5) Playfair Cipher

Key - MONARCHY

Msg - BALLOON

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

Step 1 → Creation & population of Matrix

BA LX LO ON.

SC D D SR

SC → Same column

D → Diagonal

SR → Same Row

BA → IB, JB

ON → AN

LX → SV

LO → MP

PLAYFAIR EXAMPLE -

MY NA ME IS AT UL.

D SR SC SC D SC

MY → NC

NA → RA

ME → CL

IS → XS

AT → SR

UL → EL

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

Rotate Clockwise

03/02/2020

ex-1 KEY- PLAYFAIR EXAMPLE

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

P	L	A	Y	F
A	I	R	E	X
A	M	P	L	E

Msg → MY NAME IS ATUL.

MY → XF

NA → OL

ME → IX, JX

IS → ~~IKIM~~ MK

AT → PV

UL → LR

ex-2 Key- HIPPOPOTAMUS

Msg → WHY KATTAPPA KILLED BAHUBALI

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

WH → IV, JV

KA → VC

TX → PZ

TA → HB

PX → UP

PA → HU

UB → SA

AL → KM

IX → WP

KI → HL

LX → NW

LE → ND

DB → GM

AH → CA

Steps-

1) Matrix
2) Encrypt Plain text

Encryption-

~~Before execution~~

1) If both alphabets are same, add an x after first alphabet. Encrypt the new pair and continue.
2) If both the alphabets appear in same row of matrix, replace them with alphabets to their immediate right respectively.
3) If the original pair is on the right side of the row, then wrapping around to the left side of the row happens.
4) If both alphabets appear in the same column of matrix, replace them with alphabets immediately below them respectively. If the original pair is on the bottom side of the row, then wrapping around to the top side of the row happens.
5) If both alphates are not in SR or SC, replace them with the alphabet in the same row respectively, but at the other pair of corners of the rectangle defined by original pair. The order is quiet significant here. The first encrypted alphabet of the pair is the one that is present on the same row as the first plain text alphabet.

* HILL Cipher

PT → HELLO WORLD

$$\text{Key} \rightarrow \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$$

$$\text{Pair} \rightarrow \begin{bmatrix} H \\ E \end{bmatrix} \begin{bmatrix} L \\ L \end{bmatrix} \begin{bmatrix} O \\ W \end{bmatrix} \begin{bmatrix} O \\ R \end{bmatrix} \begin{bmatrix} L \\ D \end{bmatrix}$$

$$\begin{bmatrix} 7 \\ 4 \end{bmatrix} \begin{bmatrix} 11 \\ 11 \end{bmatrix} \begin{bmatrix} 14 \\ 22 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix} \begin{bmatrix} 11 \\ 3 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 14+8 & 7+4 \\ 21+12 & 28+16 \end{bmatrix} = \begin{bmatrix} 22 & 11 \\ 33 & 44 \end{bmatrix}$$

$$= \begin{bmatrix} 14+4 \\ 21+16 \end{bmatrix} = \begin{bmatrix} 18 \\ 37 \end{bmatrix} \quad \begin{bmatrix} 18 \\ 37 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} 33 \\ 77 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 14 \\ 22 \end{bmatrix} = \begin{bmatrix} 50 \\ 130 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} 45 \\ 110 \end{bmatrix}$$

$$\begin{bmatrix} 21 \\ 34 \end{bmatrix} \times \begin{bmatrix} 11 \\ 3 \end{bmatrix} = \begin{bmatrix} 25 \\ 45 \end{bmatrix}$$

$$\begin{array}{r} 26 \\ \times\ 4 \\ \hline 104 \end{array} \qquad \begin{array}{r} 26 \\ \times\ 3 \\ \hline 78 \end{array} \qquad [-80 \pmod{26}] = 24$$

Mod-

$$\begin{bmatrix} 33 \\ 77 \end{bmatrix} = \begin{bmatrix} 7 \\ 25 \end{bmatrix} \qquad \begin{bmatrix} 18 \\ 37 \end{bmatrix} = \begin{bmatrix} 18 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} 50 \\ 130 \end{bmatrix} = \begin{bmatrix} 24 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 45 \\ 110 \end{bmatrix} = \begin{bmatrix} 19 \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} 25 \\ 45 \end{bmatrix} = \begin{bmatrix} 25 \\ 19 \end{bmatrix}$$

$$\begin{bmatrix} S \\ L \end{bmatrix} \begin{bmatrix} H \\ Z \end{bmatrix} \begin{bmatrix} Y \\ A \end{bmatrix} \begin{bmatrix} T \\ G \end{bmatrix} \begin{bmatrix} Z \\ T \end{bmatrix}$$

4/2/20

PT → CT

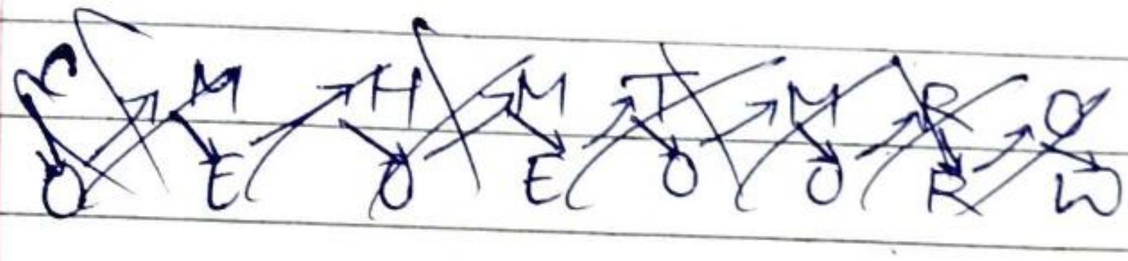
- Transposition technique
- Substitution technique
  - Caesar cipher
  - Mono ceaer cipher
  - Modified ceaer cipher
  - Poly alphabet cipher
  - Playfair
  - Hill cipher

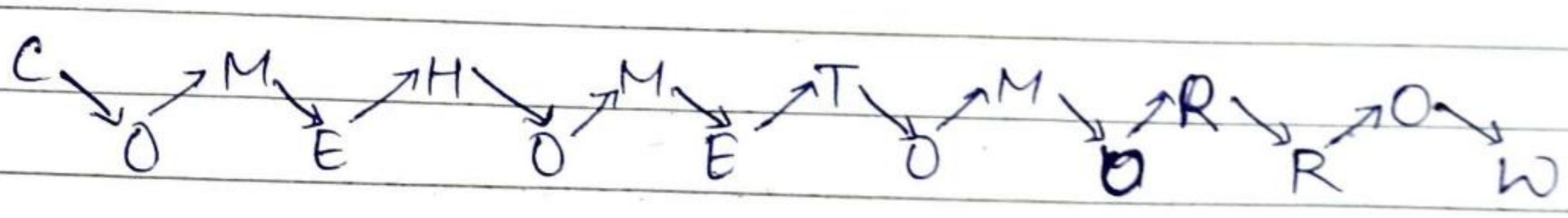
Transposition technique → Substitution techniques focus on substituting a plain text with a cipher text alphabet, but in transposition techniques, we don't simply replace 1 alphabet with another alphabets, but some permutations are also performed over the plain text.

1) Rail Fence Technique

R.F technique is an example of transposition.
It uses a simple algorithm

ex COME HOME TOMORROW





1) Write down the P.T msg as a sequence of diagonals
2) Read the P.T written in step-1 as a sequence of rows.

ex- as shown in figure above.

CT→ CMHMTMROOEOEOORW

Rail fence technique involves writing PT as a sequence of diagonals and then reading it row by row to produce cipher text.

2) Simple columnar Transposition Technique -

ex- COME HOME SWEET TOMORROW

Key → 6 (6 columns)

Order → 4,1,3,2,5,6

C1	C2	C3	C4	C5	C6
C	O	M	E	H	O
M	E	T	O	M	O
R	R	O	W		

CT1→ EOWCMRMTOOERHMOO

Basic technique-
Variations of basic transposition tech. such as rail fence tech. exists which we call simple columnal transposition technique.

The simple columnar transposition tech. simply arange the P.T as a sequence of rows of a rectangle that are read in columns randomly.

3) Simple columnar Transposition technique with multiple rounds -

P/P → C.T 1

C1	C2	C3	C4	C5	C6
E	O	W	C	M	R
M	T	O	O	E	R
H	M	O	O		

C.T2→ COOEMHWOOOTMMERR

g/p → CT 2

C_1	C_2	C_3	C_4	C_5	C_6
C	O	O	E	M	H
W	O	O	O	T.	M
M	E	R	R		

CT3 → EORCWMOOROOEMTHM

Cipher text produced by the simple columnar transposition tech. with multiple rounds is ~~much~~ much more complex to crack as compared to basic tech.

4) Veenam Cipher-
This is also called one time pad. It works like poly alphabet cipher.

5) Book cipher/Running key cipher
This also operates on the principle of veenam cipher.

06/02/20

* Rotor Machine – This m/c consist of a set of independently rotating cylinders through which electrical pulses can flow. Each cylinder has 26 g/p pins and 26 o/p pins with internal wiring that connects each g/p pin to a unique o/p pin. (Fast, Slow, Very slow)

* ~~Eee~~ Steganography → It is a tech. that facilitates hiding of a msg. that is to be kept secret inside other msg. This results in a concelment of the secret msg. itself. Historically, the sender uses method such as invisible ink,

punches
tiny pin ~~puchares~~ on special characters and pencil marks on hand-written characters. People hide secret msg. within a graphic msg. Steganography is a technique that facilitates hiding a ~~msg~~ secret msg. that is to be kept behind an image.

1. Convert image into digital form. ~~So~~
2. select the part of image where minute changes doesn't effect the image very much.
3. Convert your message into digital form.
4. Put it into the selected part of image and send the image to sender.

Internet standards & Internet Society -

IAB → Internet architecture board
IESG → Internet enggineering ~~stree~~ steering Group
ITU → International Telecommunication Union
IETF → Internet engg. Task Force
RFC → Request for comments
OSI → Open system Interconnection

IAB → It is responsible for defining the overall architecture of internet, providing guidance & broad directions to the IETF.

IETF → The protocol engg. and development arm of the internet.

IESG → Responsible for technical management of IETF, internet and the internet standard process.

* Algorithm types and modes -

1) Stream ciphes

In stream ciphe, the PT is encypted one bit at a time.

ex- Pay 100

Binary → CT

XOR → CT

2) Block cipher

In this, rather than encypting one bit at a time, a block of bit is encypted at one go. The Block cipher technique involves encyption of one block of text at a time. Decryption also takes one block of encypted text at a time.

| Pay 100 | Block

↓ AND

CT

Fiestel Stoucture -

1) **Confusion** → It is a technique of ensuring that a CT gives no clue about the original plain text. Confusion is achieved by ~~stuff~~ substitution techniques. Stream cipher relies on a concept of confusion.

2) **Diffusion** is a technique which increase the redundancy of the PT by spreading it across rows and columns. Diffusion is achieved by using transposition/ permutation techniques. Block cipher uses confusion and diffusion.

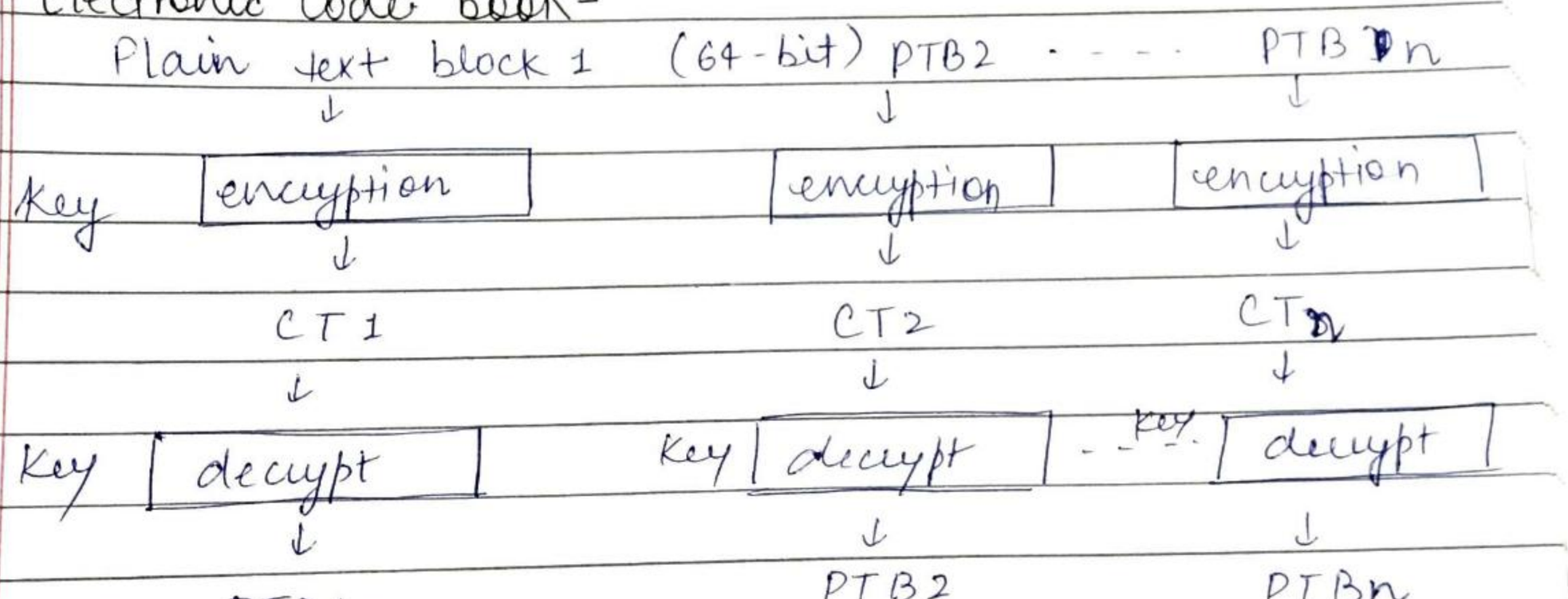
Algorithm Modes -

1) Electronic Code Block (Electronic Code Book)(ECB)
2) Cipher block chaining (CBC)
3) Cipher Feedback (CFB)
4) Output Feedback (OFB)
5) Counter mode (CTR)

1) & 2) work on block cipher.
3) & 4) work on block cipher.
↓
acting as stream cipher

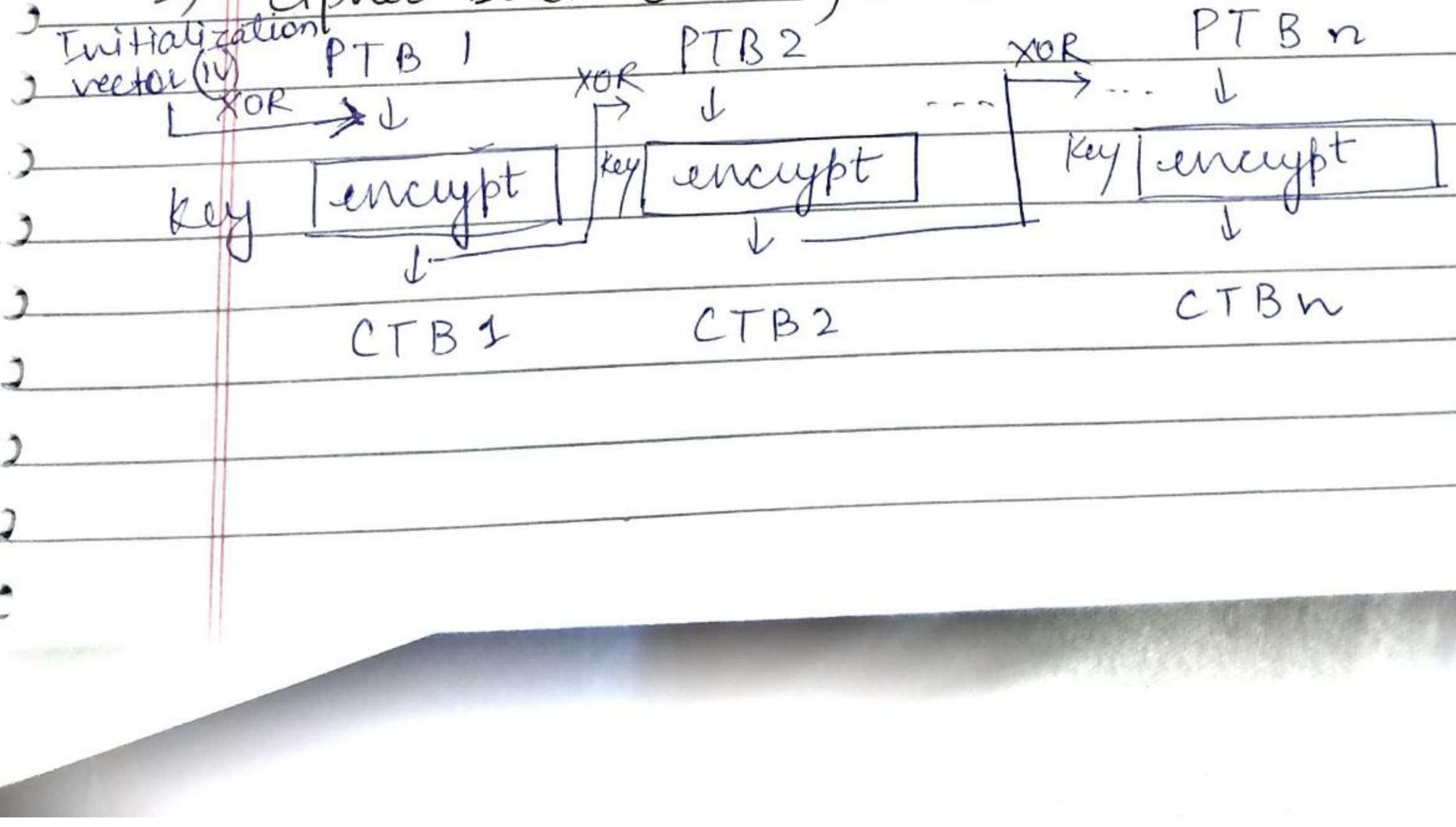
10/2/20

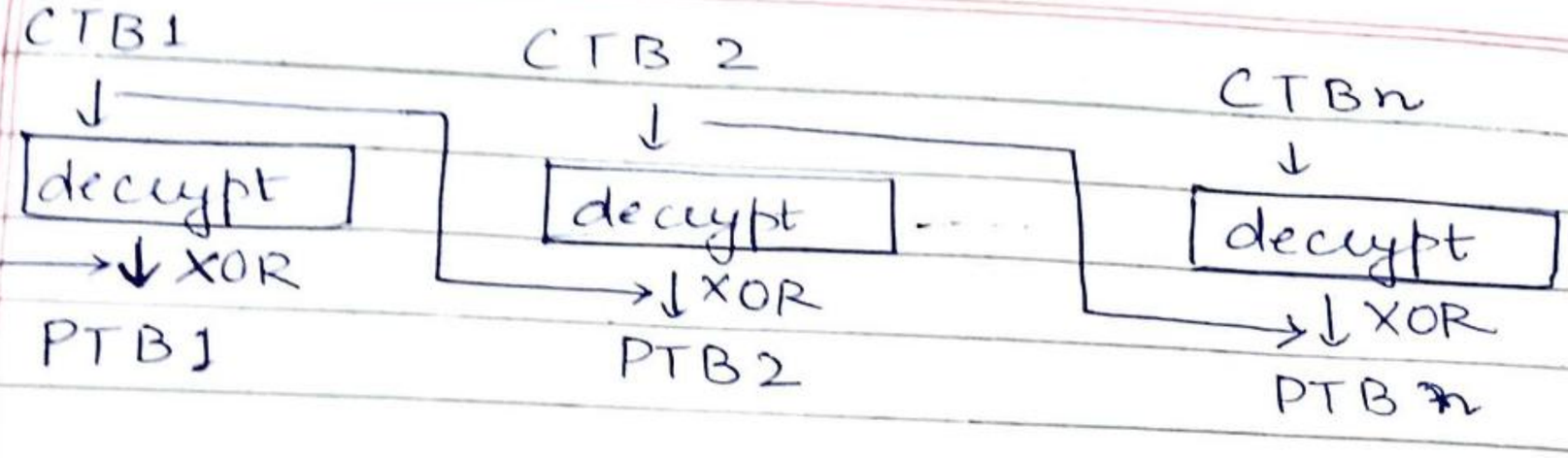
1) Electronic Code book -



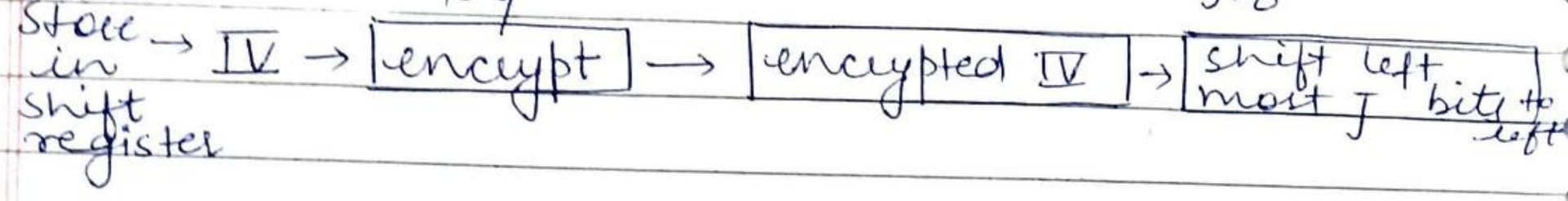
ECB mode encryption - decryption process

2) Cipher block chaining mode -





3) Cipher Feedback Mode



Left shift bits → XOR → Combine with PTB1
(C reg.) + Right J bits

Then same as chaining mode

ECB -

It is simplest mode of operation. Here, the incoming PT message is divided into block of 64 bits each. The same key is used for encryption and decryption. If PT block is repeated, it produces same CT block which will help hacker to get info. about the code.

CBC -

There is an IV. IV has no special meaning. It is used to make message unique. It is used only with first PTB. Chaining adds a feedback mechanism to a block cipher. In CBC, the result of the encryption of the previous block are fed back into the encryption of the current block.

Dis=

→ Time consuming because of the O/P of K-block depend upon the O/P of K-1 block.

→ error propagation

CFB-

Cipher feedback mode is useful in where the data is encrypted in smaller units then define in block size.

Like CBC, a 64-bit IV is used in case of CFB mode. The IV is kept in shift register to produce a coresponding 64-bit initialization vector CT. Now, the left most (MSB J bits) bits of the encrypted IV are XORed with the first J bits of PT. This produces first potion of CT(C). Then it is transmitted to the receiver. ~~Now,~~

Now, the bits of initialization vector are shifted left by J-positions. Thus the right-most J position of shift register now contain unpredictable text and these are filled with C.

11/2/20

* DES (Data encryption Standard)-

Operates on 64-bit