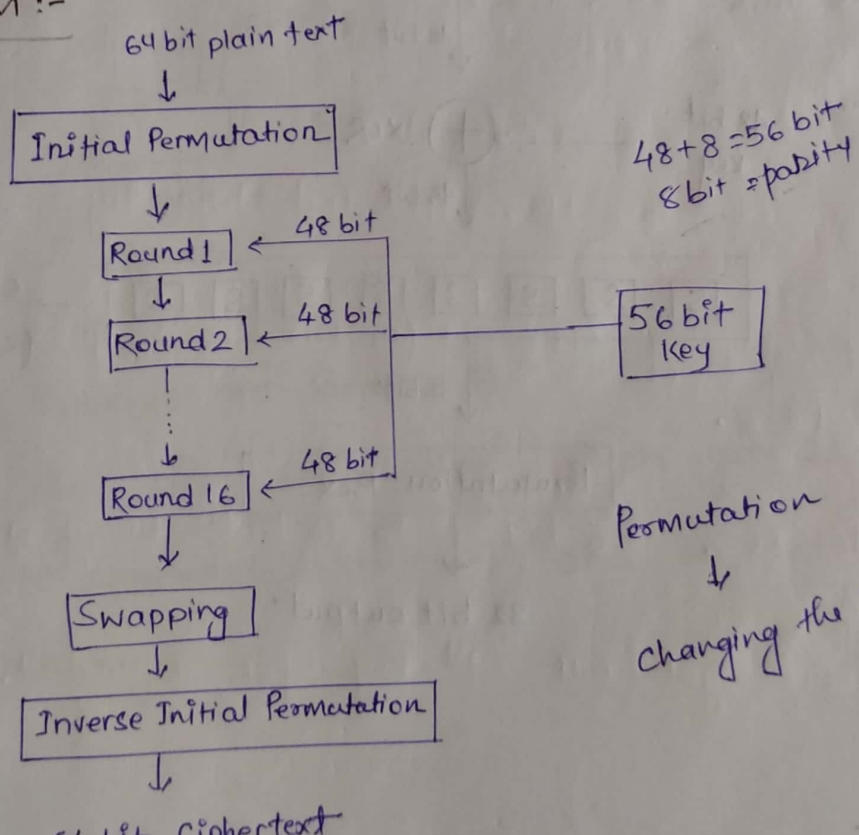
- Each bit of Ciphertext should depend on key.

DES

(Data Encryption Standard)

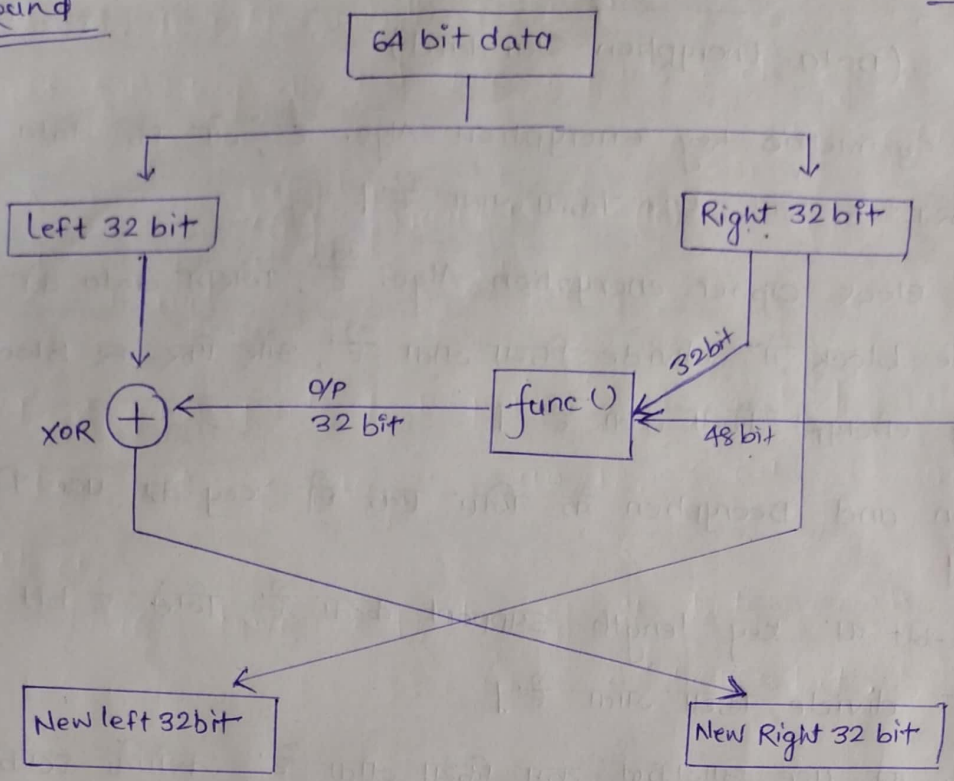
- DES एक Symmetric key encryption Algo. है, जो कि data को secure करने के लिए use किया जाता है।
- DES एक Block cipher encryption Algo. है, जिसमें data को fixed size block में divide किया जाता है, और फिर हर Block को seperately encrypt किया जाता है।
- Encryption and Decryption के लिए एक ही key का use किया जाता है।
- DES 56-bit का key length support करता है, जिसे 8 bit की Blocks में divide किया जाता है।
- इस Algo. का use आजकल कम किया जाता है, क्योंकि इसका key length बहुत छोटा है, और इसलिए इसके Encryption को तोड़ना आसान हो जाता है।
- इसकी जगह आजकल AES (Advanced Encryption Standard) जैसी Modern encryption techniques का use किया जाता है, जिसका key length 128-bit, 192-bit, 256 bit होता है।
- 64 bit block data is used.

Algorithm :-

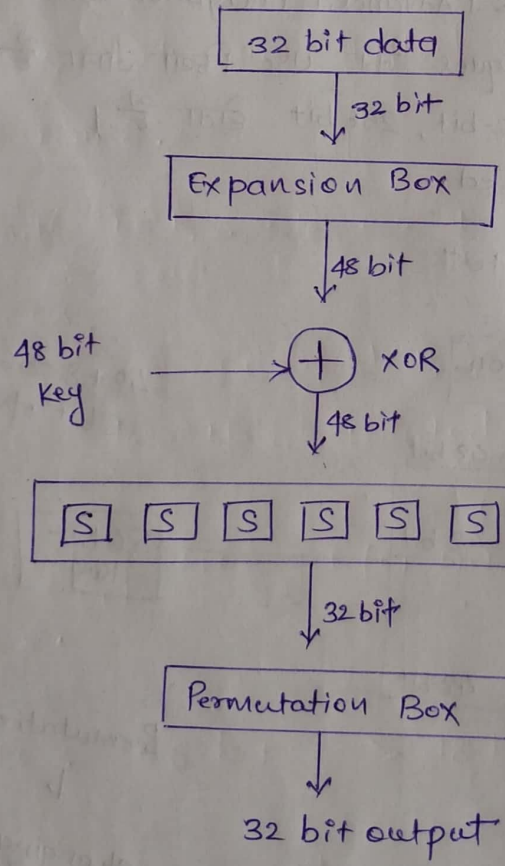


function definition

1 Round



1 Function Definition :-



(32 bit to 48 bit by using Expansion Box)

→ S-Box (Substitution Boxes)

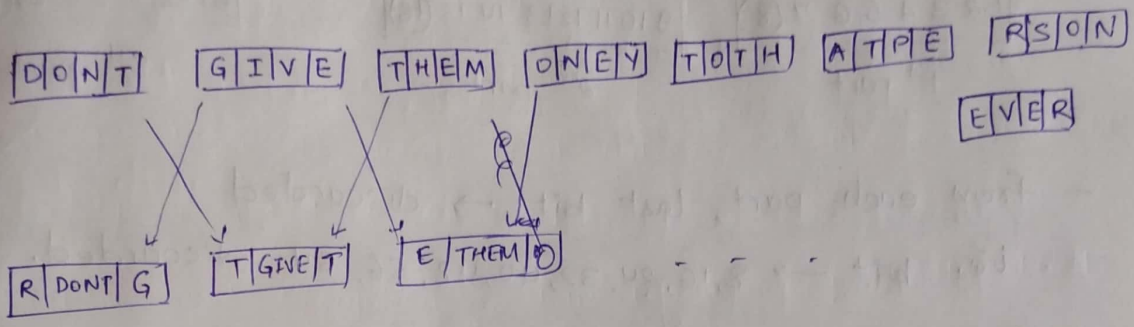
(8 S box हमको 4 bit का o/p देता)

What Happens in Expansion Box ?

- 32 bit data will be → 1's and 0's form.

But for expansion let us consider a text.

eg:



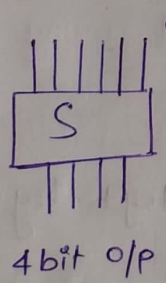
- So, Here Every 4bit block is converted to a 6 bit block.

- There were 8 blocks of 4 bit each = 32 bit
  Now, There are 8 blocks of 6bit each = 48 bit.

Now,

These 48 bits XOR wit 48 bit key.
and given/sent to S-boxes.

What Happens in S-boxes ?



S-box.

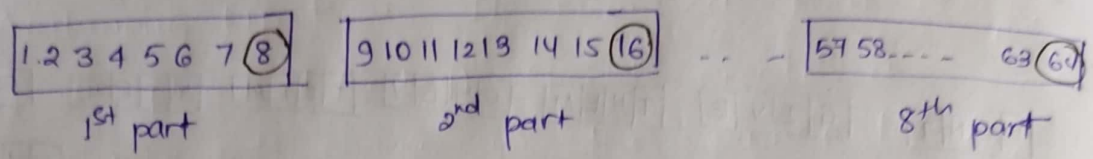
How 16 Subkeys are Generated ?

Actually we have 64 bit key which go as a i/p to PC-1 (permuted choice-1) and we get o/p as 56 bit key.

- Inside PC-1 (Permuted choice 1)

64 bit key divided into 8-parts each of 8 bit.

8 * 8 = 64 bit



- from each part, last bit → discarded

i.e. bit → 8, 16, 24, 32, 40, 48, 56, 64 discarded.

Hence,

We have 8 parts of 7 bits each

= 8 * 7 = 56 bit.

- O/p of PC-1 is 56 bits which is then divide into 2 parts of 28 bits each → C_0, D_0

Now,

these bits are shifted with left shift in each round.

in Rounds i = 1, 2, 9, 16 → 1 shift i.e rotated (left) by 1 bit

in Rounds,

~~बाकी बचे~~ Round ~~में~~

two Halves rotated left by 2 bits.

- After shifting we get (C_1, D_1) which goes as i/p to PC-2.

- Inside PC-2 56 bit → 48 bit using a predefined table.

Then we get our 1st Key for round 1.

In C_1 → 28 bit → (1-28)

D_1 → 28 bit → (29-56)

Now,

56 bit ~~से~~ How 48 Selected?

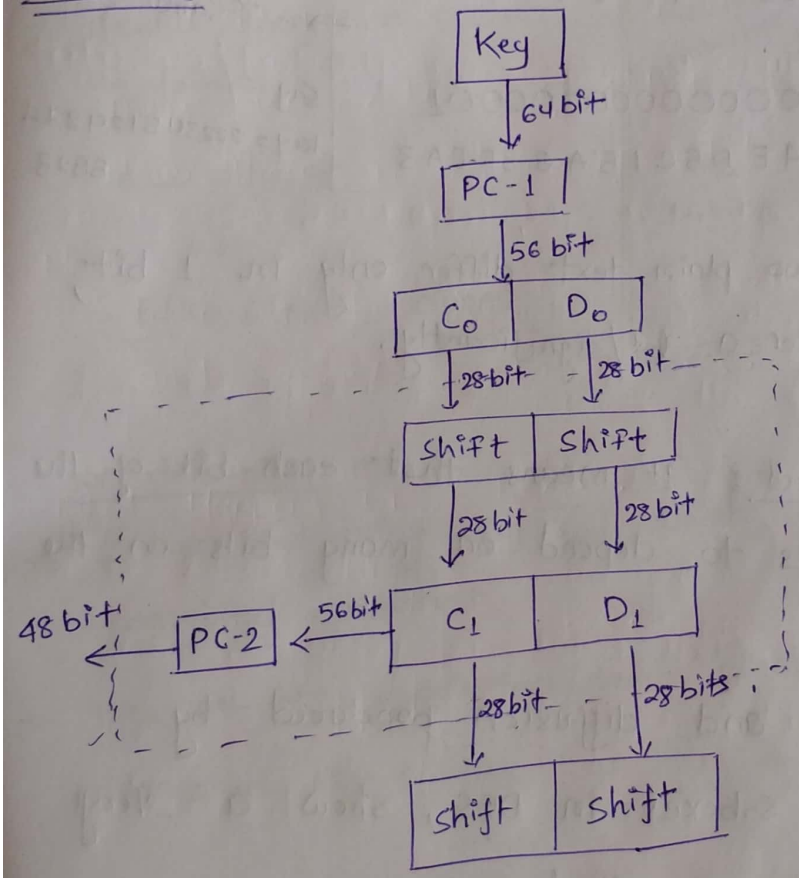
left Half C_1 (9, 8, 22, 25 positions bits are missing)

i.e. 24 left.

Right Half D_1 (35, 38, 43, 54 position bits are missing)

i.e. 24 bits left.

Means



DES Analysis

Properties

1.) **Avalanche Effect** :- It means a small change in plaintext (or Key) should create a significant change in the cipher text.

DES has been proved to be strong with regard to this property.

eg:

plain : 0000000000000000
cipher: 4789FD476E82A5F1

plain : 0000000000000001
cipher : 0A4ED5C15A63FEA3

→ Key used is same

Say Key = 22234512987ABB23

Although, the two plain text differ only in 1 bit, cipher block differ a lot/significantly.

2) **Completeness Effect** : It means that each bit of the ciphertext needs to depend on many bits on the plaintext.

The confussion and diffusion produced by D-boxes and S-boxes in DES, show a very Strong Completeness effect.

MULTIPLE DES

1. Double DES (2 DES)
2. Triple DES (3 DES)

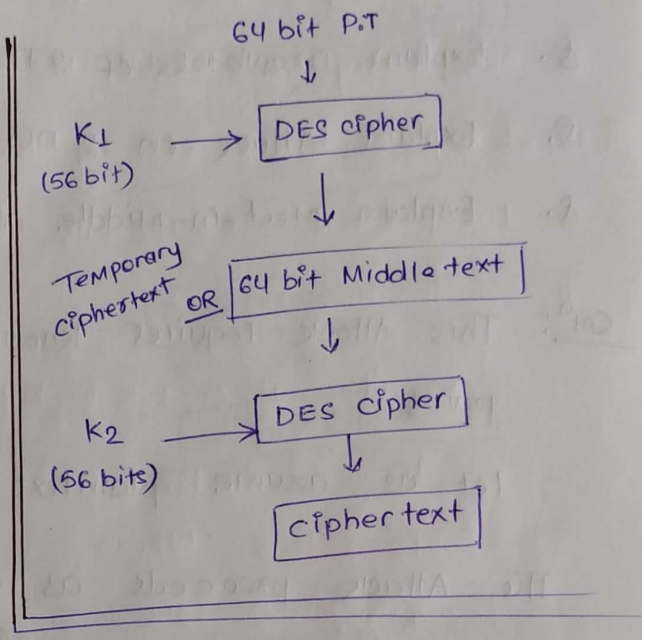
- Since DES Attack Was Vulnerable to brute force attack Variation of DES called Multiple DES were introduced.

Double DES :-

- Uses 2 diff. Keys.
  (56+56)=112 bit Key
- Double Encryption occurs as follows.

$P \rightarrow E(K_1, P)$

$E(K_2, E(K_1, P)) = \text{cipher}$



for decryption :-

- 1st decrypted using Key K_2 which produces single encrypted ciphertext.
- This 64 bit Middle text/temp. ciphertext is then decrypted using the key K_1 to get plain text.

$$\text{plain} = D(K_1, D(K_2, C))$$

first this will Happen.

Drawbacks of Double DES:

— Meet-in-the-middle Attack:

This Attack involves encryption from one end and decryption from the other end and then "matching the results in the middle" and hence the name.

Q. Explain Drawbacks of 2 DES.

Q. Explain Attack on 2 DES.

Q. Explain Meet-in-middle attack. (MIM Attack)

Soln: This Attack requires knowing some plaintext/ciphertext pairs.

let us assume plaintext = P, cipher = C

The Attack proceeds as follows:

(i) encrypt (P) for all 2^{56} possible values of K1 and Stores the result in a table and sort it.

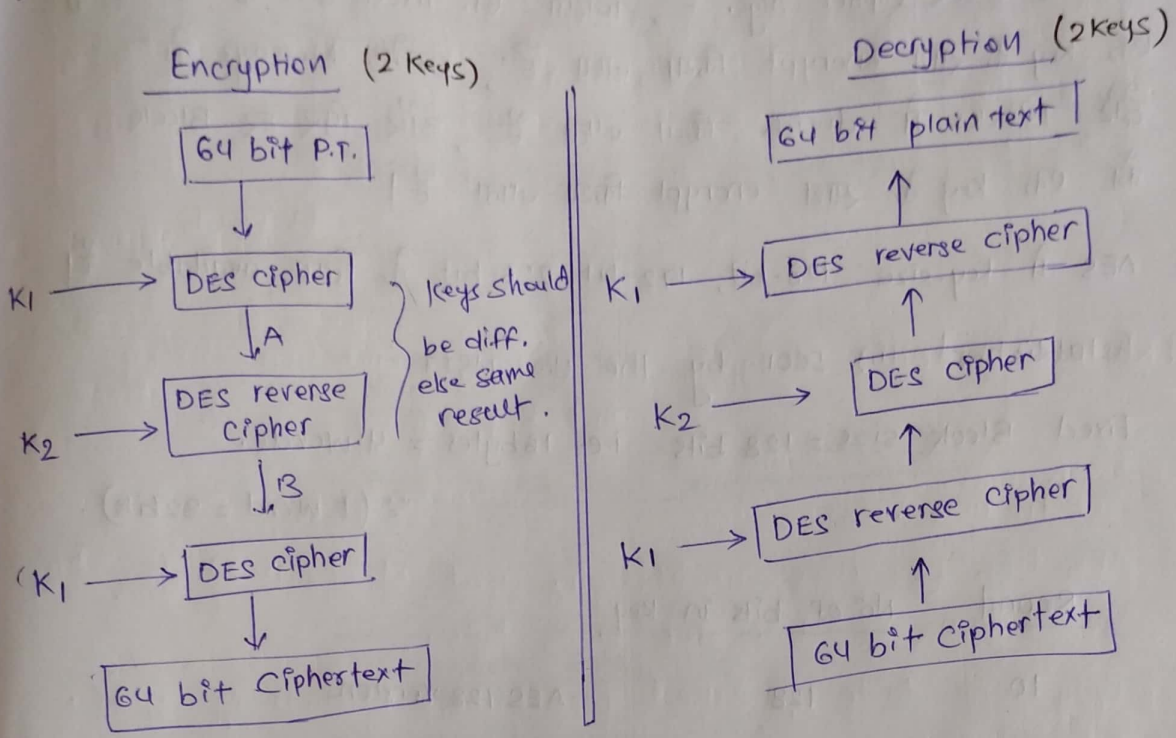
(ii) Now, Decrypt (C) using all 2^{56} possible values of K2. As each i.e. decryption result is produced, check against the table for a match.

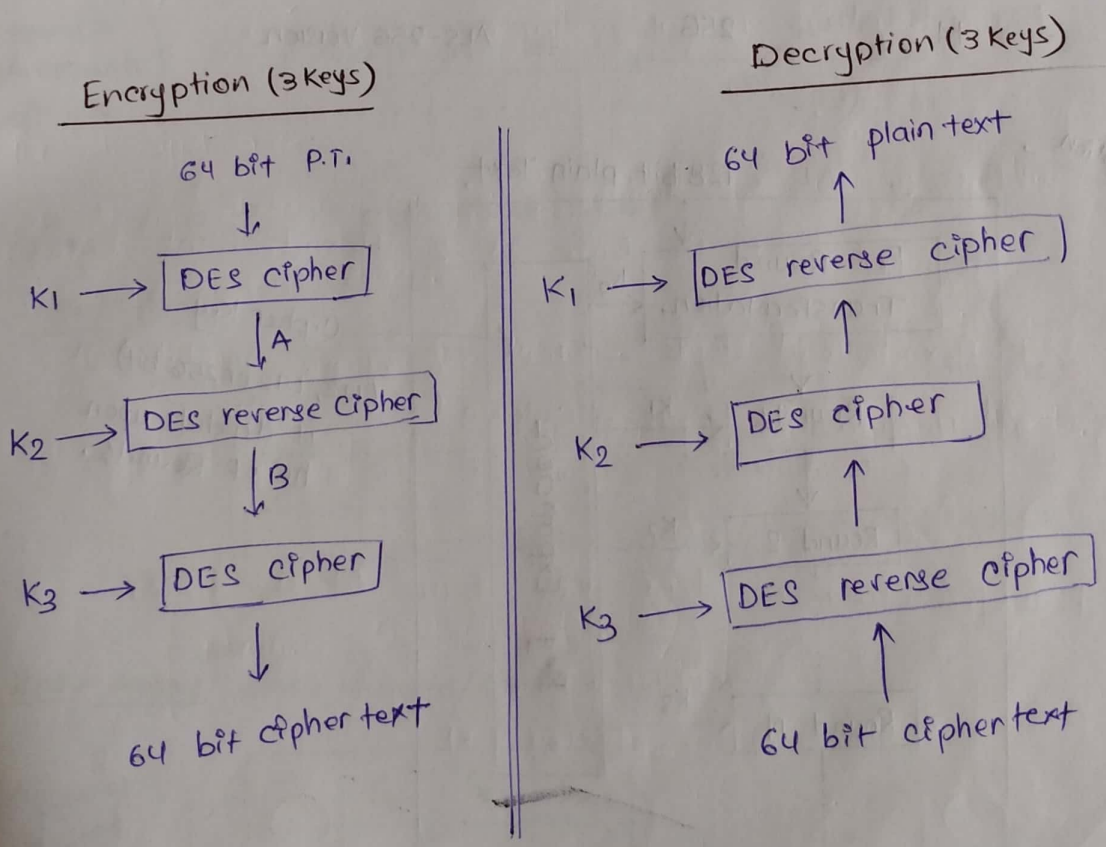
(iii) When there is a match we have located a possibly correct pair of keys.

Note: Now, More than 1 pair of keys may result in a match, but these no of pairs will be Small. We should try each possible pair of keys.

Triple DES (3 DES) :-

- 2 or 3 Keys are used.
- Much stronger than Double DES.



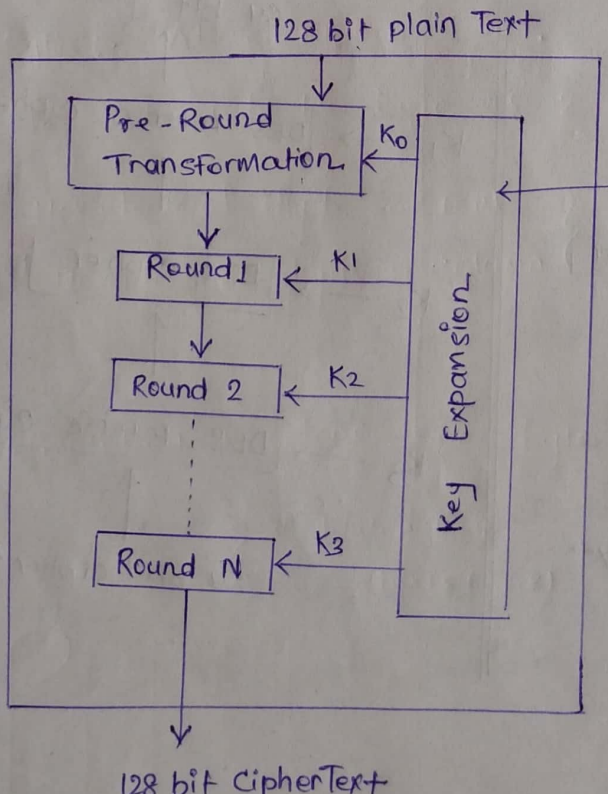


AES (Advanced Encryption Standard)

- यह एक symmetric key encryption Algo. है जो secure data communication और storage के लिए use किया जाता है।
- AES एक Block Cipher Algo. है, जिसमें एक fixed size के Block को एक Key के साथ encrypt किया जाता है, इसमें Message को छोटे Blocks में divide किया जाता है, और फिर हर Block को एक Key के साथ encrypt किया जाता है।
- AES में Key-size 128-bit, 192-bit, 256-bit के लिए available है।
- Established in 2001 by the U.S. NSIT
- Fixed Block size = 128 bits i.e. 16 bytes = 4 words.
  ∵ (1 word = 32 bit).

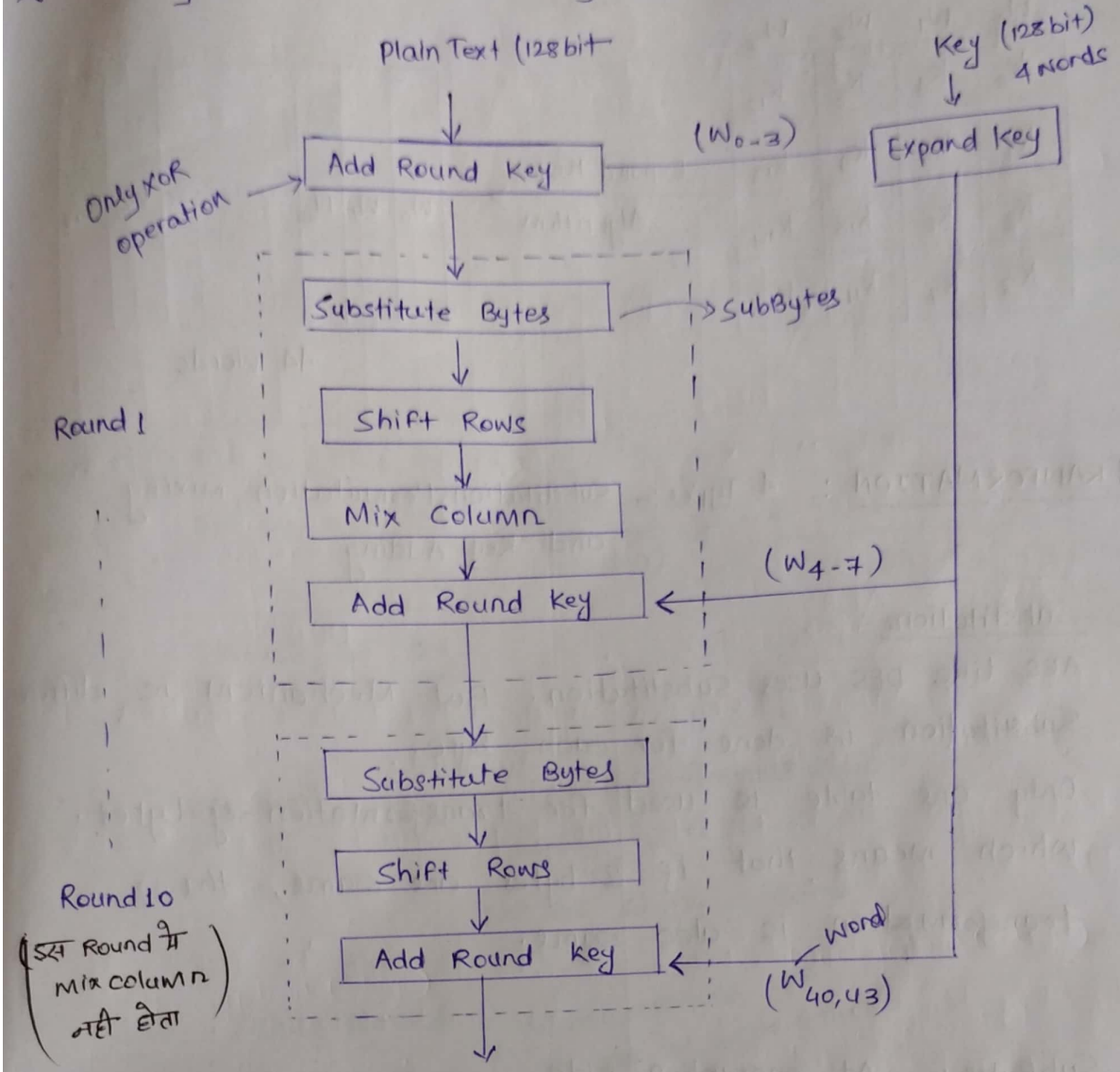
Round	No of bits in Key	
10	128	AES-128 version
12	192	AES-192 version
14	256	AES-256 version

Encryption

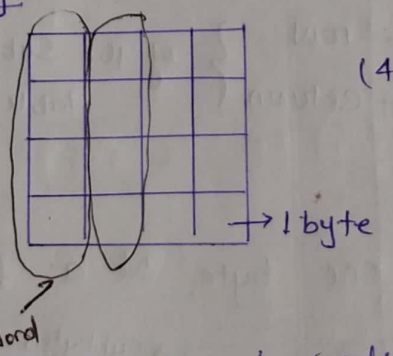


- No of keys Generated by key expansion Algo = (no of rounds + 1)

eg: If Round = 10 → Key = 10+1 = 11 ; if Round 12 → Key = 12+1 = 13

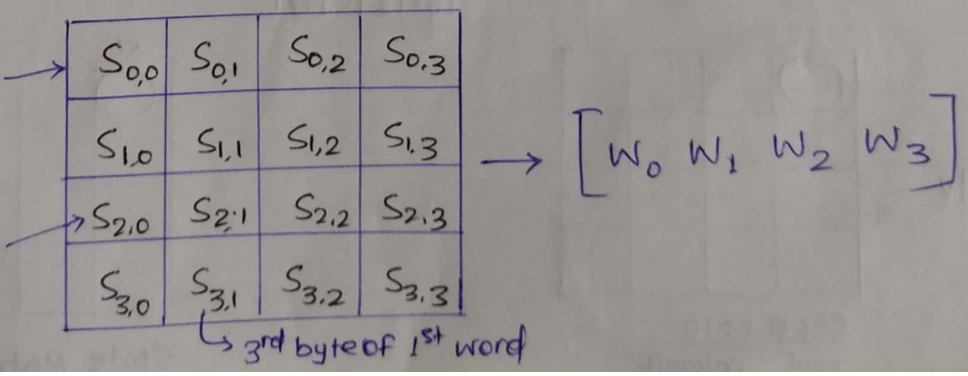


Input Array:



(4×4 i.e 16 byte i.e 128 bits)
or
4 words
1 words = 4 bytes.

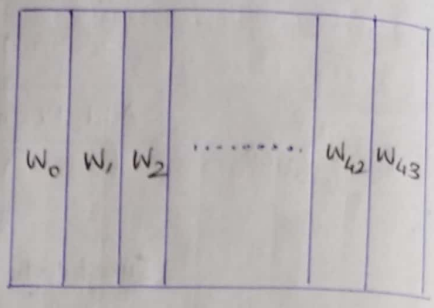
State Array (4×4) 16 bytes/4 words



Key (128 bit i.e. 4 words)

W_0	W_1	W_2	W_3
K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

Expand Key Algorithm →



44 words

TRANFORMATION : 4 Types :- Substitution, Permutation, Mixing and Key Adding

1. Substitution :

AES like DES uses Substitution. But Mechanism is different. Substitution is done for each byte.

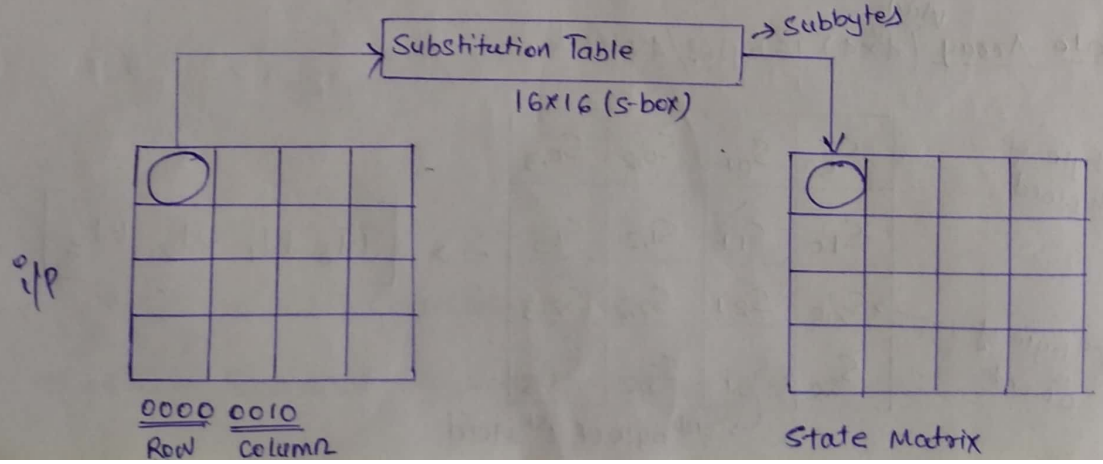
Only one table is used for transformation of bytes. Which means that if 2 bytes are same, the transformation is also same.

SubBytes :- At encryption side.

We interpret the byte as 2 Hexadecimal ~~bytes~~ digits.

1st Hexadecimal digits – row
2nd Hexadecimal digits – column
} of the Substitution table.

– Transformation is done one byte at a time.



2. Permutation :- In this we permute/shift the bytes.
In DES, permutation was done at bit level.
AES, " " is " " byte level.

Shift Rows :

- Shifting is done to the left.
- No of shifts depends on the row of the state matrix.

Row 0	63	C9	FE	30
Row 1	F2	F2	63	26
Row 2	C9	C3	7D	D4
Row 3	BA	63	82	B4

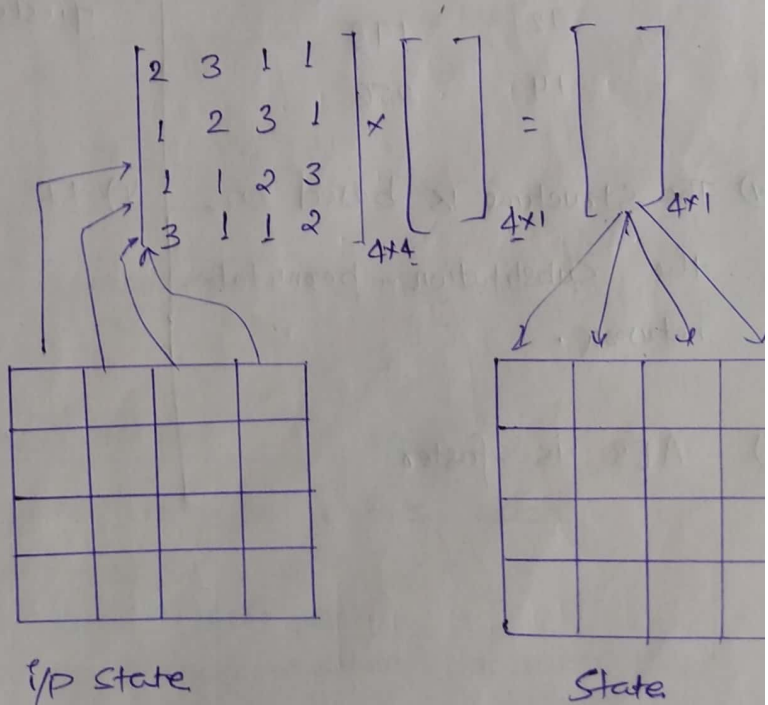
Shift Rows (left shift) →

63	C9	FE	30	0/NO SHIFT
F2	63	26	F2	1 byte shift
7D	D4	C9	C3	2 byte shift
D4	BA	63	82	3 byte shift

In decryption, we use Inv Shift ~~Rounds~~ Rows.
(Shifting is to the Right).
No of shifts = same

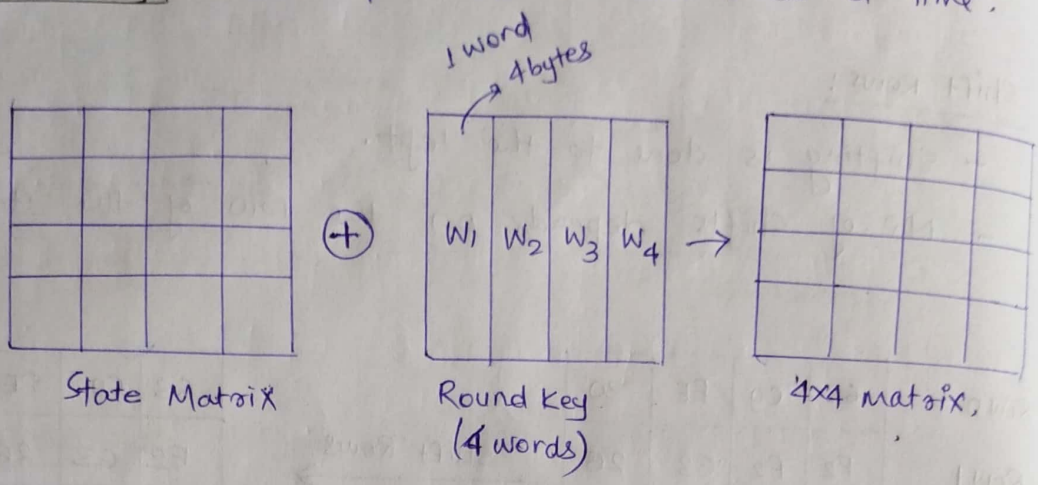
Note: Shift Rows & Inv Shift Rows } Transformations are inverses of each other.

3. Mixing :-
for Encryption.
Take Each word/column i.e 4 bytes or 4x1 matrix and multiply it with the constant matrix.
The o/p is (4x1) matrix of 4 bytes and is stored in the o/p or State matrix.



4. Key Adding :-

Add RoundKey :- Also proceeds 1 column at a time.



AES	DES
(i) Stand for Advanced Encryption Standard.	(i) Stand for Data Encryption Standard.
(ii) Key length can be 128 bits, 192 bits, 256 bits.	(ii) key length is 64 bits (56 bits in each round)
(iii) No of Round depends on the Key length.	(iii) DES involves 16 rounds of identical operations.
(iv) The structure is based on the substitution - permutation network.	(iv) The structure is based on fiestel network.
(v) AES is faster	(v) It is comperatively slower.

Round	bits
10	128
12	192
14	256

IDEA (International Data Encryption Algorith)

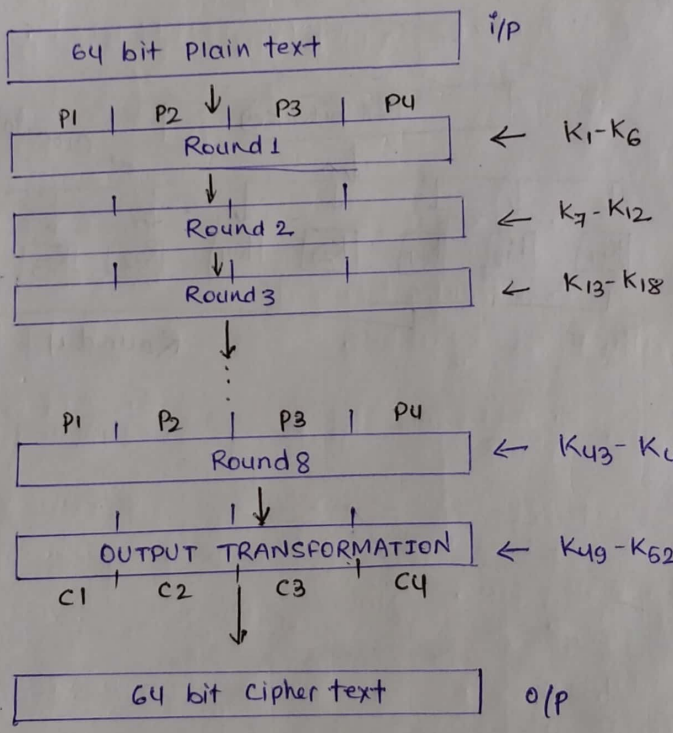
IDEA एक Symmetric Key Block Cipher Algorithm है, जो data को secure तरीके से encrypt or decrypt करने के लिए इस्तेमाल होता है।

IDEA Algo. 64-bit blocks पर काम करता है, और 128 bit Key size use करता है। ये Algo DES की तुलना में ज्यादा Secure है, क्योंकि IDEA में Block size और Key size दोनों ज्यादा होते है।

IDEA Algo. में data को 64-bit Block में divide किया जाता है, और फिर हर Block को एक साथ 64-bit Key से encrypt किया जाता है। ये Algo. Multiple Rounds of Encryption or Decryption करता है, जिसमें हर Round में Subkeys का use होता है।

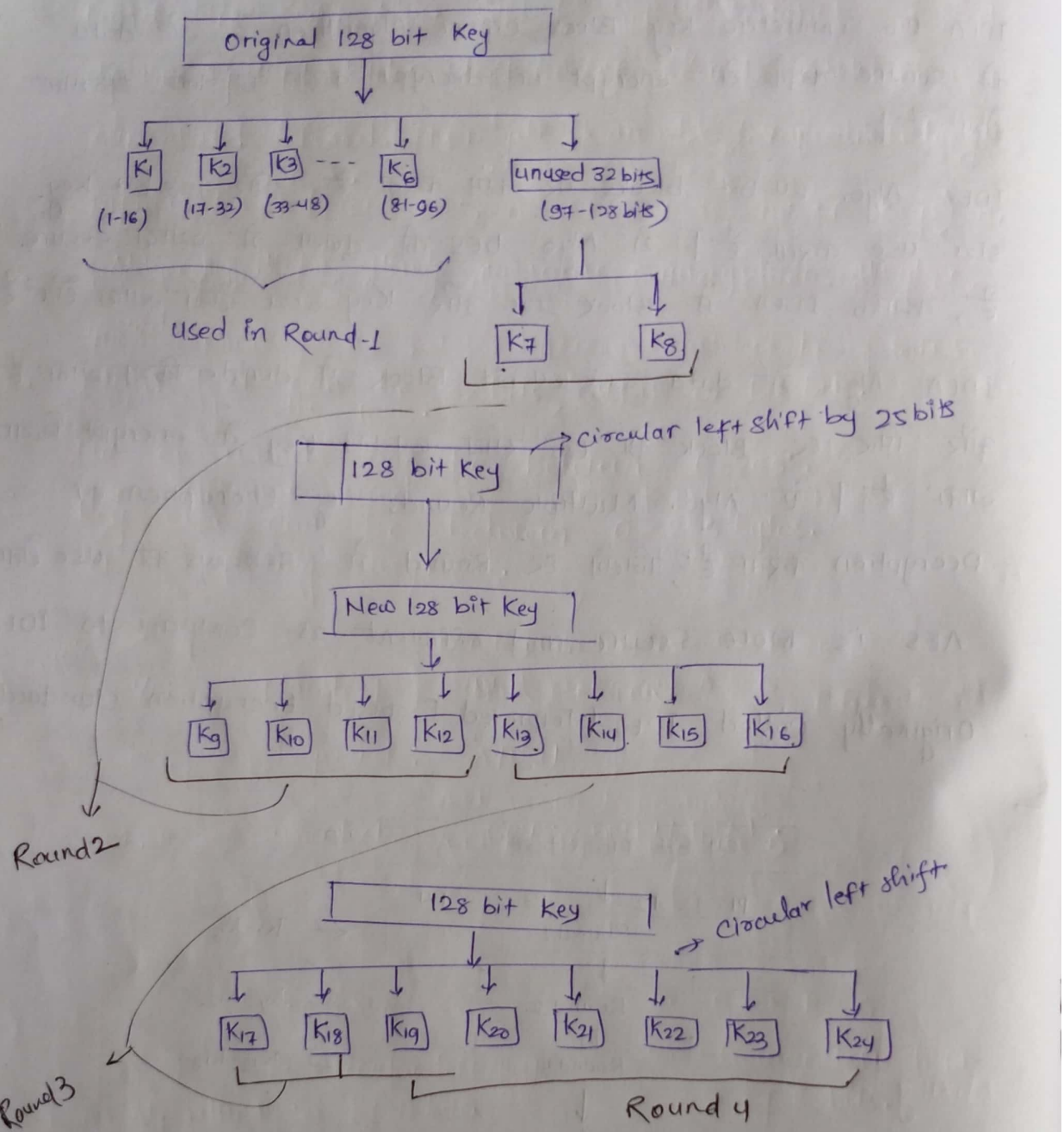
AES is More Secure and efficient as Compare to IDEA.

Originally Called IPES (Improved Proposed Encryption Standard)



- I/p divided into 4 portion P1 to P4 16 bits each.
- There are 8 similar Rounds
- Each Round uses 6 Subkeys (16bit each)
- last Round i.e. the o/p transformation pooduces the cipher text and uses 4 subkeys (16 bit each).

52 Subkeys Generation:



Single Round Details :-

$S_1 = P_1 \times K_1$

$S_2 = P_2 + K_2$

$S_3 = P_3 + K_3$

$S_4 = P_4 \times K_4$

$S_5 = S_1 \oplus S_3$

$S_6 = S_2 \oplus S_4$

$S_7 = S_5 \times K_5$

$S_8 = S_6 + S_7$

$S_9 = S_8 \times K_6$

$S_{10} = S_7 + S_9$

$S_{11} = S_1 \oplus S_9 \rightarrow$ New P_1

$S_{12} = S_3 \oplus S_9 \rightarrow$ New P_2 ⟩ swap.

$S_{13} = S_2 \oplus S_{10} \rightarrow$ New P_3

$S_{14} = S_4 \oplus S_{10} \rightarrow$ New P_4

Output Transformation,

i.e. One-Half Round

$R_1 \times K_{49} = C_1$

$R_2 + K_{50} = C_2$

$R_3 + K_{51} = C_3$

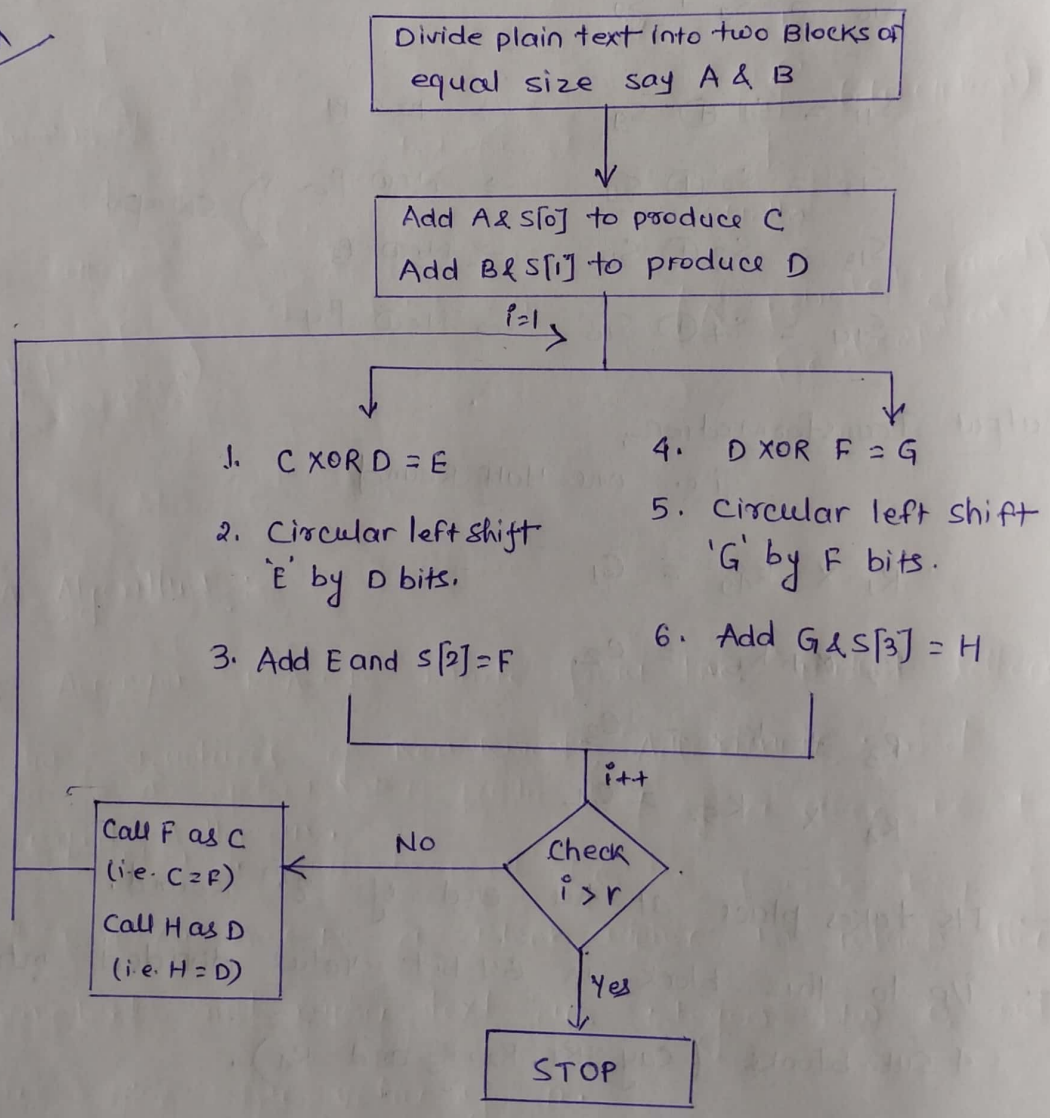
$R_4 \times K_{52} = C_4$

- It takes place at the end of 8th Round.
- i/p to this block is 64-bit value divided into 4 sub-blocks (say R_1, R_2, R_3 and R_4).

RC5 (Rivest Cipher):

- Symmetric Key Block Cipher Algorithm.
- In RC5, the word size, no of Rounds and no of Keys are not fixed. i.e. all can be variable length.
- Once w, r, k (word size, no of rounds, no of keys) are finalized then they remain same for all the rounds.
- plain text can be 32 bits, 64 bits or 128 bits.
- No of rounds can be between 0-255.
- Key size can be between 0 - 255 bytes.

Encryption



Encryption using RC5

- Encryption involved several rounds of a simple function, 12 or 20 round seems to be recommended.
- We divide the plain text block into two equal parts A and B Then They are XOR with two subkeys S[0] and S[1]

$$C = A + S[0]$$

$$D = B + S[1]$$

For i=1 to r do:

1. $C \oplus D = E$
2. perform Circular left shift on E by D bits.
3. add E and S[2*i] and store the result in F which is i/p for step 4.
4. $D \oplus F = G$
5. perform Circular left shift on G by F bits.
6. add G and S[2*i+1] and store the result in H.
7. if i<r

Call F as C and H as D and repeat the steps from 1 to 7.

else stop.

- Once both the phases are Completed the Counter is incriminated and we check if it is greater than the no of rounds, if yes. then the Algorithm termina and if no then the Algorithm iterates.

Decryption :

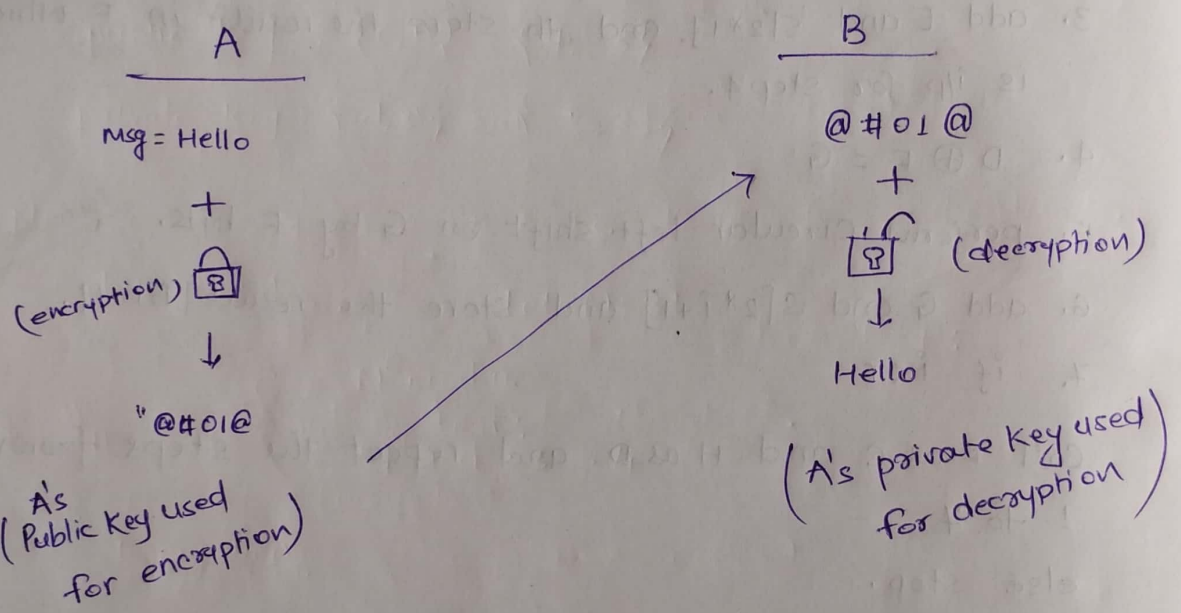
- Decryption is strightforward reversal of the encryption process.

Assymetric Key Algorithm:

- Assymetric Key Algo. also knows as public-key Algo. are cryptographic Algorithms that use a pair of keys - a public key and a private key - for encryption and decryption.

- The key used for encryption is the public key, and the key used for decryption is private key.

eg:



RSA Algorithm :-

- The Acronym RSA is made from the initial letters of the structures of Ron Rivest, Adi Shamir, and Leonard Adleman.

- The RSA scheme is a Block cipher in which the plain text and cipher text are integers b/w 0 and n-1. where for some value of n.

1. Key Generation :-

(i) Select 2 large prime no p and q.

(ii) Calculate $n = p * q$

(iii) Calculate $\phi(n) = (p-1) * (q-1)$

(iv) Choose value of e

$$1 < e < \phi(n) \quad \text{and} \quad \gcd(\phi(n), e) = 1$$

(v) Calculate

$$d = e^{-1} \bmod \phi(n)$$

i.e. $ed = \bmod \phi(n) \cdot 1.$

$$ed \bmod \phi(n) = 1$$

vi) Public key = $\{e, n\}$

vii) Private key = $\{d, n\}$

2. Encryption :

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

plaintext count = $M < n$

C - cipher text

Abh:

$M = 4$

3. Decryption :

$$M = C^d \bmod n$$

Note: (e,n) is a public key used in encryption.

(d, n) is a private key used in decryption.

Q. let $P = 3, \quad q = 11$

Sol^n $n = p * q = 3 \times 11 = 33$

$\phi(n) = 2 \times 10 = 20$

So,

let $e = 7$ as $1 < e < \phi(n) \rightarrow 1 < 7 < 20$ and $\gcd(7, 20) = 1$

Now,

$d = e^{-1} \bmod \phi(n)$

$ed = 1 \bmod \phi(n) \longrightarrow ed \bmod \phi(n) = 1$

$7 \times d = 1 \bmod \phi(n)$

$7 \times d \bmod 20 = 1 \longrightarrow$ d must be 3 because $21 \bmod 20 = 1$

$\therefore \boxed{d = 3}$

Since,

$e = 7, \quad d = 3$

public key $= \{e, n\} = \{7, 33\}$

private key $= \{d, n\} = \{3, 33\}$

Now,

Encryption

let $M = 31$

$C = M^e \bmod n$

$= 31^7 \bmod 33 = 4$

Decryption

$M = C^d \bmod n$

$= 4^3 \bmod 33$

$M = 31$

MAKAUT

Q.2 In RSA System, the public key (e) of a user is 17 and N = 187. What will be the private key of the user.

Sol^n

$e = 17, \quad N = 187$

$\because P \times Q = N$

$17 \times 11 = 187$

$\therefore P = 17, \quad Q = 11$

Now,

$\phi(n) = (p-1) \times (q-1)$

$= 16 \times 10$

$= 160$

$1 < e < \phi(n)$

$1 < 17 < 160$

& $\gcd(160, 17) = 1$

Now,

~~$ed = 1 \bmod \phi(n)$~~

~~$17 \times d \bmod 160 = 1$~~ → d should be 23

~~$\therefore 17 \times 23 \bmod 160 = 1$~~

~~of.~~

Using the Extended Euclidean Algo:

$160 = 9 \times 17 + 7$

$17 = 2 \times 7 + 3$

$7 = 2 \times 3 + 1$

Now,

$ed = 1 \bmod \phi(n)$

$17 \times d \bmod 160 = 1$ d should be 23

$17 \times 23 \bmod 160 = 1$

$161 \bmod 160 = 1$

$\therefore \boxed{d = 23}$ → private key.

Q3 Two prime No° $P = 19$, $Q = 31$, find out N, E, D in RSA encryption process.

→

$N = P \times Q$

$= 19 \times 31$

$N = 589$

Now,

$\phi(n) = 18 \times 30$

$= 540$

Now,

$1 < e < \phi(n)$ & $\gcd(e, 589) = 1$

e, n coprime let $e = 463$

$ed = 1 \cdot \text{mod}\ \phi(n)$

$463 \times d \bmod 540 = 1$ d should be 7

$\because 3241$

$\therefore d = 7$

$\therefore$ public key $(e, n) = (463, 589)$

private key $(d, n) = (7, 589)$ ✓

Authentication function:

Authentication → Verifying the users identity.

Raman → John (msg)

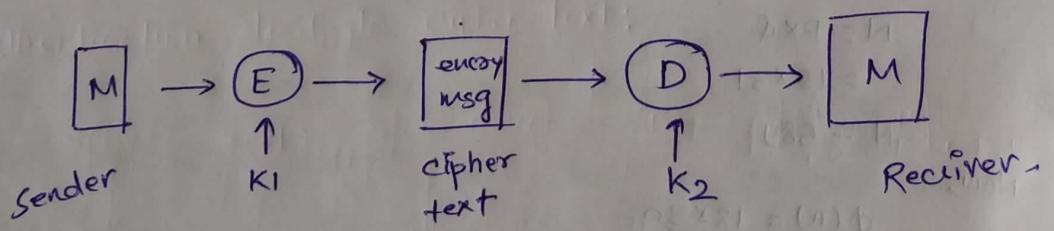
An authenticator must be there to authenticate the message.

Types of Authentication:

1. Message Encryption
2. MAC (Message Authentication Code)
3. Hash function (H)

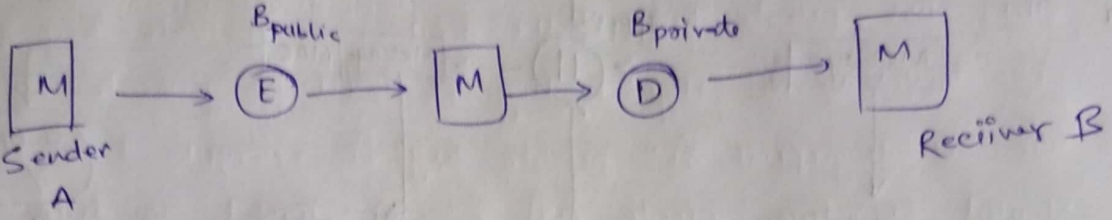
1. Message Encryption:

— cipher text is an Authenticator.



→ Key K_1 shared only b/w Sender & Receiver.

for Asymmetric Encryption:



Authentication X
Confidentiality ✓

2) MAC (Message Authentication Code):

- We will use a Secret key to generate a small fixed size of Block of data called MAC or Cryptographic checksum.
- It is then Appended with the message.
- The communicating parties will share a secret common key. which will be used to create a MAC.
- let A → Sender
  B → Receiver.

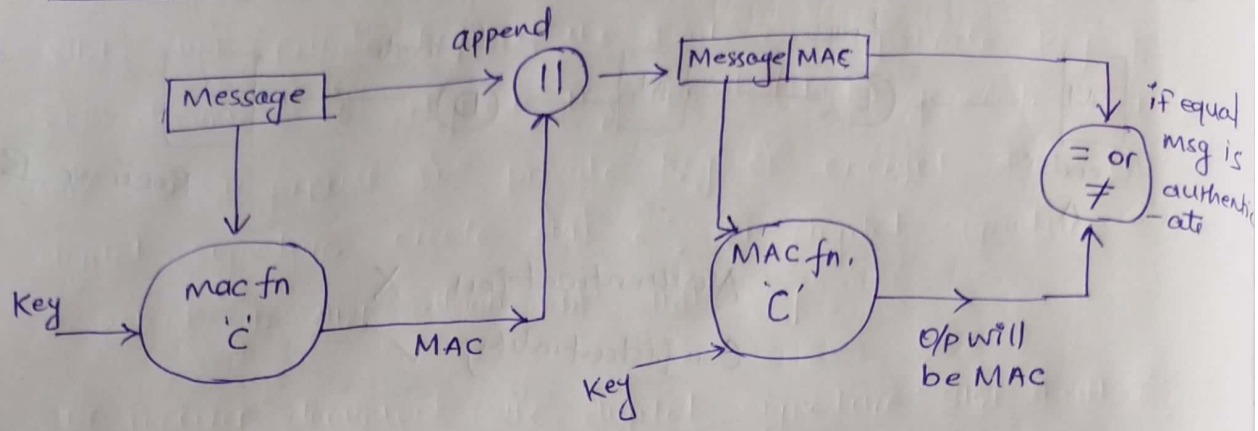
When A sends a msg to B, it calculates the MAC as a fn. of the msg and the key.

$$MAC = C(K, M)$$

Where,
M = i/p Message
C = MAC fn.
K = shared Secret key.

MAC for Authentication:

1)



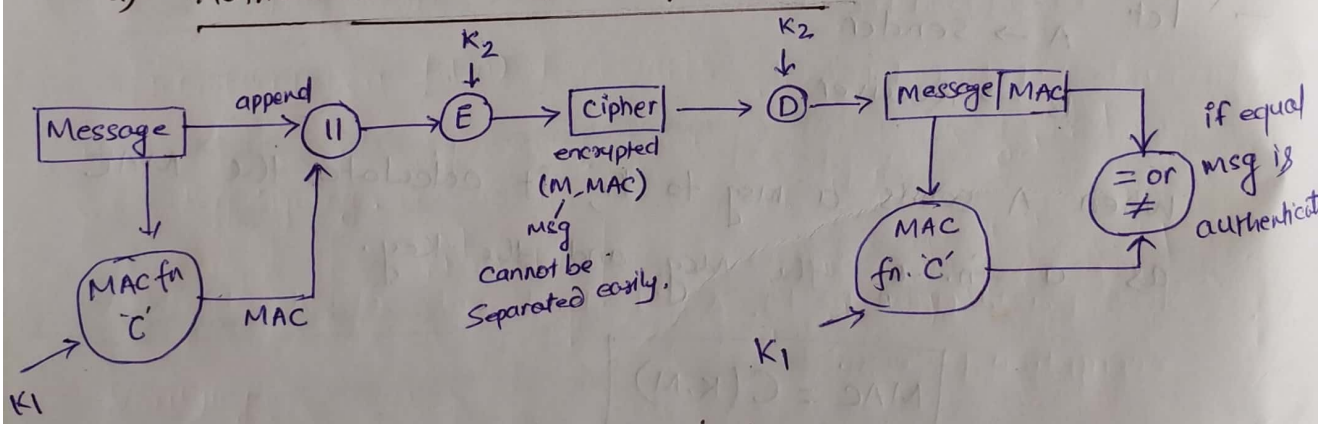
We separate the msg & the MAC.

- Only Authentication is achieved.
- No Confidentiality because if 3rd party come in b/w them he can get the message.

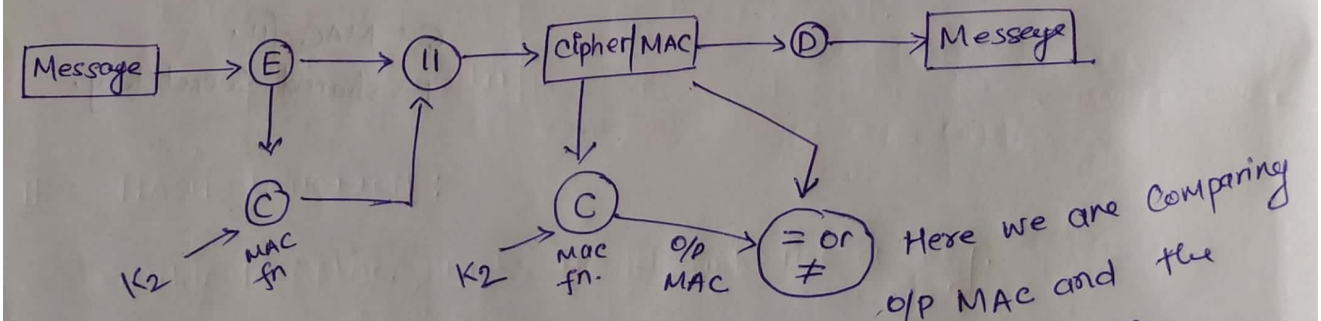
∴ no Security.

2) MAC for Authentication and Confidentiality :-

a) Authentication tied to plaintext.

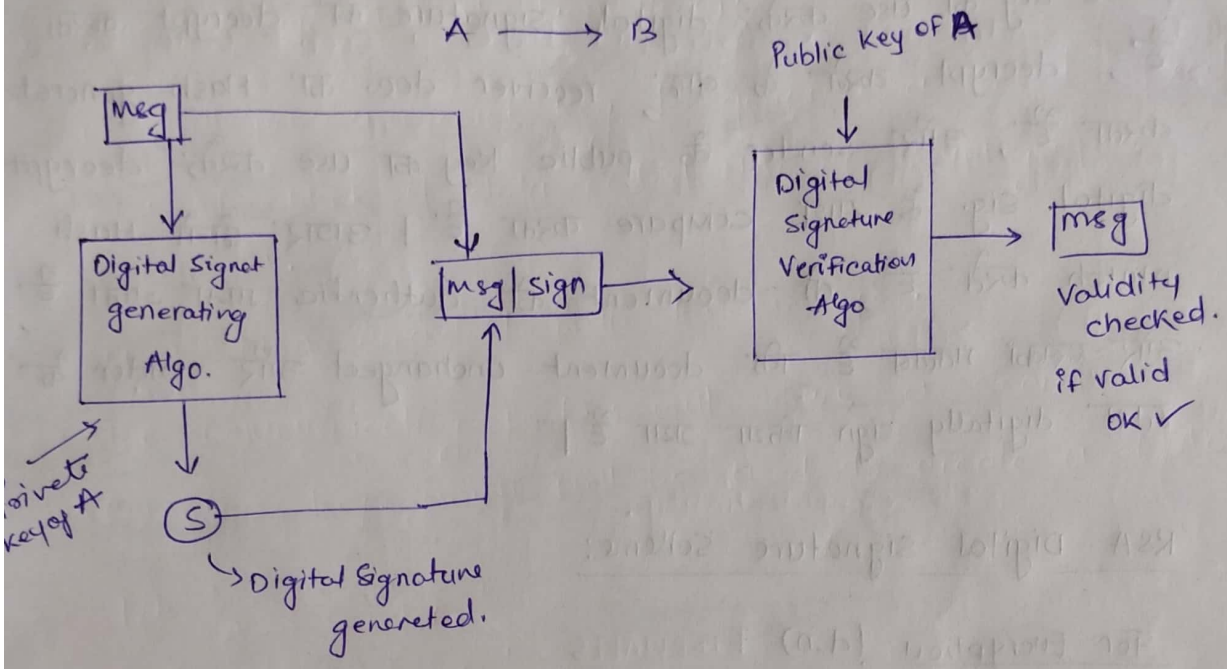


b) Authentication tied to cipher text:



Digital Signature:

- It plays Very imp. role in e-commerce, online transaction etc.
- Based on Asymmetric Key Cryptography.
  Encryption → private key
  Decryption → public key.
- used for msg authentication & non-repudiation & msg integrity.
- Not used for Confidentiality.



- Also provide msg integrity because if msg changed then at receiver side, we will not get the exact msg.
- Signature must use some info unique to the sender to prevent forgery & denial.
- It must be easy to produce digital signatures.
- It must be easy to verify & recognize digital Signatures.
- we need (i) Key Generation Algo → to generate private key.
  (ii) Signing Algo → i/p M and Private key o/p - Digital Sign.
  (iii) Verifying Algo → Using public key & sign.

- जब sender एक doc. digitally sign करता है, तो document के साथ अपने private key का use करता है, private key के use से document के digital fingerprint (Hash) generate होता है, और उस fingerprint को private key से encrypt करके एक digital signature create होती है, यह digital signature document के साथ attach की जाती है।

- जब receiver document और digital signature प्राप्त करता है, तो public key का use करके digital signature को decrypt करता है, decrypt करने के बाद, receiver doc. का Hash generate करता है, और sender के public key का use करके decrypt digital sig. के साथ compare करता है। अगर दोनों Hash match करते हैं, तो document को authentic माना जाता है, और इसका मतलब है कि document unchanged और sender के द्वारा digitally sign किया गया है।

RSA Digital Signature Scheme:

for Encryption (d,n)

Here

For Signing.

$$S = M^d \bmod n$$

यह RSA के उल्टा है।
क्योंकि Signing में sender की private key use हो रही है।

Verifying

for decryption (e,n)

$$M' = S^e \bmod n$$

HASH FUNCTION:

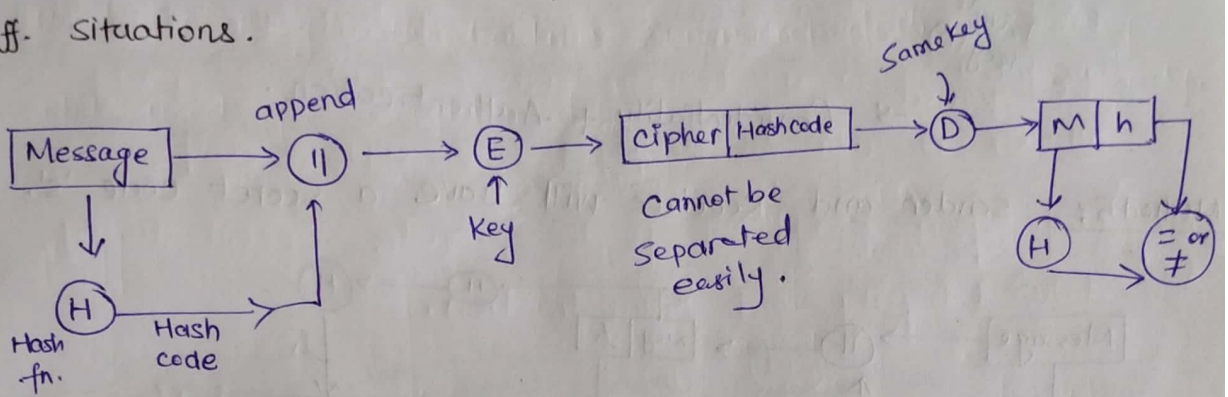
- Similar to MAC, But it doesn't use a key.
- Takes in variable size message and produce a fixed output. → called Hashcode / Hash Value / Message digest.

- The i/p is a message.
- A Hash value [h] is generated by a fn. H

[H(M) = fixed length code 'h'] h → Hash code.

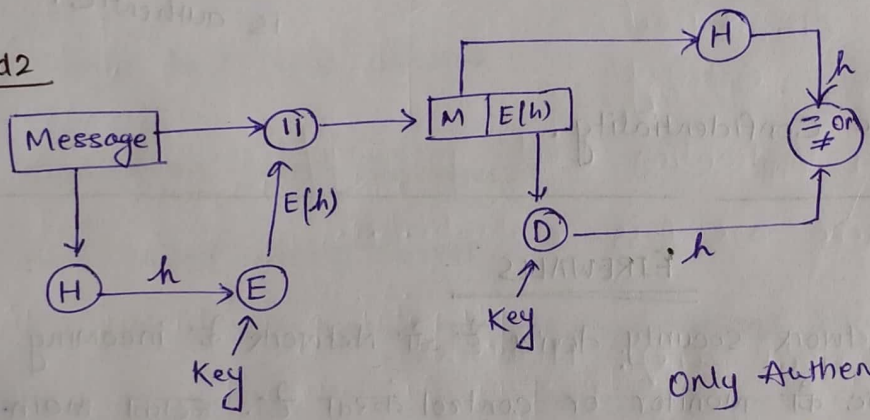
There are diff. method to provide authentication in diff. situations.

1.)



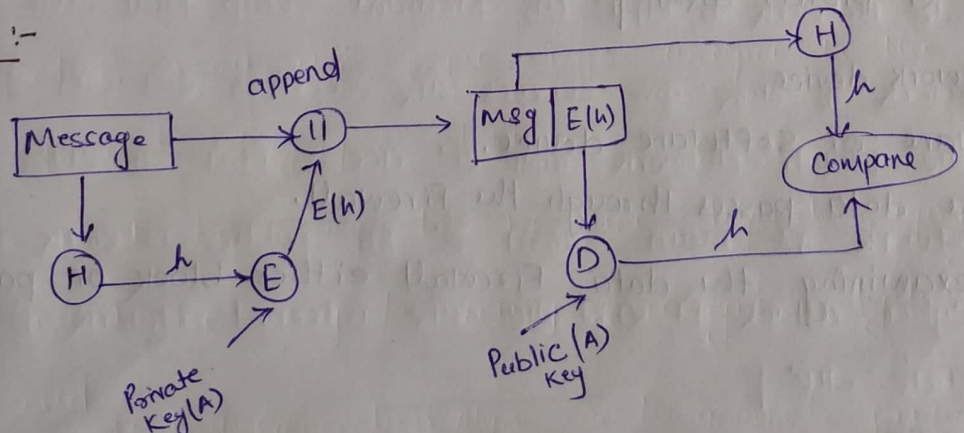
↳ authentication + Confidentiality.

Method2



Only Authentication
No Confidentiality.

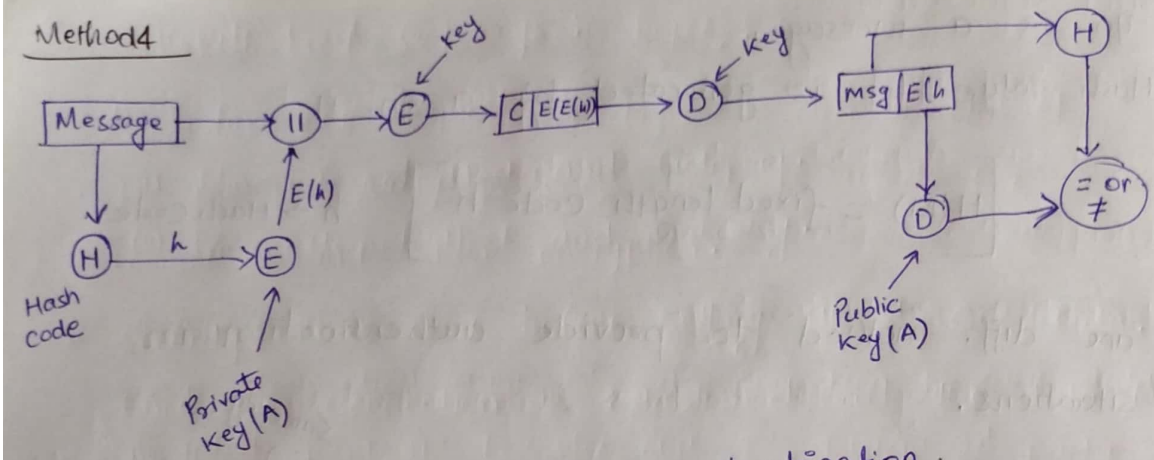
Method3 :-



→ No Confidentiality
→ Only Authentication.

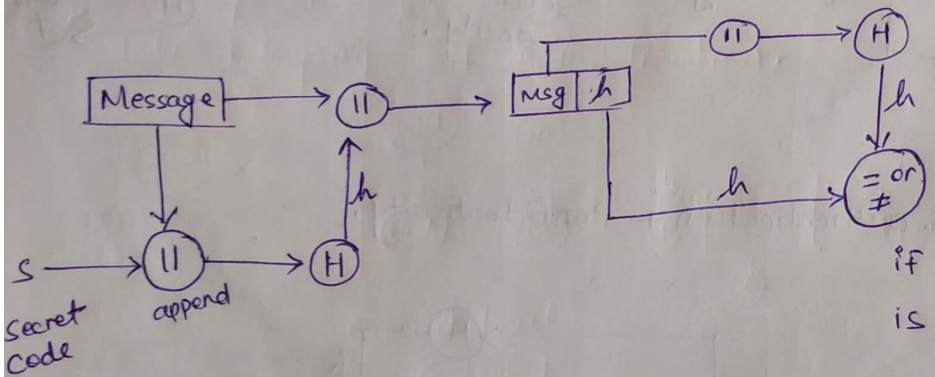
- processing time will be less as the msg is not encrypted.

Method 4



→ Confidentiality + Authentication.

Method 5: Sender and Receiver will have a secret code 's'.

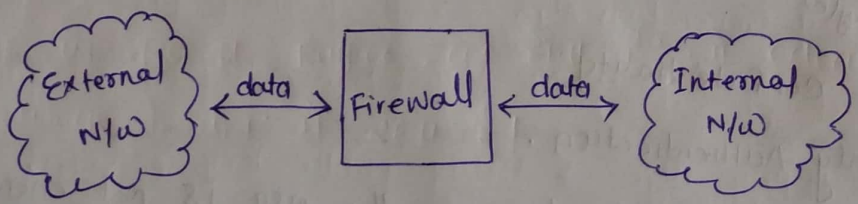


if equal it is authentic.

No Confidentiality.

FIREWALLS

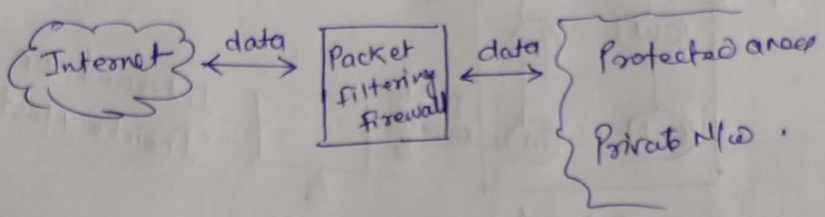
- Firewall एक Network security device है जो Network के incoming and outgoing trafic को monitor or control करता है. इसका main objective है unauthorized access, Maliciow activities or network threats से protect करना।
- A Network device
- Hardware or Software device.
- All the data passes through the Firewall.
- After examining the data, Firewall either block or pass the data.



Types of Firewalls:

1. Packet Filtering Firewalls:

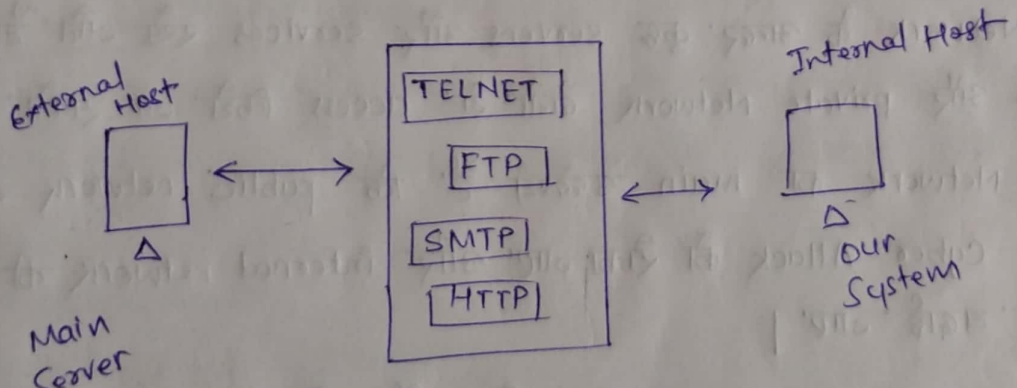
- Applies a set of Rules to each incoming IP packet and then forwards or discards the packet.
- Rules are based on source IP, destination IP, address protocol and ports.
- If rule matches, corresponding action will be taken.
- Otherwise default action is taken (discard).
- It analyses the traffic at transport layer.



- Simple but less Secure.

2. Application level Gateways:

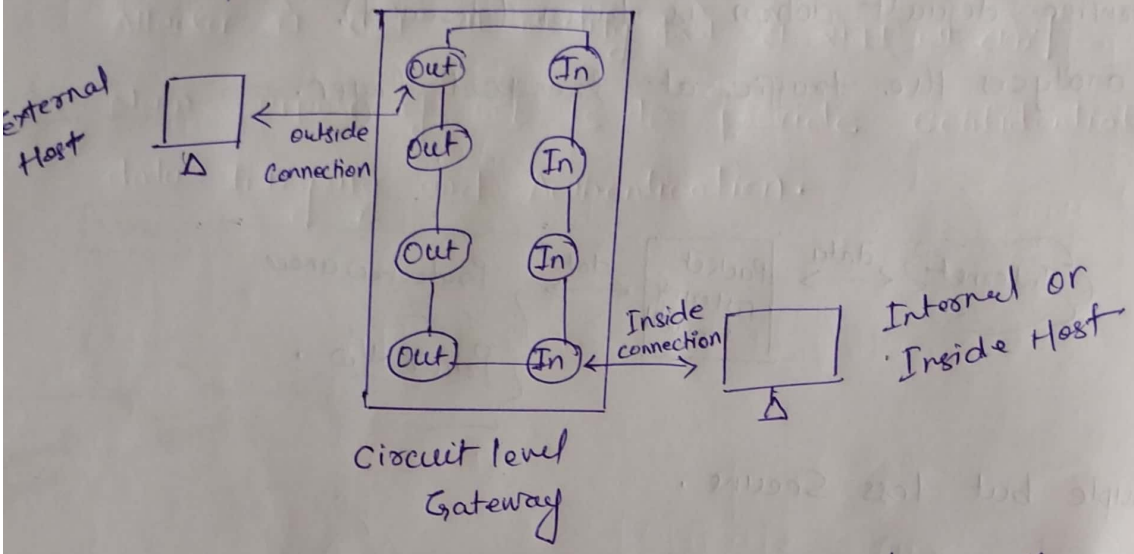
- Also called proxy server.
- Contacts users using TCP/IP applications like (TELNET, FTP ...)
- More secure than packet filtering layer.
- processing overhead. (DisAdvantage).



3. Circuit level Gateways :

→ Uses two TCP connections.
  (i) b/w internal Host and Gateway.
  (ii) b/w external Host and Gateway.

→ Security checks done before setting up a connection. Once the connection is established, all the data will be passed.



— Faster than Application level gateways/firewalls because there are less evaluations.

‡ DMZ (Demiliterized Zone): Networks

- यह एक तरह का Network Architecture होता है, जहाँ पर public और private Network के बीच एक Medium setup किया जाता है।
- इस Network के अन्दर कुछ servers और services रखे जाते है, जो public और private Network दोनों से access किये जा सकते है।

DMZ Network का main उद्देश्य है कि public network से आने वाले Cyber Attack को रोका जाए और internal network की सुरक्षा बढ़ाई जाए।

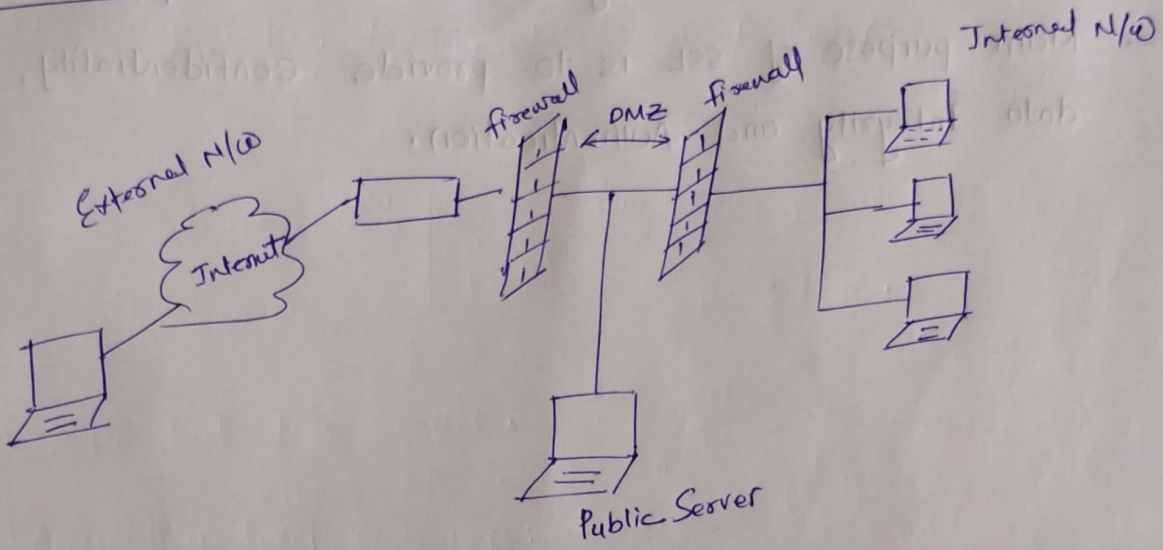
यह एक तरह का Buffer zone होता है, जो external और internal network के बीच में रहता है।

Three Network Interface:

i) Internal private network
ii) External public Network
iii) Connects to public server (DMZ)

- Two firewalls are used: → External N/w and DMZ
  → DMZ and Internal N/w.

- Architecture:



Internet Security protocols:

इसमें कुछ set of rules and guidlines है, जो internt communication और data transfer के लिए use किये जाते है, यह protocol cyber Attack, data breaches और अन्य सुरक्षा संबंधी खतरे से बचाने का काम करता है।

1. IPsec (Internet Protocol Security): यह OSI layer में Network layer पर secure communication को provide करता है। यह VPN और Remote access connections में इस्तेमाल होता है।

Uses:

- Confidentiality
- Authentication/Integrity
- Replay Attack protection.

2. SSL Protocols (Secure Sockets layer):

- Application and Transport layer के बीच में होता है।
- It is a Security protocols, that is used for Secure Connections and data encryption.
- When we use SSL, तो client और Server के बीच एक Secure Connection बनता है, इस connection के द्वारा data encrypted form में transfer होता है, जिससे 3rd party या Attacker को पढ़ने या modify करने से रोका जा सके।
- Main purpose of SSL is to provide Confidentiality, data Integrity and Authentication.