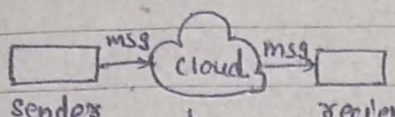
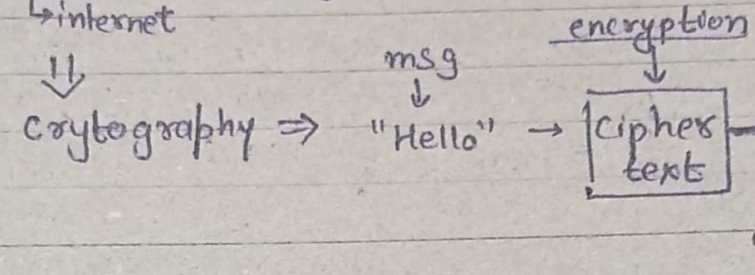
CRYTOGRAPHY (& network Security)



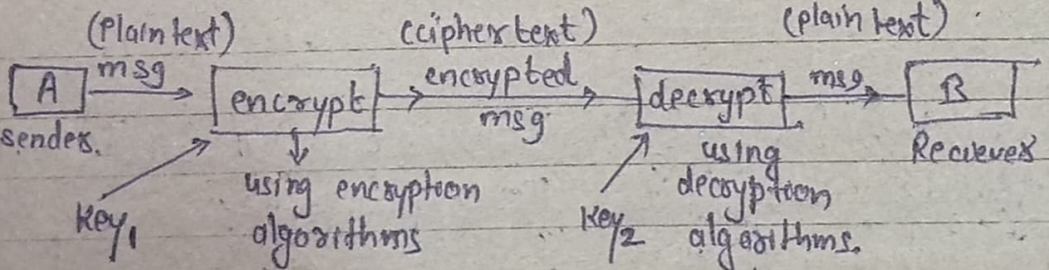
} possibility of data breach or leakage



* ~~Imptnce of~~ Importance of cryptography is for the security of data transmission, no one can corrupt your data, protect valuable data

* The art of protecting info. by transforming it into an unreadable format

* cryptography is about constructing and analysing protocols that prevent third party or the public from reading private messages.



1) if keys are same → Symmetric cryptography
2) if keys are diff. → asymmetric cryptography

Encryption : process of transforming information from readable to unreadable format.
Encryption algorithms are used to encrypt the inform/data

Decryption : process of transforming data/info from unreadable → readable format
decryption algorithms are used to decrypt info/data.

Key → strings of bits used by cryptographic algorithm to transform plain text → cipher text or vice versa.
It is used for secure communication

Types of Cryptography

Symmetric Cryptography

It is the simplest kind of encryption technique that involves only 1 key to encrypt and decrypt (or ciphers and decipher) info.

It is also called Private key/ Secret key cryptography

The most popular system is DES (Data Encryption system)

fastest in execution

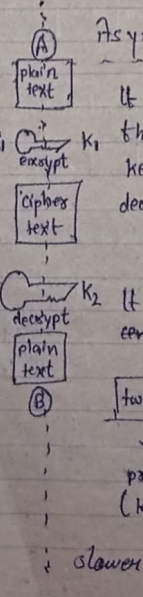
Asymmetric cryptography

It is the encryption technique that involves a pair of key for encryption and decryption of info

It is also called public key cryptography

two key → public key (known to everyone)
private key (known to only particular person)

slower in execution



using private key can be decrypted using public key.

Popular asymmetric key algo → RSA, DSA, Elliptic curve etc.

less complex and less computational power is required	more complex and ∴ more computational power needed
used for the transfer of bulk data (b/c executes faster)	used for secretly exchanging the secret key
Sharing the key in b/w sender and recievers is not safe	no problem of key sharing b/c of private key concept.
Algorithms ⇒ DES, AES, RC4, 2DES, 3DES	Algo ⇒ RSA, Deffie Hellman, DSA, etc.

Security Goals

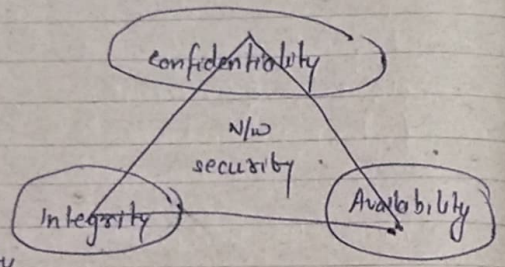
① Confidentiality – It is the most common concept of info. secu. It allows authorized user to access sensitive & protected data. The data sent over the network should not be accessed by unauthorized users / individual.
Attackers will try to capture data. To avoid this, various encryption technique are used to safeguard our data so that even if attacker gains access, he will not be able to decrypt it.

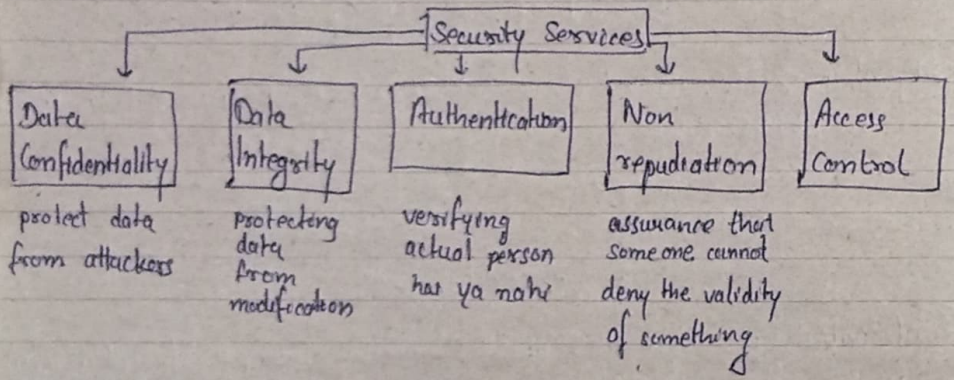
2) Integrity - means that changes need to be done only by the authorized entities and through authorized mechanisms & nobody else should modify our data.

3) Availability - data must be available for the authorized users. Info is useless if we cannot access it.

C. } triad
I } in
A } cryptography
&

confidentiality, Integrity & availability

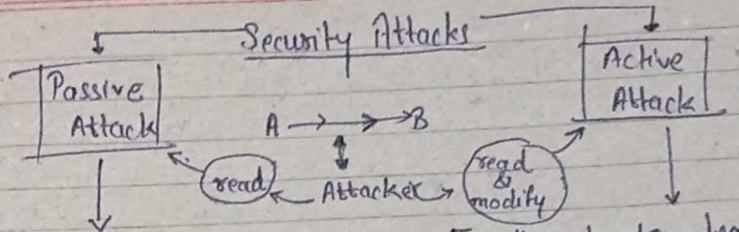




Repudiation ⇒ Denial of truth or validity of something i.e. act of claiming that something is invalid

4) Non Repudiation ⇒ is a service, which provides proof of the origin of data and the integrity of the data

5) Access Control ⇒ to whome the access should be given can be decided or the prevention of unauthorized use of a resource



It attempts to learn or make use of the info from the system but does not affect the system resources.

The attacker will only see the data he will not modify it.

We can prevent it using better encryption technique

It attempts to learn and alter system resources / info.

he can see + modify msg.

Types

1. Release of message content
The attacker/hacker will easily be able to understand the data/info

2. Traffic analysis
If we have encryption protection, an opponent might still be able to observe the pattern of these msg
The attacker could determine the location and the identity of communication host

Types

1. Masquerade
When one entity pretends to be another entity

2. Modification of msg
Some portion of the msg is altered or the msg is delayed or reordered to produce unauthorized effect

and could observe the frequency and length of the msg being exchanged.

This info might be helpful in guessing the nature of communicatⁿ that was taking place

③ Replay
It involves passive capture of a msg and its subsequent retransmission to produce an unauthorized effect

④ Denial of Services
It prevents normal use of communication facilities by overloading or disabling the network

Passive attacks are difficult to detect b/c they donot involve any alteration of data.
So, the sender & receiver will not be able to know whether a third person is reading their msg or not

Security Mechanisms

Security mechanisms are used to provide security.

1) Encipherment → The use of mathematical algos to transform data into a form that is not readily intelligible to cipher text (plain text → cipher text)

2) Digital Signature → It is a 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 sensor for authentication.

3) 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 new checkvalue from the received data and compare the newly created check-value with the one received.
If both the values are same the integrity of the data has been perished

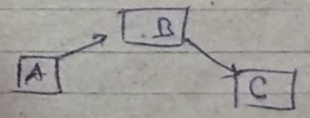
4) Authentication exchange - In this, two entities exchange some messages to prove their identity to each other

5) Traffic Padding - In this technique we add some extra bits with the data while encryption.

6) Routing Control → Means selecting & continously changing different available routes b/w the sender & the receiver to prevent the attacker from eavesdropping on a particular route

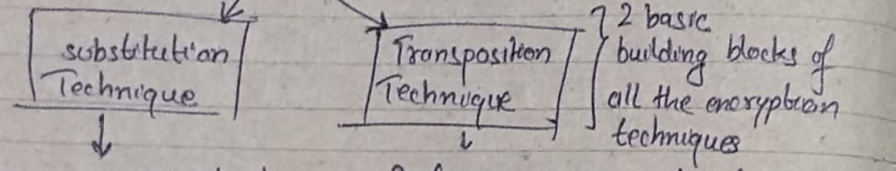
7) Access control → These methods proves that a user has access right to the data.

8) Notarization → means selecting a third trusted party to control the communication b/w two entities. This can done (for eg) to prevent repudiation



Classical Encryption Technique

Symmetric encryption also reffered to as conventional encryption is of 2 types or we can say it has 2 technique

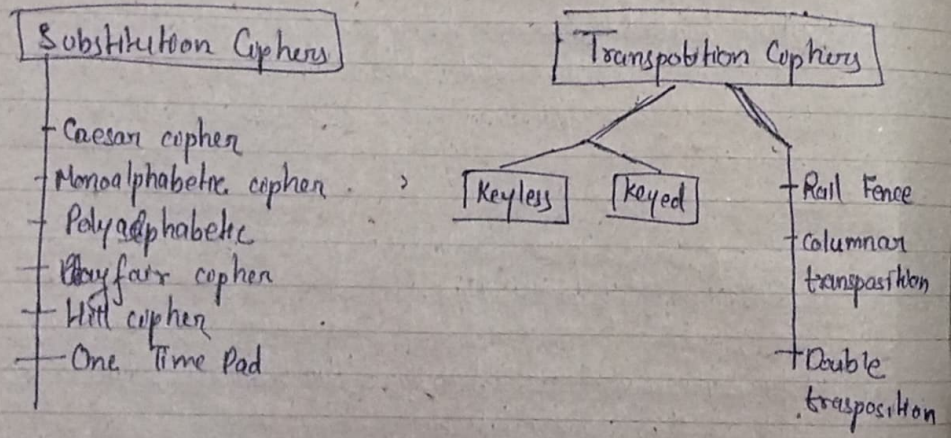


① It the one in which the letters of the P.T. are replaced by other letters or by numbers or symbols

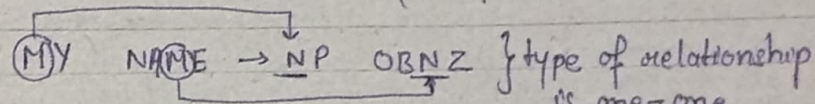
Name → IWPX

② Performing some sort of permutation on the p.T. letters i.e. it recordes the symbols i.e. rearrangement of the letters of P.T.

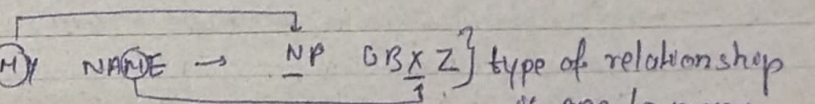
Name → amNe or emaN



Monoalphabetic Substitution ciphers: A single cipher alphabet for each plain text alphabet is used throughout the process.
i.e. fixed substitution : if 'N' → "I" use X always, using 'X' only in place of 'N'



Polyalphabetic Substitution ciphers: There is no fixed substitutions. Each occurrance of a character may have a diff. substitute.
i.e. we can use more than 1 substitution for the same letter.

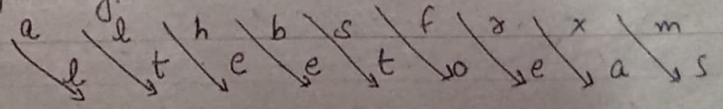


Transposition Technique

1) No replacement of character
2) we will rearrange the charater position i.e. we will apply some sort of permutation on the plaintext letter

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

e.g. "all the best for exams" → plaintext rows → 2/3/4...
To encrypt this with a rail fence of depth2, we write the following.



encrypted msg is :-
ALHBSFRXMLTEETOEAS

Note → used for short messages
→ easy to break by the attacker

Row transposition cipher

We write the message in a rectangle, row by row, and read the msg off, column by column, but permute the order of column.

Key → integer value (unique digits from 0-9)

e.g. 45312
e.g. 4321 etc.

{ numbering on the basis of alpa. order } if given key is CRYPTO → convert into int ⇓ 146352

↳ In key there should not be any repetition.

eg Plain text → attack postponed until two am

Key →	4	3	1	2	5	6	7
	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	x	z

extra/dummy bits

[Sometimes left blank (Irregular case)]

cipher text:
↳ TTNA APTM TSUO AODW COIX KNLY PETZ
1 2 3 4 5 6 7

explanation → 1) To encrypt, start with the column labelled as (1) in our example column 3.
write down all the letters of the column.

2) Now, proceed to column no. 4 which is labelled as column (2), then , 2, 1, 5, 6 and 7th column.

Problem → can easily be understood by the attacker / 3rd party
→ used for short msg.. only.

It can be made more secure by performing more than 1 stage of transposition so, the result will be a more complex permutation.

Key →	4	3	1	2	5	6	7
	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

→ NSCY AUOP TTWL
TMDN AOIE PAAT
TOKZ } there is no space in b/w

Double transposition : * columnar transposition / Row transposition cipher applied twice
* The key in case 2 can be same / diff 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 used as → 564321] → decoded by the alphabetical order of letters in the key

key

3	1	4	5	2
1	2	3	4	5

encryption ↓ ↑ Decryption

encryption (enemy → ecmyn) decryption.

Caesar Cipher

* It is also called shift ciphers/ additive ciphers.
* Each letter in the plaintext is replaced by a letter corresponding to a no. of shifts in the alphabet.
* It is a monoalphabetic caesar cipher.
* It is one of the earliest and simplest method of encryption tech.

Note: Julius Caesar used an additive cipher to communicate with his officers. For this reason, additive ciphers are sometimes called ~~case~~ caesar ciphers.

He used a key of 3 for communications

plain →	Meet	me			
cipher →	PHHW	PH			

Z	e	b	r	q
C	H	E	U	D

Cipher text

$$C = E(K, p) = (p+k) \bmod 26$$ *encryption

(p: message, k: key, plain)

For decryption

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

if (C-K) is -ve then add 26 to it

Numerical value is assigned to each letters

a	b	c	d	e	f	...	x	y	z
0	1	2	3	4	5	...	23	24	25

If the cryptanalyst/attacker knows a cipher text, then he can apply brute force technique to find the plain text by using all the possible 25 keys.

key PHHW PH

3 → [(P-3)(H-3)(H-3)(W-3)]%26 [(P-3)(H-3)]%26

meet me

P = 15 - 3 = 12 = M

since it is a part of asymmetric encryption same key is used for encryption & decryption

$1 \le K \le 25$

message → "HELLO"

let key = 4

C(H) = (p+k) mod 26 = (7+4) mod 26 = 11 = L

C(E) = (p+k) mod 26 = (4+4) mod 26 = 8 = I

C(L) = (p+k) mod 26 = (11+4) mod 26 = 15 = P

C(O) = (p+k) mod 26 = (14+4) mod 26 = 18 = S

cipher → LIPPS

Decryption C = LIPPS

$P = (C-K) \text{ Mod } 26$

$P(L) = (L-4) \text{ Mod } 26 = (11-4) \text{ mod } 26 = 7 = H$
$P(I) = (I-4) \text{ mod } 26 = (8-4) \text{ mod } 24 = 4 = E$
$P(P) = (15-4) \text{ mod } 26 = (11) = L$
$P(S) = (18-4) \text{ mod } 26 = (14) = O$

text = HELLO

Playfair Cipher Algorithm

It was invented in 1854 by charles wheatstone. But was named after Lord playfair, when promoted the use of cipher.

cipher → Algo for encrypting and decrypting.

cipher text → process which applies different types of algos to convert plaintext → coded is called cipher text.

Algorithm

1) Create 5x5 matrix that is called guid 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 & J will be combined together
3) convert the text into ~~plain~~ pairs of alphabet
   e.g. Heya → He ya
4) pairs cannot be made with same letters. Break the letters into single and add 'X' to the previous letters

   eg. HELLO → He lx lo
   Helloe → He lx lo e = alone problem.

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
(but if x is already there the add 'z' to it)

4) Code will be forced using 3 rules:
   i) If both the alphabets are in the same row, replace them with alphabets to their immediate right
   ii) If both alphabates are in the same column, replace them with alphabets immediately below them.
   iii) If not in same row/columns replace them with alphabets in the same row respectively, but at other pair of corners.

Key → Abhi

Plaintext → BM → ER

RW → WB

FG → GK

UQ → QR

QW → RV

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

KL ⇒ DP
KS ⇒ FU

FL ⇒ DN (row wise)

Vigenere Cipher

i) desined by Blaise de Vigenere (16^{th} cent. French Mathem.)

ii) It is a polyalphabatic substitution cipher.

The encryption is done using a (26×26) matrix or ie a Table

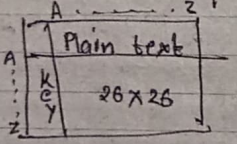
Method ① → Vigenere Table → used to find the ciphere text.

eg: Plain text = GIVE MONEY
Key = LOCK

Soln

G	I	V	E	M	O	N	E	Y
L	O	C	K	L	O	C	K	L

Repeat the letter of the key so that the no. of letters in P & K ie. plain text and key becomes equal



Cyphere → RWXOXCPOJ

For Decryption,

Cipher →	R	W	X	O	X	C	P	O	J
key →	L	O	C	K	L	O	C	K	L
↓ Rows in table									
plain →	G	I	V	E	M	O	N	E	Y

method-2 when table is not given.

1) Encryption

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

2) Decryption

$D_i = (E_i - K_i) \bmod 26$ // D_i → Decryption.

eg: plain text → "she is listening"
key → "PASCAL"

∴ Key stream → (15, 0, 18, 2, 0, 11) The key stream is the repetition of this initial key stream (as many times needed.

P	S	H	E	I	S	L	I	S	T	E	N	I	N	G
P_i →	18	7	4	8	18	11	8	18	19	4	13	8	13	6
K_i →	15	0	18	2	0	11	15	0	18	2	0	11	15	0
C_i	7	7	22	10	18	22	23	18	11	6	13	19	2	6
C →	H	H	W	K	S	W	X	S	L	G	N	T	C	G

← $(E_i - K_i) \bmod 26$

← $(P_i + K_i) \bmod 26$

VERNAM CIPHER

i) Used for encrypting alphabetic text.
ii) Simply a type of substitution cipher

In this, we assign a number to each character of plain-text like (a=0, b=1, c=2, ... z=25).

Length of key used for encryption = Length of plaintext

eg: Plain Text → RAMSWARUPK
Key → RANCHOBABA

Plain text →	17	0	12	18	22	0	17	20	15	10
Key →	17	0	13	2	7	14	1	0	1	0
(PT + key) →	34	0	25	20	29	14	18	20	16	10
if > 26 -26 →	8	0	25	20	3	14	18	20	16	10
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
if < 0 +26 →	17	0	12	18	22	0	17	20	15	10
plain text →	R	A	M	S	W	A	R	U	P	K

HILL CIPHER ~ Poly Alphabetical cipher

* developed by Lester Hill in 1929
* encrypts a grp of letters called polygraph (like in playfair cipher, we saw it was encrypting a pair of letter which was called as a digraph), so, here it can be a polygraph (digraph, trigraph, etc)
* This method makes use of mathematics

To encrypt $C = KP \bmod 26$ (K: key, P: Plain text.)

Step 1 → choose a key (key matrix must be a square matrix)

we can take any key

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

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

eg: Plain text = ATTACK
Let key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

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

So, $\begin{bmatrix} A \\ T \end{bmatrix} \begin{bmatrix} I \\ A \end{bmatrix} \begin{bmatrix} C \\ K \end{bmatrix}_{ex1}$ if nxn then nx1 ?

Now, encryption begins,

i) so, 1st vector → $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 10 \\ 19 \end{bmatrix}$, key $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

$C = KP \bmod 26$

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

$C = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix}$

corresponding alphabets = $\begin{bmatrix} F \\ K \end{bmatrix}$

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

ii) Now 2nd vector $\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

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

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

TA becomes MF

iii) $\begin{bmatrix} C \\ K \end{bmatrix} \rightarrow \begin{bmatrix} 2 \\ 10 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$

CK becomes IO

Plain Text => ATTACK
Cipher text => FKMFIO

} polyalphabatic cipher

Now, Decryption

Find inverse of key matrix K^{-1}

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

eg plain → ATTACK , key $K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

cipher → FKMFIO

$C = FK\ MK\ IO$

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

determinant of Matrix ⇒ $d = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$ $d = |ad - bc|$

eg $d = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = |12 - 9| = 3$ ∴ determinat value $d = 3$

Now find multiplicative inverse of determinant.

i.e $dd^{-1} \equiv 1 \bmod 26$ (Identity matrix).

$3d^{-1} \equiv 1 \bmod 26$

so, $d^{-1} = 9$

use hit & Trial method

$1 \bmod 26 = 1$
$3 * d^{-1} \bmod 26 = 1$
$3 * 9 \bmod 26 = 1$
$27 \bmod 26 = 1$

another example

$5 * x \equiv 1 \bmod 26$

Let $x = 5$

$5 * 5 \bmod 26 = 25$

$x \neq 11$

$5 * 11 \bmod 26 = 3$

let $x = 21$

$5^x \bmod 26 = 105 \bmod 26 = 1$

Multi Inverse of $5 = 21$

$26(n) + 1$

So, till now determinant $d = 3$

$d^{-1} = 9$

Now we will find adjoint of the matrix.

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

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

Before decryption, we have to remove -ve value.

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

$adj(K) = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$ and $d^{-1} = 9$

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

$= d^{-1} adj(K)$

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

Now find its modulo 26

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

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

No, we will decrypt it.

cipher = FK MF IO

$C = \begin{bmatrix} F \\ K \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}$ $\therefore$ plain text, $P = K^{-1} C \bmod 26$

$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \bmod 26$

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

Similarly

$C = \begin{bmatrix} M \\ F \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$ $\therefore$ $P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 24 + 125 \\ 300 + 90 \end{bmatrix} \bmod 26 = \begin{bmatrix} 149 \\ 390 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 17 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$

again

$C = \begin{bmatrix} I \\ O \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$ $\therefore$ $P = \begin{bmatrix} 2 & 25 \\ 22 & 18 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \end{bmatrix} \bmod 26$

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

Plain text ⇒ ATTACK

HILL CIPHER (3×3) matrix example:

Let plaintext = "SAFEMESSAGES"

Let key = "CIPHERING" = $\begin{bmatrix} C & I & P \\ H & E & R \\ I & N & G \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$

Since, key is a 3×3 matrix, plain text should be converted into column vectors of length 3 ie.

(n×1) matrices → (3×1) matrices

So, we get SAF EME SSA GES

$\begin{bmatrix} S \\ A \\ F \end{bmatrix} \begin{bmatrix} E \\ M \\ E \end{bmatrix} \begin{bmatrix} S \\ S \\ A \end{bmatrix} \begin{bmatrix} G \\ E \\ S \end{bmatrix}$

$C_1 = KP \bmod 26$

$C_1 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 111 \\ 211 \\ 174 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix} = \begin{bmatrix} H \\ D \\ S \end{bmatrix}$

$C_2 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 164 \\ 144 \\ 212 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} I \\ O \\ E \end{bmatrix}$

$C_3 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 180 \\ 198 \\ 378 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 \\ 16 \\ 14 \end{bmatrix} = \begin{bmatrix} Y \\ Q \\ O \end{bmatrix}$

$C_4 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 314 \\ 364 \\ 208 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} C \\ A \\ A \end{bmatrix}$

∴ SAFEMESSAGE ⟶ HDSIOEYQOCAA

encrypt → $C = KP \bmod 26$

Decrypt → $P = K^{-1}C \bmod 26$

Plain text → SAFEMESSAGE

Cipher ⟶ HDSIOEYQOCAA

key k = CIPHERING = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$

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

$d = \begin{vmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 16 \end{vmatrix} = 2(64 - 13(17)) - 8(7(16) - 8(17)) + 15(91 - 32)$

$= 1243$

$d \cdot d^{-1} = 1 \bmod 26$

$1243\,(d^{-1}) = 1 \bmod 26$

$k = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} = 64 - 15(17) = -197$

$= 7(16) - 17(8) =$

$\begin{bmatrix} -197 & -94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix}$ ⟸

↳ cofactor matrix,

$= 24 - 17(13) = -197$

$= 42 - 17(8) = -94$

$= 91 - 32 = 59$

$= 48 - 15(13) = -147$

$= 12 - 15(8) = -108$

$= 26 - 64 = -38$

$= 68 - 60 = 8$

$= 34 - 105 = -71$

$= 8 - 42 = -34$

$adj(k) = \begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix}$ ← Adjoint matrix.

Removing -ve sign.

$adj(k) = \begin{bmatrix} -197+26(7) & 147 & 76 \\ 94 & -108+26(5) & 71 \\ 59 & 38 & -48+2(26) \end{bmatrix}$

$= \begin{bmatrix} 11 & 147 & 76 \\ 34 & 22 & 71 \\ 59 & 38 & 4 \end{bmatrix}$

$K^{-1} = \begin{bmatrix} 55 & 735 & 380 \\ 470 & 110 & 355 \\ 295 & 190 & 20 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}$

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

$P_1 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix} \text{Mod} = \begin{bmatrix} 380 \\ 338 \\ 447 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} S \\ A \\ F \end{bmatrix}$

// $\begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 186 \\ 168 \\ 264 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} = \begin{bmatrix} E \\ M \\ E \end{bmatrix}$

// $\begin{bmatrix} 24 \\ 16 \\ 24 \end{bmatrix} \text{Mod } 26 = \cdots = \begin{bmatrix} S \\ S \\ A \end{bmatrix}$

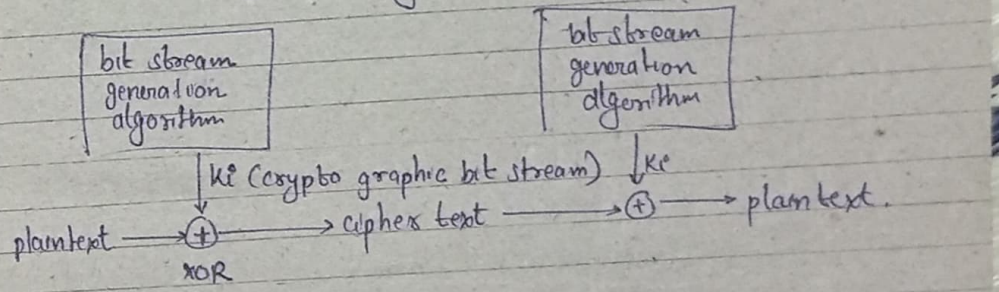
// $\begin{bmatrix} \cdot \\ \cdot \\ \cdot \end{bmatrix} \text{Mod } 26 = \cdots = \begin{bmatrix} G \\ E \\ S \end{bmatrix}$

Stream Cipher & Block Cipher

* used to convert plain text → cipher text.

1) Stream Cipher : It is the one that encrypts a digital data stream one bit or 1 byte at a time.
It is a symmetric key cipher (i.e. key for encrypt & Decrypt)

generate key in the form of bit



eg:
```
  1 0 1 1 0 1 1 0   → plaintext
⊕ 0 1 0 1 0 1 0 1   → key.
-----------------
  1 1 1 0 0 0 1 1
```

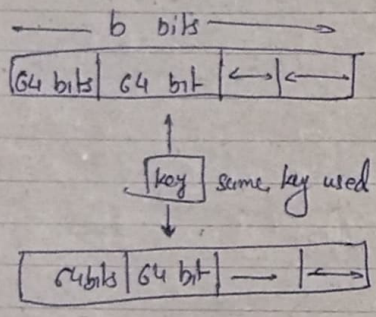
to decrypt.
```
  1 1 1 0 0 0 1 1   ← cipher
  0 1 0 1 0 1 0 1   ← key
-----------------
  1 0 1 1 0 1 1 0   → plaintext
```

2) Block cipher : In this, a block of plain text is treated as a whole and used to produce the cipher text of equal length.

Typically a block size of 64 and 128 bits

* symmetric key cipher (1 key used only)

* key will be applied on each block.



eg of block cipher

→ DES (64 bit block size) cipher & plain text.

Shannan's theory of confusion & Diffusion

① The terms confusion and diffusion were introduced by claude

② Shannan's concern was to prevent crypto analysis, based on statistical analysis. The reason is as follows:

Assume attacker has some knowledge of the statistical characteristic of the plaintext (eg in a msg, the frequency distribution of the various letters may be known)

If these statistics are in any way reflected in the ciphertext,

Block ~~Stream~~ cipher	~~Block~~ Stream Ciphers
① Plain→cipher text by taking plain text block at a time.	1 bit or 1 byte of plain→cipher text
② It uses 64 bit or more	Stream cipher uses 8 bits
③ Complexity of block cipher is simple	while stream cipher is more complex
④ uses confusion as well as diffusion concept.	uses only confusion concept
⑤ In this reverse encrypted text is hard	Reverse encrypted text is easy (user have to do XOR again)
⑥ ECB (electronic code book) CBC (Cipher Block chaining) algorithmic modes are used.	CFB (cipher feedback) OFB (output feedback) algorithmic mode used

the crypto ~~reflected in the ciphertext, the~~ ie attacker may be able to deduce the encryption key.

Theus shannon suggested 2 methods for frustating the attacker.

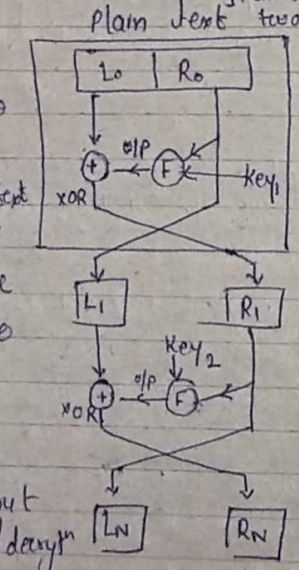
① Confusion
② Diffusion
} properties for creating a secure cipher

Diffusion : In simple words, if a symbol in the plaintext is changed, several or all symbols in the cipher text will also change

The idea of diffusion is to hide the relationship b/w the ciphertext and plain text

Confusion: It hides the relationship b/w cipher & the key.
If a single bit in the key changed then most/all bits of the cipher text will also be changed

Fiestel Cipher Structure
* most of the block ciphers technique follows this structure
i) The plain text is divided in 2 equal halves L_0 & R_0
→ The 2 halves of the data pass through n rounds of processing and then combine to produce the ciphertext block
→ On the right half we apply a function and in the fn we will use a subkey generated from the master key.
The o/p of this XORed with the left half and these o/p will be swapped.



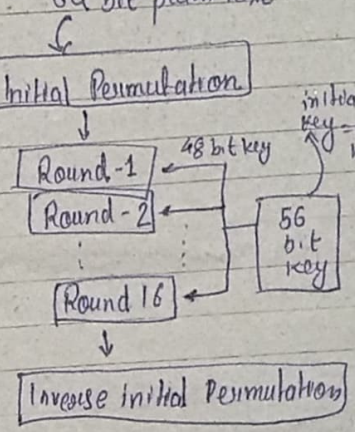
→ we will have n-rounds depends on algo
If any algo, we divide the plaintext in 2 halves & apply the fn on RHS and XOR, it with the LHS & the op is swapped then, that algo follows fiestel structure.

Block size: Larger size, more security
Key ": ↑ key size, means security but may decrease speed of encrypt/decrypt
no. of rounds: ↑ rounds, ↑ secure
Subkey generation algo: more complex algo, harder for attackers to steal
function / Round function F: more complex fn, harder for the cryptanalyst to check.

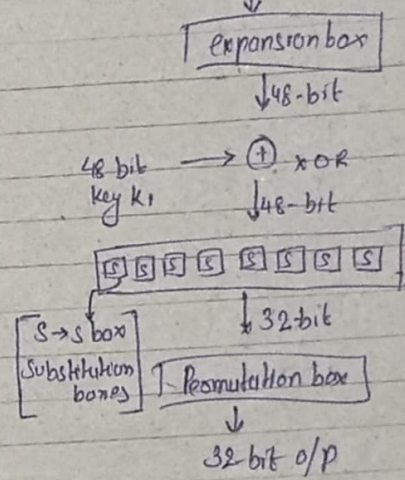
→ Data Encryption Standard
② Symmetric cipher
③ 64-bit plain text block
④ 16 rounds of fiestel structure

DES → ① Initial permutation
② 16 fiestel rounds
③ swapping / left right swap
④ final permutation / Inverse Initial Permutation

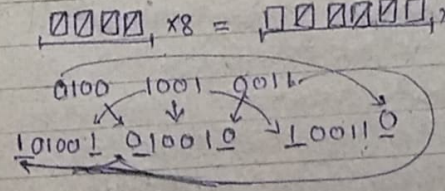
Basic structure



Function definition



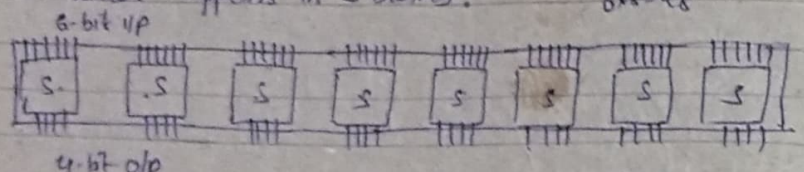
④ What happens in expansion box
32-bit data will be → 1's & 0's form, 32/8→4, 48/8→6

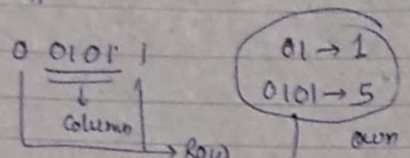


so the original values will be in the middle. and the 1st & last block will take value from previous block's last bit & next block's first bit

There were 8 blocks of 6 bits now, these 48 bits XOR with 48 bit key

Now what happens in S-boxes?





01 → 1
0101 → 5

Every S-box has its own unique table having diff values at differ. intersection of rows & columns.

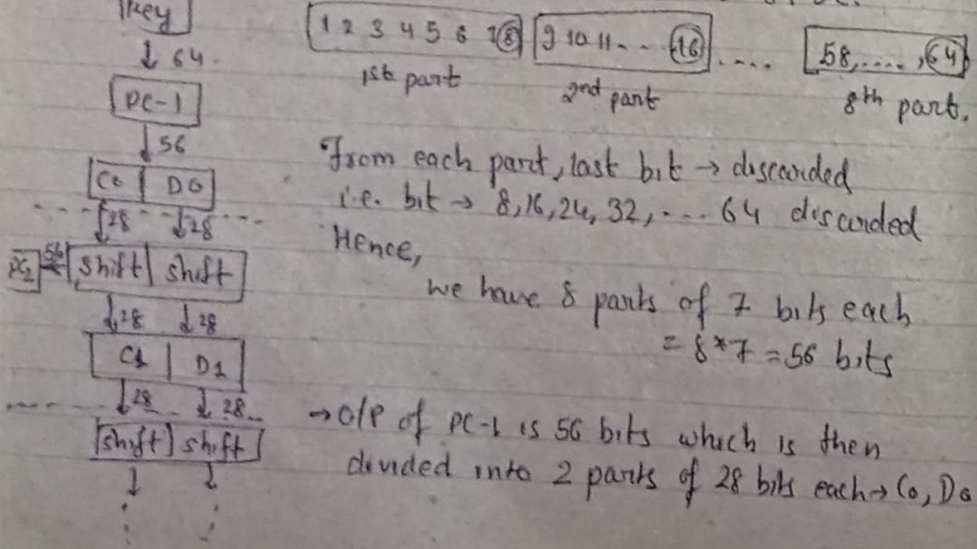
the intersection of rows & column will gives out the value

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

64 bit key divided into → 8 parts each of 8 bit
8*8 = 64 bit.



1 2 3 4 5 6 7 (8) | 9 10 11 ... (16) | ... | 58, ... (64)
1st part, 2nd part, 8th part.

From each part, last bit → discarded
i.e. bit → 8, 16, 24, 32, ... 64 discarded

Hence,
we have 8 parts of 7 bits each
= 8*7 = 56 bits

→ o/p of PC-1 is 56 bits which is then divided 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 ie rotated left by 1 bit.

In other words,
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 bits using 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 Now 48 selected?
Left half (C_1 7, 8, 22, 25 position bits are missing) ie 24 left
Right half D_1 (35, 38, 43, 54 position bits are missing) ie remaining ie 24 left.

DES Analysis

Properties

1) Avalanche effect → It means a small change in plain text (or key) should create a significant change in the ciphertext.
DES has been proved to be strong with regard to this property.

eg: Plain → 0000000000000000
Cipher → 4789FD476E82A5F1
Plain → 0000000000000000
0A4ED5C15A63FEA5

key used is same say key = 2223451298788825

Although there two plain texts differ only in 1 bit, cipher text block differs a lot/significantly

2. Completeness effect → It means that each bit of the ciphertext needs to depend on many bits on the plaintext.
The confusion and diffusion produced by D-boxes & S-boxes in DES, show a very strong completeness effect.

DES weakness

- Key size : Critics believe that the most serious weakness of DES is its key size of 56 bits.
b/c, with todays technology (like parallel processing a powerful processor) it can easily be cracked. (256 keys)

→ ∴ we use triple DES (2DES) with
two keys (112 bits)
triple DES with 3 keys (168 bits)

ii) Weak keys → four out of 256 keys are called weak keys.
~~after the parity drop~~ a weak key is the one which after the parity drop consist of ~~of~~ all 0's, all 1's or half 0's and half 1's

* The disadvantage of using a weak key is:
If we encrypt a block with a weak key and subsequently encrypt the result with the same weak key, we get the original block.
The process creates the same original block if we decrypt the block twice.

(So, if after a 2 decryption, if the result is the same then, attacker is successful

iii) Semi weak key → six key pairs are called semi weak keys
A semi weak key creates only two different round keys, and thus each of them is repeated 8 times. (

iv) Possible weak keys : There are 48 keys that are called possible weak keys.
A possible weak key is a key that creates only 4 distinct round keys, in other words, the 16 round keys are divided into 4 grps and each grp is made of 4 equal keys.

v) Key clustering : means 2 or more dif keys can create the same ciphertext from the plaintext.

Weakness in cipher Design
i) Two specifically chosen i/ps to S-box array can create the same o/p

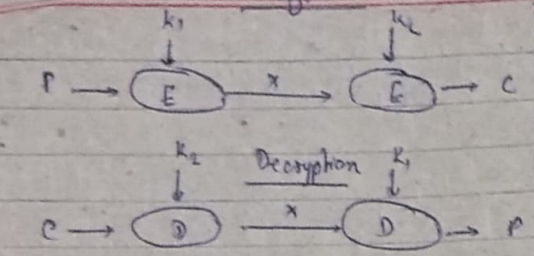
---

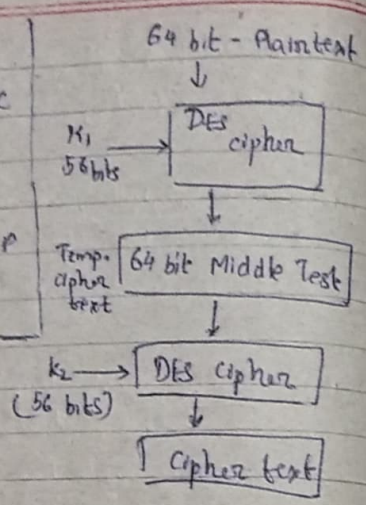
Multiple DES → Double DES (2DES)
→ Triple DES (3DES)

Since DES attack was vulnerable to brute force attack, variation of DES called multiple DES were introduced

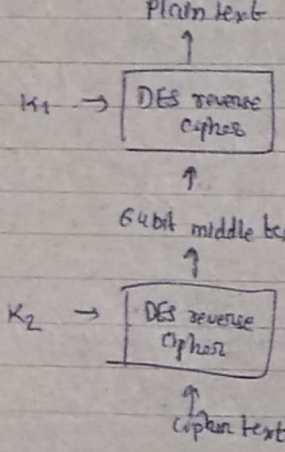
1. Double DES : uses 2 dif keys (56+56) = 112 bit key.
→ Double encryption occurs as follows:
P → E (K1, P)
↓
E(K2, E(K1, P)) = Cipher

Encryption





→ For decryption,
1st decrypted using key K_2 which produces single encrypted ciphertext,



In decryption, keys are applied in reverse order

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

Drawback of Double DES : (Meet-in-the-middle attack.)

This attack involves encryption from 1 end and decryption from the other end and then "Matching the result in the middle" (MIM attack)

This attack requires knowing some plaintext / ciphertext.
Let us assume Plaintext = P, ciphertext = C.

Some pair of

plain text known & ciphertext known

current pairs of all 2^{56} possible values of K_1

decrypt pairs of all 2^{56} possible values of K_2

no. of rows in Table = no. of possible secret keys	Plain	cipher	Middle
2^{56}	...	...	
	...	...	
	...	...	

cipher	middle	cipher
..		
..	..	
..	..	

So, AT the results in table 1
→ (K_1, K_2)
→ (K_1, K_2)

→ we will compare these values with the values of the 1st table computed earlier.

$$\text{Decrypt}(K_2, C) = \text{Encrypt}(K_1, P)$$

∴ (K_1, K_2) is the key pair used.

The attack proceeds as follows:
i) Encrypt P for all 2^{56} possible values of K_1 and store the result in a table ~~sort~~ and sort it.
ii) Now, decrypt C using all 2^{56} possible values of K_2. As each 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.

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.

So, it takes twice as long to break double DES using brute force.

---

* Triple DES → 2 or 3 keys are used
→ much stronger then double DES.