TUTORIAL NO - 03

1 Write a short note on General Greedy Method.

- The greedy method builds a solution in stages. At every stage, it selects the best choice concerning the local considerations.
- A locally optimal partial solution cannot be altered later. Such locally optimal partial solutions generated at each stage, finally build a global solution.
- Thus, the greedy approach provides a step-by step progressive solution by expanding a partial solution at every stage until the global solution is built. The global solution is not always optimal.
However, many times it proves to be an optimal solution.
- The greedy approach is simpler and quite powerful to solve a wide variety of optimization problems.
- The greedy method is used to solve the optimization problem which means the problem asks for either minimum result or the maximum result.
- Some of the classic problems that can be solved effectively by the greedy method are listed below:

1. Knapsack problem
2. Job sequencing problem
3. Minimum spanning tree problem
4. Optimal storage on tapes problem.

2 Solve the knapsack problem, n=4, m=30 profit $(P_1, P_2, P_3, P_4) = (27, 20, 24, 15)$ and weight $(w_1, w_2, w_3, w_4) = (15, 10, 18, 10)$.

item	i_1	i_2	i_3	i_4
Profit	27	20	24	15
Weight	15	10	18	10
P_i/w_i	1.8	2	1.33	1.5

Weight of knapsack = 30

~~P_1/w_1~~ ~~$\sum w_i x_i$~~ ~~$\sum p_i x_i$~~

Item	Profit	Weight	Remaining Weight
i_2 (1)	20	10	30-10=20
i_1 (1)	27	15	20-15=5
i_4 (1/2)	7.5	5	5-5=0

Total profit : 20+27+7.5 = 54.5

Total Weight : 10+15+5 = 30.

3 Find an optimal solution to the knapsack instance $n=6$, $c=20$.
Profit $(P_1, P_2, P_3, P_4, P_5, P_6) = (12, 5, 15, 7, 6, 18)$
Weight $(w_1, w_2, w_3, w_4, w_5, w_6) = (2, 3, 5, 7, 1, 15)$

item	1	2	3	4	5	6
Profit (P_i)	12	5	15	7	6	18
Weight(w_i)	2	3	5	7	1	15
P_i/w_i	6	1.66	3	1	6	1.2

Item	Profit	Weight	Remaining Weight
x_1 (1)	12	2	20-2 = 18
x_5 (1)	6	1	18-1 = 17
x_3 (1)	15	5	17-5 = 12
x_2 (1)	5	3	12-3 = 9
x_6 (3/5)	$3/5 \times 18$ = 10.8	9	9-9 = 0

Total profit = 12+6+15+5+10.8
= 48.8

Total Weight = 2+1+5+3+9
= 20.

4 Solve the job sequencing with deadline problem using Greedy approach n=7

$(P_1, P_2, P_3 \ldots P_7) = (15, 5, 20, 18, 6, 30, 70)$

$(d_1, d_2, d_3 \ldots d_7) = (1, 3, 4, 3, 2, 1, 2)$

Descending order

P_7	P_6	P_3	P_4	P_1	P_5	P_2
70	30	20	18	15	6	5

d_7	d_6	d_3	d_4	d_1	d_5	d_2
2	1	4	3	1	2	3

Job	Assigned Slot	Profit	Next Slot	Action.
ϕ	-	-		Assign slot [1,2] to Job 7
7	[1,2]	70	6	Assign slot [0,1] to Job 6
7,6	[1,2] [0,1]	30+70	3	Assign slot to [3,4] to Job 3
7,6,3	[1,2] [0,1] [3,4]	30+70+20	4	Assign slot [2,3] to Job 4
7,6,3,4	[1,2] [0,1] [3,4], [2,3]	30+70+20+18	5	Slot not available So reject Job 5.

7,6,3,4 [1,2] [0,1] 30+70+20+18 2 Slot not available
[3,4] [2,3] So reject Job 2

J = {7,6,3,4}

Profit = 30+70+20+18
= 138

5 Solve the job sequencing with deadline problem using Greedy approach for following instance n=7.
$(P_1, P_2, P_7) = (3,5,20,18,1,6,30)$ and
$(d_1, d_2 \ldots d_7) = (1,3,4,3,2,1,2)$

decending Order

P_7	P_3	P_4	P_6	P_2	P_1	P_5
30	20	18	6	5	3	1

d_7	d_3	d_4	d_6	d_2	d_1	d_5
2	4	3	1	3	1	2

Job	Assigned slot	Profit	Next Slot	Action
ϕ	-	-	7	Assigned slot [1,2] to Job 7
7	[1,2]	30	3	Assign slot [3,4] to Job 3

7,3	[1,2] [3,4]	30+20	4	Assign slot [2,3] to Job 4
7,3,4	[1,2] [3,4] [2,3]	30+20+18	6	Assign slot [0,1] to Job 6.
7,3,4,6	[1,2] [3,4] [2,3] [0,1]	30+20+18+6	2	Reject job 2 due to slot is not available
7,3,4,6	[1,2] [3,4] [2,3] [0,1]	30+20+18+6	1	Slot not available reject job 1
7,3,4,6	[1,2] [3,4] [2,3] [0,1]	30+20+18+6	5	Slot not available Reject job 5

Job = {7,3,4,6}

Profit = 30+20+18+6

= 74

6 Solve the job sequencing with deadline problem using greedy approach for following instance n= 5

$(P_1, P_2 \ldots P_7) = (3,5,20,18,1,6,30)$ and

$(d_1, d_2 \ldots d_7) = (1,3,4,3,2,1,2)$

$(P_1, P_2 \ldots P_5) = (45, 15, 20, 7, 65)$

$(d_1, d_2 \ldots d_5) = (1, 3, 2, 1, 2)$

Descending Order

P_5	P_1	P_3	P_2	P_4
65	45	20	15	7

d_5	d_1 ,	d_3	d_2	d_4
2	1	2	3	1

Job	Assigned Slot	Profit	Next Slot	Action
ϕ	-	-	5	Assign [1,2] slot to job 5
5	[1, 2]	65	1	Assign [0,1] slot to job 1
5, 1	[1,2] [0,1]	65+45	3	Assign slot not available so reject job 3.
5,1	[1,2] [0,1]	65+45	2	Assign slot [2,3] for job 2
5,1,2	[1,2] [0,1] [2,3]	65+45 +15	4	reject 9 job 4 due to unavailable slot.

Job = {5, 1, 2}
Profit = 65 + 45 + 15
= 125.

Topic - 1

13/sep/2022

Classical Encryption Techniques & DES
[Data Encryption Standard]

[a] OSI Security architecture -

1] Security Attack
2] security mechanism
3] Security services

Q. What is threats?

⇒

"A threat is a possible security risk that might exploit the vulnerability of system."

Hacking information OR the data from other way there will no any security.

Q. What is Attack?

⇒

"An attack is an intentional unauthorized action on system."

Directly attack on system and break the security & Hack the information called attack"

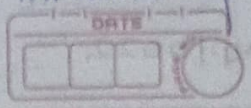
1] Active attack -

An active attack is an attempt to change the system resource.

[Modified the information]

14/Sep/2022
WED

goal of passive attack is obtain information that is being transmited

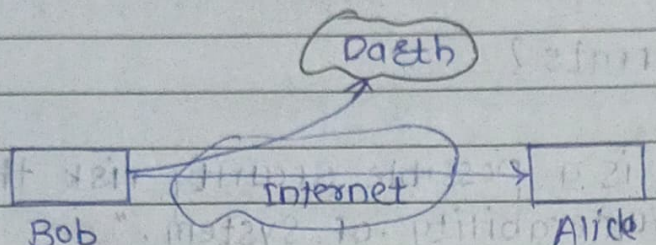


1] Passive attack. [only listening]

A passive attack is an attempt to understand or retrive data from system without influencing. OR modification

TYPES of Passive Attack :-

1] Release of message content



2] Traffic Analysis - Encryption pattern will be obtain by third party. and understanding the communication bet^n the sender & reciver.
[and exchange the message or data bet^n sender & reciver

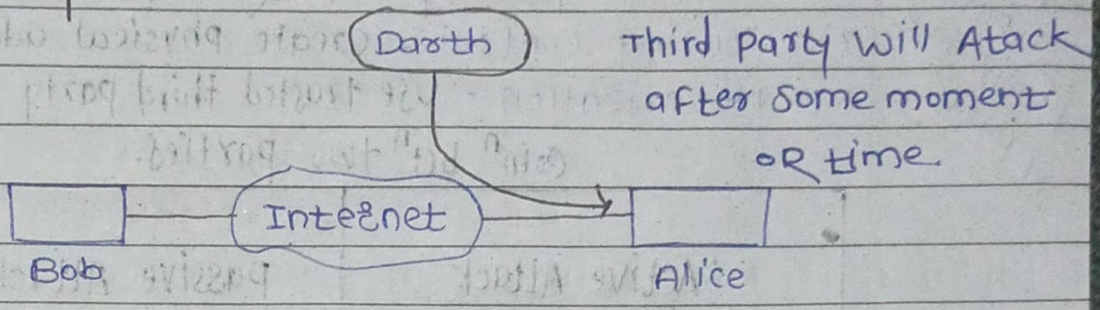
1] Release of message content -

- When the any message or data will send by the sender & reciver get this data.
- Hence, this process will carried out again & again but both sender & reciver is no idea about his data OR convertiation will read by the third party after he will not disturb to sender & reciver.
- third party OR Hacker will only learn the conversiation.

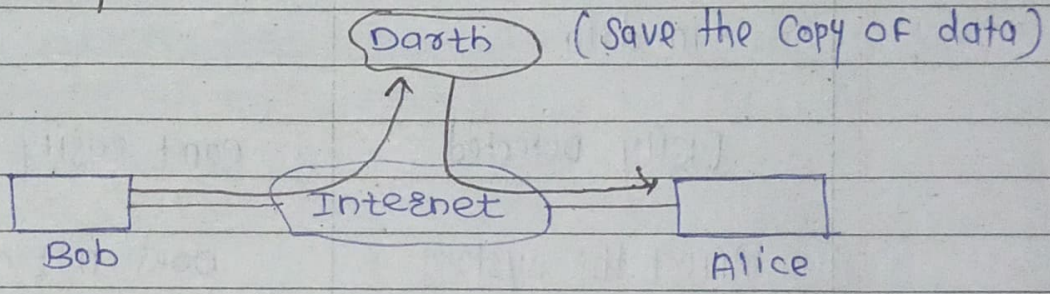
2] Active Attack :- modification of data.

1) masqureds - Third party will send the message.
2) Replay - message will change by the third party
3) Modification of message -
4) Denial of Service (DoS)

1] Masqueeads :-



2] Replay :-



3] Modification of message -
modification will be done by the third party and send the data for the Eeciverѕ.

4] Denial of Service (DoS) :-
Third party will creates the number of IP address so bob is not getting the service from the Server side. Becaus Server is overloded by the third party.

* A process that is designed for detect, prevent & detect the ~~recover from~~ attack.

Security Mechanism :-

1) Encipherment - Hiding or Covering data, Planetext to ciphertext
2) Digital Signature - append short check value of data.
3) Access Control - Emitations are require like ID & Pass.
4) Data integrity - sender can electronically sign data & recver can electronically verify the
5) Authentication Exchange - Information exchange.
6) Traffic padding - Fack Frames added in datastream
7) Routing Control - Create physical address.
8) Notarization - use trusted third party to control com^{n} bet^{n} two parties.

[code is know only sender & reciver]

No modification of data & No miss use of data

Active Attack	Passive Attack
Modification will done in data	No modification
Easily detected	Can't easily detect
Affect the system	Does not affect to system
~~Easy~~ ~~to~~ Difficult to prevent	Easy to prevent
TYPES :- - masquerads - Replay - modification of message	TYPES :- - Release of the message - traffic analysis

16/Sep/2022
Friday

2] # Security Mechanism :-

- Types of Security mechanism :-

1) Specific security mechanism :-
(Related to the protocol)

2) Pasivasive security mechanism :-
↓ (Different polysis)

a) Trusted Functionality - Specified policies
b) Security label - For Identification the resource.
Security purpose → c) Event detection - For detecting the attack
d) Security Audit Trail - We hace to check the Collection is Correct OR not
e) Security recovery.
↓
most important thing because recover for the attack & get the data into original position.

3] # Security Services :-

1) Authentication (protection) - a] Peer entity - Root of message is fixed.
b] Data origin - sended data is original
2) Access Control - Limitation on internet
3) Data Confidentiality - maintain the data with us only
4) Data integrity - No any modification OR file will not delete
5) Nonrepudiation - the things we are Sending to Reciver then Reciver not denail the message will geating to me.

19/sep/2022
monday

Cryptography :-

"It is a technique in which plain text is converted into the cipher text using encryption & decryption keys called cryptography and again cipher text is convert in plain text

Plain Text → Encryption Algorithm → Cipher Text → Decryption Algorithm → Plain Text

1) Public key
2) private key

- symetric cryptography :- "For the purpose of encryption ~~purpose~~ & decryption ~~purpose~~ same key will be provided is called as symmetric cryptography" and also known as private key cryptography.

- Asymmetric key cryptography :- "For the purpose of encryption public key is use & for Decryption private key is used called Asymmetric key cryptography."

OR

"public & private keys are uses for Decryption & encryption called Asymmetric key cryptography."

NOT In Syllabus :-

- Encryption Scheme :-
  1) Unconditional Scheme
  2) Computational Scheme.

★ Symmetric cipher :-

1) Substitution Technique - Changing the latter byanother
2) Transposition Technique - only change positions.

1) Substitution Techiques -

Latters are replaced by othe letter of symbols.

For ex -

B → x
a → M
g → A

Bag → xMA → Bag

cipher text

2) Transpositon Technique -

Applying some sort of permutati-on on plain text letters.

For ex -

NESo

→ ESoN, SNEO, OSEN, SONE, ENOS

21/sep/2022
wedensday

Substitution :-

In this cipher the text is convert from plain text to cipher text on base of key.

1] Caesar cipher :-
- oldest
- Easy to implement

Algorithm :-

'P' → 'C'

K = 3 Fixed value.

1) $C = E(P_1 k) \bmod 26$
$= (P+k) \bmod 26$
$P = D(C_2 k) \bmod 26$
$= (C-k) \bmod 26$

Cryptography :-

FUBSWRJUDSKB

11] Shift cipher :-

As Compare to Caesar cipher, shift cipher key cannot break, because the key value changes everytime from 0-25. this method takes extra time as Compare to Caesar cipher.

Monoalphabetic cipher :-

The cipher line can be any permutation of 26 Character/ alphabet.

e.g.

$S = \{a, b, C\}$

a = m

every time we will change 'a' as m is generated. To overcome broot force attack this method every time e.g.

G z GE WVGR NCP.

EXECUTE PLAN ← Guising.

27/Sep/2022

Tuesday

Playfair Cipher :- [Digraph method]

1) Create Diagram - 5x5 matrix
2) Repeating letter - filer letter
3) Same column (↓) wrap around
4) Same Row (→) wrap around
5) Rectangle (⇄) Swap

key - Monarchy.

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

Plain Text :- attack

at	ta	ck	← PT
RS	SR	DE	← CT

Plain Text :- mosque

mo	sq	ue	← Plain Text
ON	TS	mL	← cipher Text

- Filer letter :- balloon

ba ll oo nx ← Filer letter.

Filer letter fils at that position where repetation take place, after fileing this Filer letter we can stop repetation.

forex :-

balloon

ba ll oo nx

ba lx lo on

V. Imp - 8 marks

Example

- Hide the gold under the carpet.
  Key - plaintext

⇒

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

hide the gold under the carpet (X) ← Filler letter

hi	de	th	eg	ol	du	nd	er	th	ec
RB	FX	BD	XF	VE	MP	PK	BO	BO	XT

ar	pe	tx
JQ	LT	EB

A	I/J
X	B
Q	H
Q	R

X is the filler letter

ciphertext is →

RB FX BD XF VE MP PK BO BO XT JQ LT E

Plain Text & matrix of 3x3 will takes

↑

Hill Cipher :- [multiletter cipher]

- multiletter cipher
- "Lester Hill" in 1929 was developed
- Encrypt a group of letters
  - diagraph, trigraph, polygraph

Algo. :-

1) $E = E(K, P) = PX \; K \bmod 26$
2) $P = E(K, C) = CX \; K^{-1} \bmod 26$
   $= PXK \times K^{-1} \bmod 26$
   $= P \bmod 26$

Example :-

PlainText = Pay more money

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \quad \cdot \begin{bmatrix} P & a & y \\ 15 & 0 & 24 \end{bmatrix}$$

$$\text{cipher Text} = \begin{bmatrix} 15 & 0 & 24 \end{bmatrix} \times \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$= \begin{bmatrix} 15X17 + 0X21 + 24X2 \\ 15X17 + 0X18 + 24X2 \\ 15X5 + 0X21 + 24X19 \end{bmatrix}$$

$$= \begin{bmatrix} 303 & 303 & 531 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 17 & 17 & 11 \end{bmatrix}$$

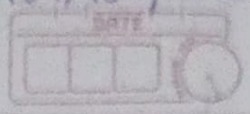
R R L

plain text = pay

Cipher text = RRL

A b c d e f g h i j k l m n o p q r s t u v w
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

x y z
23 24 25



- [m o ε]
  12 14 17

$$\text{cipher Text} = [12 \;\; 14 \;\; 17] \times \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$= \begin{bmatrix} 12\times17 + 14\times21 + 17\times2 \\ 12\times17 + 14\times18 + 17\times2 \\ 12\times5 + 14\times21 + 17\times19 \end{bmatrix}$$

$$= \begin{bmatrix} 204 + 294 + 34 \\ 204 + 252 + 84 \\ 60 + 294 + 323 \end{bmatrix}$$

$$= [532 \;\; 490 \;\; 677] \bmod 26$$

$$= [12 \;\; 22 \;\; 1]$$

↓

= M W B

plain text = moε
cipher text = MWB

- [e m o]
  4 12 14

$$\text{cipher text} = [4 \;\; 12 \;\; 14] \times \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$= \begin{bmatrix} 68 + 252 + 28 \\ 68 + 216 + 28 \\ 20 + 252 + 266 \end{bmatrix}$$

$= [348 \quad 312 \quad 538] \bmod 26$

$= [10 \quad 0 \quad 18]$

↓

= K A S

Plain text = emo

cipher text = KAS

- [n e y]
  13 4 24

$$\text{cipher text} = [13 \quad 4 \quad 24] \times \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$= \begin{bmatrix} 221 + 84 + 48 \\ 221 + 72 + 48 \\ 65 + 84 + 456 \end{bmatrix}$$

$= [353 \quad 341 \quad 605] \bmod 26$

$= [15 \quad 3 \quad 7]$

↓

= P D H

Plain text = n e y

cipher text = P D H

Final Result:-

Plain text = Pay more money

cipher text = RRL MWB KAS PDH

28/Sept/2022

WED

Cipher text to plain text Conversion

- Plain Text :- [usually ordinary readable text]

$$P = D(k, C)$$
$$= C \times K^{-1} \bmod 26$$

$$K^{-1} = \left(\frac{1}{\text{determinant}} \times \text{Adjoint} \right) \bmod 26$$

$$\text{Det} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

For example :-

$$|A| = \begin{vmatrix} +a & -b & +c \\ d & e & f \\ g & h & i \end{vmatrix}$$

$$\det(A) = a * \begin{vmatrix} e & f \\ h & i \end{vmatrix} - b * \begin{vmatrix} d & f \\ g & i \end{vmatrix} + c * \begin{vmatrix} d & e \\ g & h \end{vmatrix}$$

$$= aei - afh - bdi + bfg + cdh - ceg$$

$$\text{Det} = 17 \times \begin{vmatrix} 18 & 21 \\ 2 & 19 \end{vmatrix} - 17 \begin{vmatrix} 21 & 21 \\ 2 & 19 \end{vmatrix} + 5 \begin{vmatrix} 21 & 18 \\ 2 & 2 \end{vmatrix}$$

$$= 17 * (342 - 42) - 17 * (399 - 42) + 5 * (42 - 36)$$

$$= (5100 - 6069 + 30) \bmod 26$$

$$= (-939) \bmod 26$$

$$\text{Det} = 23$$

$$\text{Adj} = \begin{vmatrix} + & - & + \\ 17 & 17 & 5 \\ -21 & +18 & -21 \\ +2 & -2 & +19 \end{vmatrix}$$

$$= \begin{vmatrix} (18\times19-21\times2) & -(21\times19-2\times21) & +(21\times2-18\times2) \\ -(17\times19-2\times5) & +(17\times19-2\times5) & -(17\times2-17\times2) \\ +(17\times21-18\times5) & -(17\times21-21\times5) & +(17\times18-21\times17) \end{vmatrix}$$

$$= \begin{vmatrix} 300 & -357 & 6 \\ -313 & +313 & 0 \\ 267 & -252 & -51 \end{vmatrix} \quad \text{mod } 26$$

Then now Convert column to row

$$\text{Adj} = \begin{vmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{vmatrix} \quad \text{mod } 26$$

$$\text{Adj} = \begin{vmatrix} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & 1 \end{vmatrix} \quad \text{mod } 26$$

$$= \begin{vmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{vmatrix}$$ add 26 at the number.

Then

$$K^{-1} = \left(\frac{1}{D} \times \text{Adj}\right) \text{ mod } 26$$

$$K^{-1} = \frac{1}{23} \begin{vmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{vmatrix} \bmod 26$$

$$= 17 \begin{vmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{vmatrix} \bmod 26$$

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

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

- **RRL**

$$(17\ 17\ 11) \times \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{vmatrix} \bmod 26$$

$$\begin{vmatrix} 68 + 255 + 264 \\ 153 + 289 + 0 \\ 165 + 102 + 187 \end{vmatrix} \bmod 26$$

$$(587 \quad 442 \quad 544) \bmod 26$$

$$(15 \quad 0 \quad 24)$$

$$RRL = P \quad a \quad y \leftarrow \text{plain text}$$

- MWB

(12 22 1)

$$(12\ 22\ 1) \times \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{vmatrix} \bmod 26$$

$$\begin{vmatrix} 48+330+24 \\ 108+374+0 \\ 180+132+17 \end{vmatrix} \bmod 26$$

$$(402 \quad 482 \quad 329) \bmod 26$$

$$(12 \quad 14 \quad 17)$$
$$\downarrow \quad \downarrow \quad \downarrow$$

MWB = m o r

cipher Text — plain text

- KAS

(10 0 18)

$$(10\ 0\ 18) \times \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{vmatrix} \bmod 26$$

$$\begin{vmatrix} 40+0+432 \\ 90+0+0 \\ 150+0+306 \end{vmatrix} \bmod 26$$

$$(472 \quad 90 \quad 456) \bmod 26$$

$$(4 \quad 12 \quad 14)$$
$$\downarrow \quad \downarrow \quad \downarrow$$

KAS = e m o

(POH)

(15 3 7)

(15 3 7) *	4	9	15	mod 26
	15	17	6	
	24	0	17	

60 + 45 + 168	mod 26
135 + 51 + 0	
225 + 18 + 119	

(273 186 362) mod 26

↓ ↓ ↓

POH = (13 4 24)

↓ ↓ ↓

PDH = n e y ← plain text

Opher text

04/oct/2022
Tuesday

polyalphabetic cipher :- [vignere cipher]

$Ci = (Pi + Ki) \bmod 26$
$Pi = (Ci + Ki) \bmod 26$

key value will be repeat at the end of plain text

ex. key - deceptive
PT - wearediscovered save yourself
CT - ZICVTWQNGRZGVTWAVZHCQYGLMGJ

key	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d	e	c			
PT	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o			

key	e	p	t	I	v		e
PT	u	r	s	e	i		f

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8
PT	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	4
CT	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22	0	24	25	7	2	16	24	6	11	12

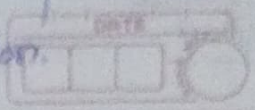
key	21	4
PT	11	5
CT	6	9

Autokey - use to overcome repetation of words.

- In this case we have key & PT. In key we can add PT into key as long PT
- vignere propose autokey system in which keyword is concatinated with PT. itself to provide running key.

→ more secure.
→ unbreakable.

- Apply on binary numbers.
- XOR operation.

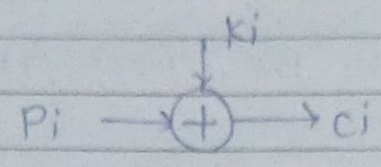


Veenam cipher :- [Gilbart 1918]

$C_i = P_i \oplus k_i$

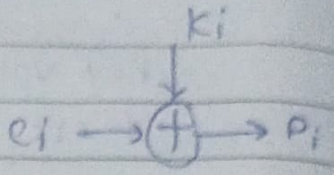
$P_i = C_i \oplus k_i$

Cryptographic Stream generator



Encryption

Cryptographic Stream generator



Decryption.

- method - One time Pad. (only one time key is use)
  - Different keys are use for encryption.

Disadvantage -

- ~~Receiver~~ Reciver dont know about key. which used. by Sender.

- One time pad :-
  - improvment to verram ~~cipher~~ cipher.
  - It yileds ultimate insecurity
  - Random key is used. as long as message.
  - The key need not be repeted
  - The key which is used to encrypt & decrypt a single msg. and then it is discorded.
  - Each new message requires a new key of same length. as the new msg.
  - Such a schem known as one time pad which is unbreakable.

- Disadvantages :-
  - practical problem of making large quantity of Random key
  - problem of key distribution & protection.

11/oct/2022
Tuesday

Transposition Technique :- Change position of letter.

1] Rainfence Technique
2] Row-Coloumn Technique

1] Rainfence Technique :-

- only change position of letter.
- we have plain text as well as key size like, 2, 3.
- Then we have to split the plain text in to the key size i.e. 2, 3 rows
- Then read 1st row then read 2nd row & ther 3rd row

For ex :-

PT = thank you very much

⟹

t		a		k		o		v		r		m		c	
	h		n		y		u		e		y		u		h

Then,

CT = takovrmchnyueyuh

- Again rainfence technigu apply on CP Text for the purpose of more Sequrity.

depth 3 CT = tkymhnyueyuhaorc as a PT.

⟹

t				h				e				a			
	k		m		n		u		y		h		o		c
		v				y				u				r	

CT = theakmnuyhocvyur

2] Row-Column Transposition :-

- size of rectangle will choose by Sender & reciver.

PT - kill Corona virus at twelve am tomorrow

Key - 43215 - choose by Sender & reciver.

Rec - 7X5

⟹

	1	2	3	4	5
1	k	i	l	l	c
2	o	r	o	n	a
3	v	i	r	u	s
4	a	t	t	w	e
5	l	v	e	a	m
6	t	o	m	o	r
7	r	o	w	x	y

CT = LNUWAOXLORTEMWIRITVOOKOVALTRCASEMRY

12/oct/2022
WED

Stream cipher means only one byte convert into cipher text, called "stream cipher"

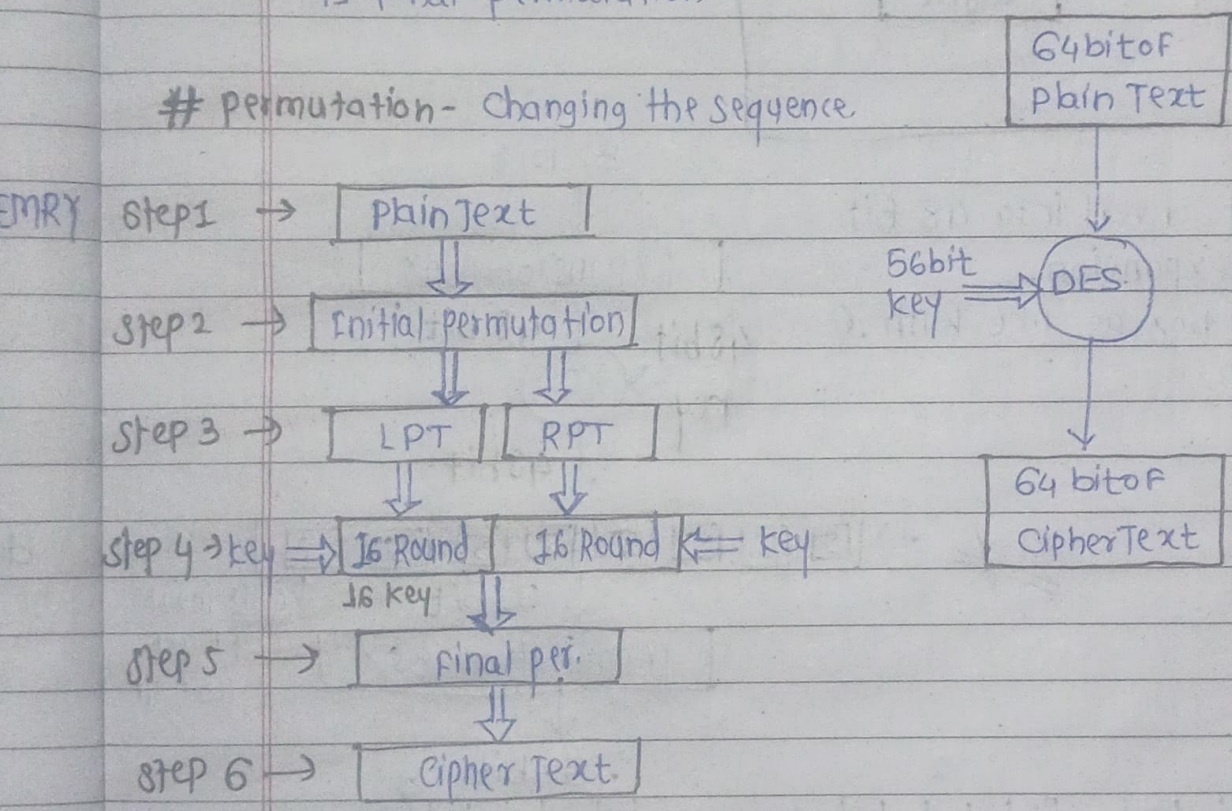
Block cipher principles :-
Whole block going to convert into cipher.

1) Number of Rouds -
2) Design of function F- How design the function.
3) key schedules Algorithm.

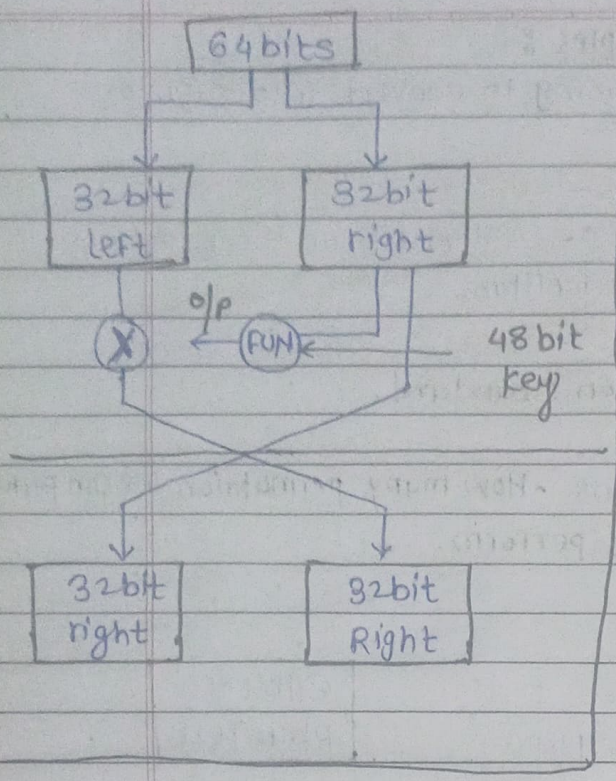
DES - Data Encryption Standard.

1] Initial permutations - How many permutaion we can perform
2] Round - 16 rounds perform.
3] Swapping
4] Final permutation

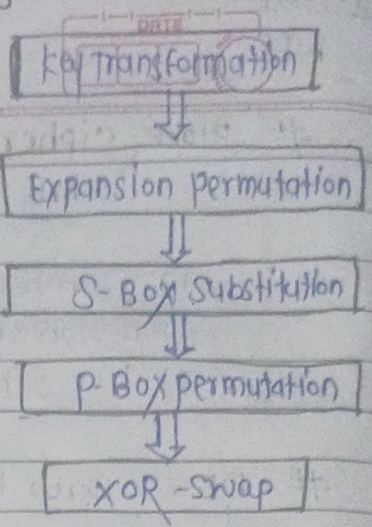
permutation - Changing the sequence.

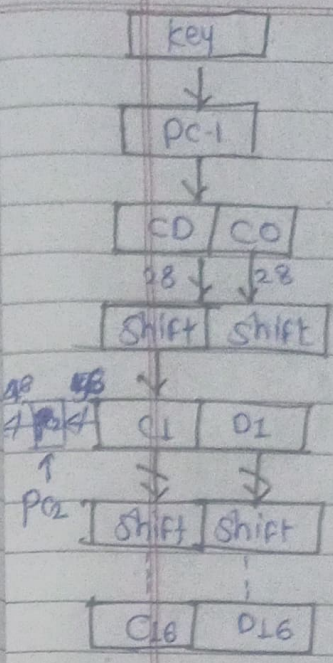


Keysize - 64 bit
56 bit
48 bit

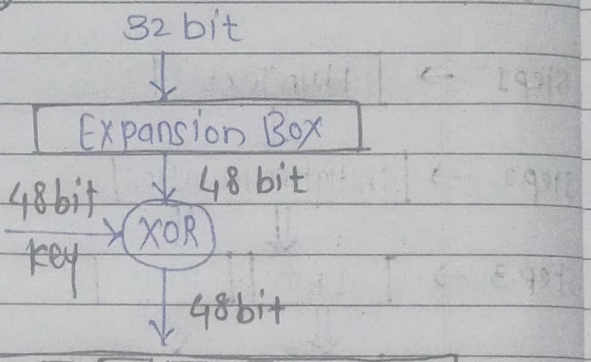


Rounds -





- 32 bit convert into 48 bit using expansion.
- Take 8 box as like with 6 partition.



for ex.