Subject : CNS

Q2.

A] Explain Transposition cipher with illustrative examples

Ans

- A transposition cipher does not substitute one symbol for another (as in substitution cipher), but changes the location of these symbols
- It reorders (jumbles) the given plain-text to give the cipher-text
- They are of two types: Keyed and keyless Transposition Cipher.

Keyless Transposition Cipher:

- In this cipher technique, the message is converted to ciphertext by either of two permution techniques:
- a. Text is written into a table ~~row~~ column-by column and is then ~~be~~ transmitted row by-row.

Eg: We need to send the message "DEFENDTHE EASTWALL"

Arranging into tables we get:

D	F	N	T	E	A	T	A	L
E	E	D	H	E	-	S	W	L

Now, the message is send ~~the~~ row by row, so Ciphertext is "DFNTEATALEEDHESWL"

- Similarly (b) method, we can arrange the same above message into tables with four columns

D	E	F	F ~~ed~~
N	D	T	H
E	E	A	S
T	W	A	L
L			

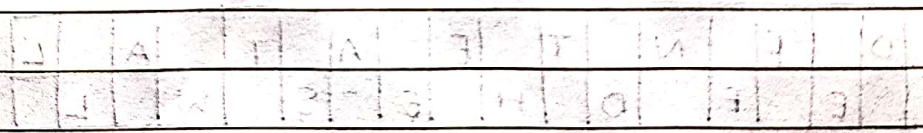
∴ The data is then transmitted column-by-column as "DNETLEWFTAAEHSL"

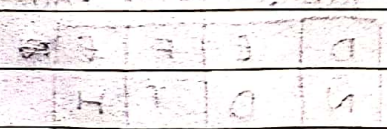
Keyed Transposition Ciphers.

- In this approach, rather than permuting all the symbols together, we divide the entire plaintext into block of predetermind size and then permute each block independently.
- Suppose A want send a message to B "We Have an attack". Both A and B agreed to had.

WEHAV | EANAT | TACKX

- The last characters x is a bogus character so as to complete the block size of 5.





Q3.

A]

Ans • Encryption algorithms are divided into two categories based on input types, as block ciphers and stream cipher. Block cipher is an encryption algorithm which takes fixed size of input say b bits and produces a ciphertext of b bits again. If input is larger than b bits it can be divided further. for different applications and uses.

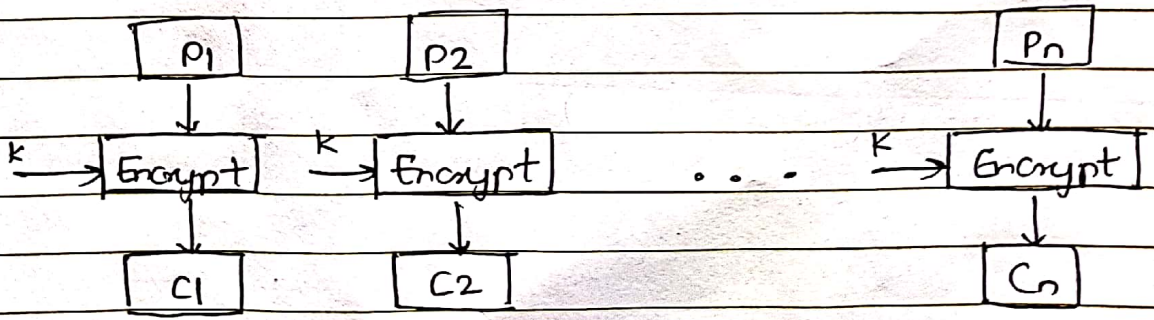
• There are several modes of operations for a block cipher.

1. Electronic Code Book (ECB)-

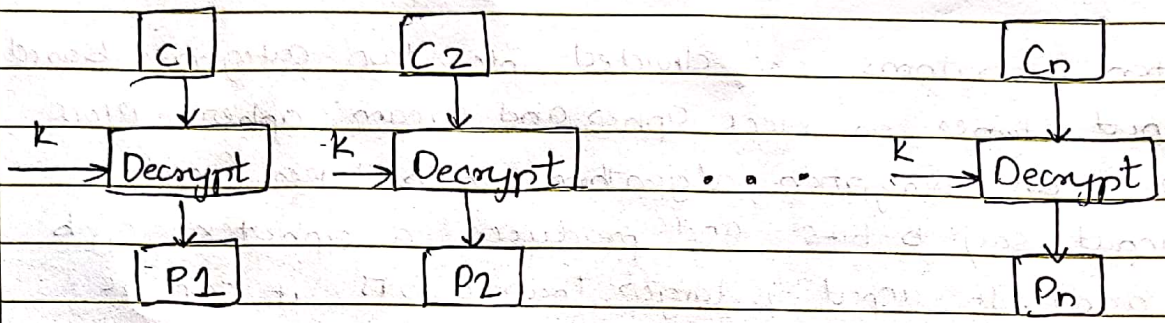
Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of block of encripted ciphertext. Generally, if a message is larger than b bits in size, it can be broken down into bunch of blocks and the procedure is repeated.

Procedure of ECB is illustrated below:

Encryption:-



Decryption :-



Advantage

- Parallel encryption of blocks of bits is possible, Thus it is a faster way of encryption.

Disadvantage

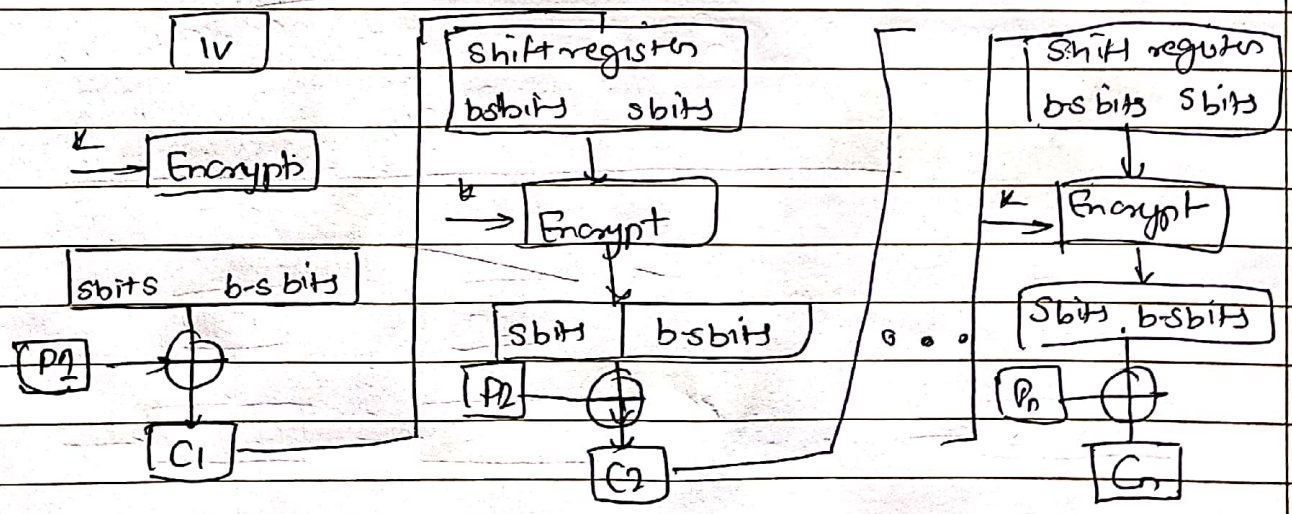
- Prone to cryptanalysis since there is a direct relationship between plaintext.

Q3
A]

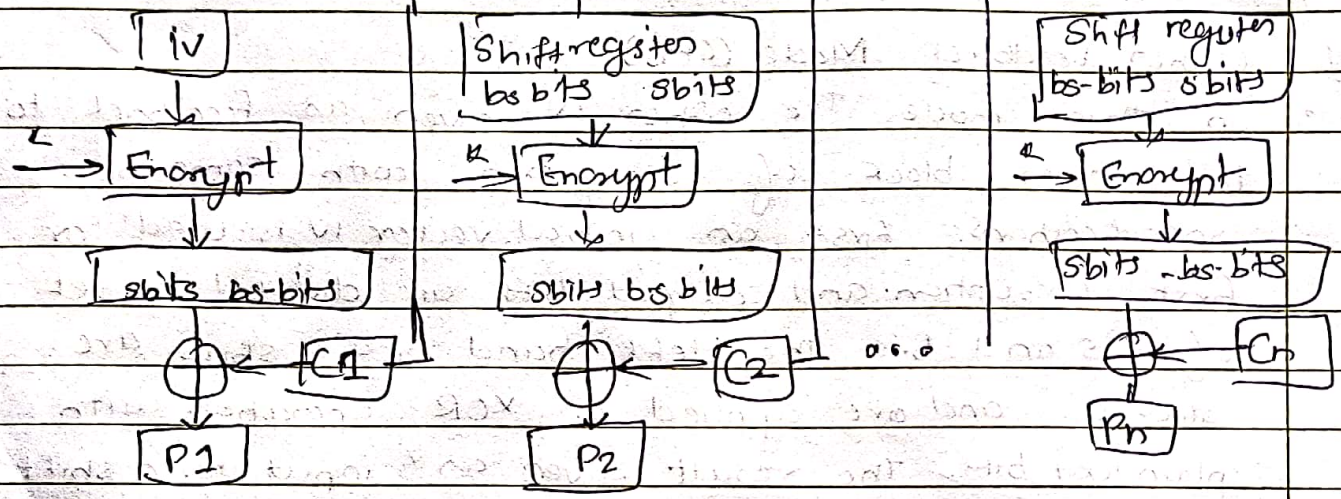
Ans Cipher Feedback Mode (CFB).

In this mode the cipher is given as feedback to the next block of encryption with some new specifications. First an initial vector IV is used for first encryption and output bits are divided as set of s and b-s. The left hand side sbits are selected and are applied an XOR operation with plain text bits. The result given as input to a shift register and the process continues. The encryption and decryption process for the same is shown below both of them use encryption algorithm

Encryption



Decryption



Subject : CNS

Q5.
B] Explain short note on Eavesdropping and Active Attacks.
Ans -
- An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device.
- Eavesdropping is a deceptively midterm. The attackers are usually after sensitive financial and busines information that can be sold for criminal purposes. There also is a booming trade in so-called Spouseware, which allows people to eavesdrop on their loved ones by tracking their smartphone use.
- Active Attacks.

An Active attack attempt to alter system resources or effect their operations, Active attack involve some modification of the data stream or creation of false statement.

There are five types of Active attacks as follows
1. Masquerade
2. Modification of messages.
3. Repudiation
4. Replay
5. Denial of service.

Q6.

A] Ans

Virus	Worms	Trojan Horse
• Virus is a software or computer program that connect itself to another Software or computer program to harm Computer system.	• Worms replicate itself to cause slow down the computer system	• Trojan Horse rather than replicates capture some important information about a computer system or a computer network.
• Virus replicates itself	• Worms are also replicates itself.	• But Trojan horse does not replicate itself.
• Virus can't be controlled by remote	• Worms can be controlled by remote	• Like worms, Trojan horse can also be controlled by remote.
• Spreading rate of Viruses are moderate	• While Spreading rate of worms are faster than virus and Trojan horse	• And Spreading rate of Trojan horse is slow in comparision of both virus and worms
• The main objective of virus to modify the information	• The main objective of worms to eat the system resources	• The main objective of Trojan horse to steal the information.

Subject : CNS

Q 4.

A]

Ans

- Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principle.
- The main components of kerberos are:

1. Authentication Server (AS):

The Authentication server performs the initial authentication and ticket for Ticket Granting service.

2. Database:

The Authentication server verifies access rights of users in databases.

3. Ticket Granting server (TGS).

The Ticket Granting server issues the ticket for the server.