unit-1

Security attacks

Any action that compromises the Security (Persona… Information owned by ~~an~~ another organisation is called Security attacks

Securityattacks can classified as
(1) Passive attacks (2) Active attacks

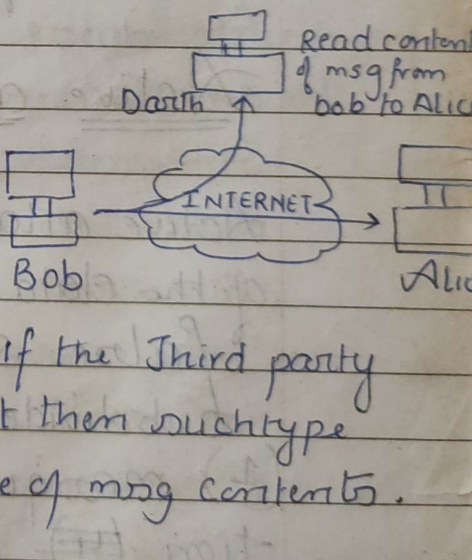
(1) passive attacks

A passive attack attempts to learn or make use of information but doesnot affect system resources

Two types of passive attacks

(a) Release of msg contents

A telephone conversation, an electronic mail msg & a ~~tranf~~ transferred file may contain sensitive or confidential information, if the Third party gets to read these content then suchtype of attack is called release of msg contents.



(b) Traffic analysis

Suppose that we had a way of marking The contents of messages or other information traffic so that opponents, even if they captured The message, could not extract the information from the message an opponent might still be able to observe the pattern of these msg. The opponent could determine the location & identity of communicating hosts & could observe the frequency & length of msg being exchanged. This might be useful in guessing the nature of the communication that was taking place.

→ Passive attacks are very difficult to detect because they do not involve any alteration of the data.

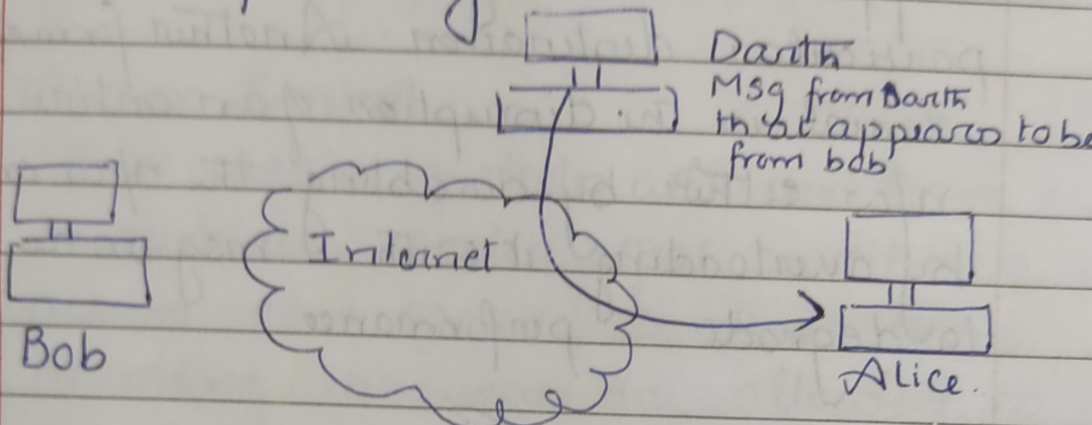
→ However it is feasible to prevent the success of these attacks, usually by means of encryption

Active attacks

Active attacks involve some modification of the data stream or the creation of false stream. This can be further subdivided as:
(1) masquerade (2) Replay (3) modification ~~(4)~~ of msg (4) denial of service

(1) masquerade takes place when one entity pretends to be a different entity. for example, authentication sequences can be captured & replayed after a

a valid authentication ~~sequences can be captured & ..~~ has taken place, thus enabling ~~an authorized entity~~ to obtain extra privileges by impersonating an entity that has those privileges.



(2) <u>Replay</u>
involves the passive capture of a data unit & its subsequent retransmission to produce an ~~..~~ unauthorized effect.

(3) <u>Modification of msg</u>
simply means that some portion of msg is altered, or that msg are delayed or reordered, to produce an ~~..~~ unauthorized effect. for example, a msg meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts"

(4) Denial of Service
prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all msg directed to a particular destination. Another form of denial is the disruption of an entire n/w either by disabling the n/w or by overloading it with msg so as to degrade performance

Security Services

According to X.800, a security service ensures adequate security of the systems or of data transfer.
X.800 divides services into five categories & fourteen specific services

(A) Authentication
The assurance that the communicating entity is the one that it claims to be.
Two specific authentication services are defined in X.800

(1) PEER ENTITY AUTHENTICATION
provides authentication for the identity of a

peer entity in an association

(2) DATA ORIGIN AUTHENTICATION
provides authentication of the source of a data unit. It does not provide protection against the duplication or modification.

(B) Access Control
This service controls who can have access to resource, under what conditions access can occur, & what those accessing resources are allowed to do.

(C) Data confidentiality
Confidentiality is the protection of transmitted data from passive attacks

(1) CONNECTION CONFIDENTIALITY
The protection ~~alt~~ of all user data on a connection

(2) CONNECTIONLESS CONFIDENTIALITY
The protection of all user data in a single data block

(3) Selective-FIELD CONFIDENTIALITY
The ~~condif~~ confidentiality of Selected fields within the user data on a connection or in a single data block.

(4) TRAFFIC FLOW CONFIDENTIALITY
The protection of the Information that might b

derived from observation of traffic flows

(D) DATA INTIGRITY

The assurance that data received are exactly as sent by an authorized entity.

(1) CONNECTION INTEGRITY WITH RECOVERY

provides for the Integrity of all users data on a connection & detects any modification, insertion, deletion or replay of any data within an entire data sequence with recovery attempted.

(2) CONNECTION INTEGRITY WITHOUT RECOVERY

same as above, but provides only detection without recovery

(3) SELECTIVE - FIELD CONNECTION INTEGRITY

provides for the Integrity of selected fields within the user data of a data block transferred over a connection & ~~takes the form of determination~~ determines whether the selected fields have been modified or not.

(4) CONNECTIONLESS INTEGRITY

provides for the INTEGRITY of SINGLE CONNECTIONLESS data block & may provide detection of data modification

(4) SELECTIVE-FIELD CONNECTIONLESS INTEGRI
provides for the integrity of selected fields within a single connection less data block & determines whether the selected fields have been modified

(E) Non-Repudiation
provides protection against denial by one of the entities involved in communication of having participated in all or part of communication.

(1) NONREPUDIATION, ORIGIN
proof that the msg was sent by the specified party.

(2) NONREPUDIATION, DESTINATION
proof that the msg was received by the specified party.

Security MECANISMS.

Security Mechanisms are mechanisms designed to detect, prevent or recover from attacks. These mechanism can be divided into two:

(1) Specific Security mechanism
may be incorporated into appropriate

protocol layer in order to provide some of the OSI security Services.

(1) **Encipherment**

The use of mathematical algorithms to transform data into a form that is not readily intelligible.

(2) **Digital Signature**

data appended to, or a cryptographic Transformation of, a data unit that allows a recipient of the data unit to prove the source & Integrity of the data unit & protect against forgery.

(3) **Access Control**

A Variety of mechanism that enforce access rights to resources.

(4) **Data Integrity**

A Variety of mechanism used to assure the integrity of a data unit

(5) **Traffic Padding**

The insertion of bits into gaps in a datastream to frustrate traffic analysis attempts.

(6) **Routing Control**

Enables selection of particular physically secure routes for certain data

(7) **Notarization**

The use of a trusted third party to assure certain properties of a data exchange.

(2) Pervasive Security Mechanisms

Mechanisms that are not specific to any particular OSI security Service or protocol layer

(1) Trusted Functionality

That which is perceived to be correct with respect to some criteria

(2) Security Recovery

deals with req from mechanisms, such as event handling & management functions, & takes recovery actions.

Symmetric Encryption

→ Symmetric encryption is a form of cryptosystem in which encryption & decryption are performed using the same key. It is also known as conventional encryption.

→ Symmetric encryption transforms plaintext into ciphertext using a secret key & an encryption algorithm. Using the same key & a decryption algorithm, the plaintext is recovered from ciphertext.

→ Cryptography is most often associated with scrambling plaintext into ciphertext, then back again. Therefore it is science or study of the techniques of secret writing, especially code & cipher system.

→ Cryptanalysis is the study of analyzing information system in order to study hidden aspects of the systems.
Cryptanalysis is used to breach cryptographic security systems & gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

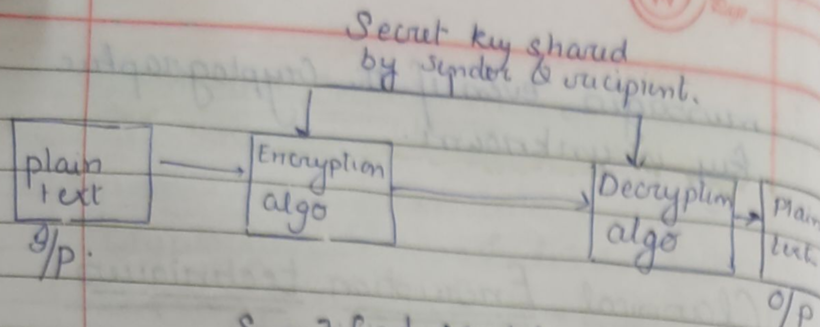
Classical Encryption techniques

Also k/a symmetric encryption scheme has five ingredients:

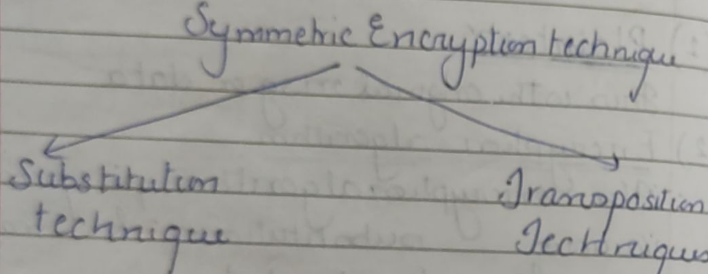
(1) Plaintext
This is the original msg or data
(2) Encryption algorithm
The encryption algorithm performs various substitutions & transformations on the plaintext.
(3) Secret key: The secret key is also I/p to the encryption algorithm. The key is a value independent of plaintext & of the algorithm.

(4) Ciphertext: This is a Scrambled msg produced as output. It depends on the plaintext & Secret key.
For a given plaintext two different keys will produce two different ciphertext.
(5) Decryption algorithm

This is essentially the encryption algo run in reverse. It takes ciphertext & Secret key & produces original plaintext.



Simplified Model of Conventional Encryption



Substitution Technique

A Substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

(1) Caesar Cipher

The earliest known use of a substitution Cipher, & the simplest, was by Julius Caesar. The Caesar Cipher involves replacing each letter of the alphabet with the letter Standing three places further down the alphabet.

Plain: meet me after the Party
Cipher: PHHW PH DIWHU WKH SDUWB

Note that the alphabet is wrapped around so that the letter following Z is A.

The algo can be expressed as:

$$C = E(3, P) = (P + 3) \bmod 26$$

(C → cipher text; E → Encry. algo; 3 → key; P → plain text)

$$\boxed{P = D(3, C) = (C - 3) \bmod 26}$$

In General Caesar algorithm Shift may be of any amount.

Problem

If it is known that a given ciphertext is Caesar Cipher, Then brute force cryptanalysis is easily performed: simply try all 25 possible keys.

(2) Monoalphabetic Ciphers

A monoalphabetic Substitution Cipher, also known as a simple substitution Cipher relies on a fixed replacement structure. That is, the Substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.

Plain text → A K A N K
Cipher " → E O E V O

~~(3) Polyalphabetic Ciphers~~

→ There is however, another line of attack. If the Cryptanalyst knows the nature of the plaintext, then the analyst can exploit the regularities of the language.

→ Monoalphabetic ciphers are easy to break they reflect the frequency data of the original alphabet.

(3) Polyalphabetic Cipher

~~Another is~~ It is an improvement on the Simple monoalphabetic technique. The idea is to use different monoalphabetic substitution as one proceeds through the plaintext message. ~~The~~ This approach is called Polyalphabetic Substitution cipher.

~~Feature~~

One of the main problems with Simple Substitution Cipher is that they are so vulnerable to frequency analysis. ~~of~~ Given a sufficiently large cipher text, it can easily be broken by mapping the frequency of its letters. A Polyalphabetic substitution Cipher involves the use of two or more cipher alphabets. Instead of there being a one to one relationship b/w each letter & its substitute, there is a one to many relationship b/w each letter & its substitute.

Vigenere Cipher is a polyaphabetic substitution based on tableau.

table given at the back.

Note that each row of table corresponds to Ceaser Cipher. The first row is a shift of 0; the second is a shift of 1 & the last is a shift of 25.

The Vigenere Cipher uses this table together with keyword to encipher a msg for suppose plaintext is

TO BE OR NOT TO BE

using keyword: RELATIONS.

We begin by writing the keywords, repeated as many times as necessary, above plaintext. To derive ciphertext using the tableau, for each letter in plaintext one finds intersection of the row given by corresponding keyword & column given by plaintext letters itself.

Keword	RELATIONSRELATION
Plaintext	TOBEORNOTTOBETHAT
Ciphertext	KSMEHZBBLKSMEMPOG

(4) Playfair Cipher

→ The best-known multiple-letter encryption cipher is the Playfair which treats plaintext as single units & translate these units into ciphertext.

→ This algo is based on the use of a 5×5 matrix of letters constructed using keyword.

→ let us construct this matrix suppose keyword is MONARCHY. **

→ fill the matrix by letters of keyword (minus the duplicates) from left to Right & from top to bottom

→ Remaining place in matrix is filled by remaining letters in alphabetic order.

→ The letter I & J are counted as one letter.

Plaintext is encrypted two letters at a time, according to the following rules:

(1) Repeating plaintext letters that are in the same pair are separated with filler letters, such as x so that balloon would be treated as ba lx lo on

(2) Two plaintext letters that fall in same row of a matrix are each replaced by the letter to the right with the first element of the row circularly following last. for eg ar is encrypted as RM

(3) Two plaintext letters that fall in same column are each replaced by letter beneath, with top element of the column circularly following the last. For eg: mu is encrypted as CM

(4) otherwise, each plaintext letter in a pair is replaced by letter that lies in its own row & column occupied by other plaintext letter.

Thus hs becomes BP

ea becomes IM or JM

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

HA | DO | BB
HA | DO | OB | BX | BX
BO | HR | AH | IA | IA

(5) Hill cipher

→ Hill Cipher is a polygraphic Substitution Cipher based on linear algebra.

→ Invented by Lester S. Hill in 1929

→ The encryption algorithm takes m successive plaintext letter & substitutes for them m ciphertext letters.

This can be expressed in term of column vectors & matrices.

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \mod 26$$

OR

$C = KP \mod 26$ → for ENCRYPTION

$P = K^{-1} C \mod 26$ → for decryption

(6) **ONE-TIME-PAD**

→ This scheme was suggested by Joseph

→ Joseph suggested the use of random key which is taken as long as the msg. This key is used for encrypting & decrypting single msg.

Example

Plaintext: HOW ARE YOU
Keyword NCB TZQ ARX

H	O	W	A	R	E	Y	O	U
7	14	22	0	17	4	24	14	20
N	C	B	T	Z	Q	A	R	X
13	2	1	19	25	16	0	17	23
↓	↓	↓	↓	↓	↓	↓	↓	↓
20	16	23	19	42	20	24	31	43
U	Q	X	T	Q	U	Y	F	R

TRANSPOSITION TECHNIQUES

A transposition cipher is a method of encryption by which the positions held by units of plaintext are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.

1. Reverse Cipher
   Write the msg backward
   plain I CAME
   Cipher EMACI

2. Rail-fence Cipher.
   here plaintext is written down as a sequence of diagonals & then read off as a sequence of rows: for example

meet me after

```
m   e   m   a   t   r
  e   t   e   f   e
```

Cipher → MeMatretefe

Steganography

Methods of Steganography conceal the existence of msg, whereas the methods of Cryptography conceals the meaning of msg.

Various Steganography Techniques that have been used historically are:

- **Character marking**
  Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light

- **Invisible Ink.**
  A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

- **Pin punctures** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

Steganography is however more sophisticated in todays world than above examples.

, allowing a user to hide large amount Information within image & audio files. The forms steganography are used in conjunction with cryptography so that Information is doubly protected.

Stream Cipher & Block Cipher

Stream Cipher

- It is a process that encrypts the msg bit by bit
- Example of Stream cipher is Vernam cipher also k/a One-time pad, Vigenere Ciper etc.

→ ~~For~~ It uses an infinite stream of pseudorandom bits as the key. For a stream cipher implementation to be secure, it's pseudorandom generator must be unpredictable & should never be reused.

→ One time pad, which is supposed to employ a purely random key, can potentially achieve "perfect secrecy". That is, it's suppose to be fully immune to brute force attacks. The problem with one time pad is that in order to create such a cipher, it's key should be long or even longer than plaintext.
In other words If you have 500Megabyte videofile that you like to encrypt you would need a key that's at least 4 Gigabytes long.

Block cipher

→ A block cipher is one in which a block of plaintext is treated as a whole & used to produce a cipher block of equal length.

→ A block cipher is an encryption algorithm that encrypts a fixed size of n-bits of data - known as a block - at one time.

→ Typically a block size of 64 or 128 bit is used.

→ If plain text is smaller than block size then padding is used.

→ Majority of symmetric cipher used today are actually block cipher. DES, Triple DES, AES are some example of block cipher.

→ In 1949, Shanon introduced the idea of Substitution-Permutation (S-P) networks in his paper which now forms basis of modern block cipher.

→ SP n/w are based on the two primitive cryptographic operations ~~we have seen before~~:

- ✦ substitution (S-box)
- ✦ permutation (P-box)

Substitution Operation

→ here a binary word is replaced by some other binary word.

→ Substitution operation is done in S-box.

→ ~~An S-box can have different number of inputs & outputs (If I/p is n bits then o/p is almost 2^n bits). Therefore here o/p grows rapidly.~~

Permutation Operation

→ A binary word has its bits reordered

→ The reordering forms the permuted order. This operation is performed in P-Box.

→ ~~This operation is performed in P-box. It take I/p of n bits & o/p generated is n! bits. which grows more slowly & hence is less secure.~~

Shannon Combined these two primitives & called it mixing transformation.

→ **Avalanche Effect**

where changing one I/p bit results in changes of approx half the O/p bits.

→ **Completeness Effect**

where each O/p bit is a complex function of all I/p bits

Diffusion & Confusion

The terms diffusion & confusion were introduced by claude Shannon

→ Shannon's Concern was to thwart cryptanalysis based on statistical analysis. The reasoning is as follows. Assume the attacker has some knowledge of the statistical characteristics of the plaintext. For example, in a human-readable msg in some language, the frequency distribution of the various letters may be known or there may be words or phrases likely to appear in msg. If these statistics are in a way reflected in the ciphertext, the cryptanalyst may be able to deduce the encryption key or part of key etc.

Shannon suggests two methods for frustating statistical cryptanalyst
1. Diffusion
2. Confusion.

DIFFUSION

In diffusion, the statistical structure of plain-text is dissipated into long range statistics of the ciphertext. This is achieved by having each ~~plaintext digit~~ ciphertext digit be affected by many plaintext digits.

In a block cipher, diffusion can be achieved by repeatedly performing some permutation

The mechanism of diffusion seeks to make the statistical relationship b/w the plaintext & ciphertext as complex as possible in order to thwart attempts to deduce the key.

CONFUSION

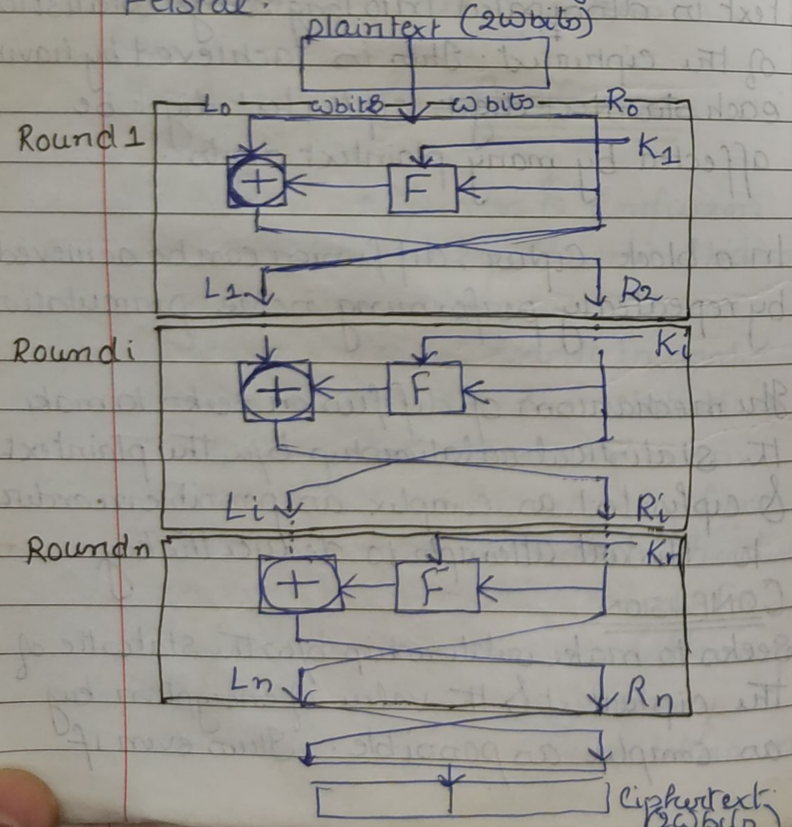
Seeks to make relationship b/w the statistic of the ciphertext & the value of encryption key as complex as possible. Thus even if can get some idea of ciphertext statistic he will not be able to deduce key because of complex relationship.

This is achieved by the use of a complex Substitution algorithm.

Feistel Cipher Structure

→ A feistal cipher is a block cipher with a symmetric structure.

→ Named after IBM cryptographer, Horst Feistal.



→ plaintext block of length 2w bits is i/p to the encryption algo

→ plaintext block is divided into two halves L_0 & R_0

→ The two halves pass through n Rounds of processing & then combine to ~~provide~~ produce the ciphertext.

→ Each round i has i/p L_{i-1} & R_{i-1} derived from previous round. The subkey K_i is derived from overall key K

→ All rounds have same structure. A substitution is performed on the left half of data. This is done by applying rounding function F to the right half of data & then taking X-OR of O/P of function & left half data.

→ After this permutation is performed that consist of interchanging of two halves of data.

→ This structure is a particular form of S-P network proposed by Shanon.

→ Exact realization of Feistal n/w depends on the choice of following parameters & design features.

(1) **Block Size**

Larger block size means greater security but

reduced encryption/decryption speed for a given algo. The greater security is achieved by greater diffusion.
Traditionally, a block size of 64 bit has been considered reasonable. However new AES uses 128 bit block size.

2- **Key SIZE**
Larger key size means greater security but may decrease encryption/decryption speed. Key size of 128 bits has become common.

3- **Number of Rounds**
mutiple Rounds offer increasing security. A typical size is 16 rounds.

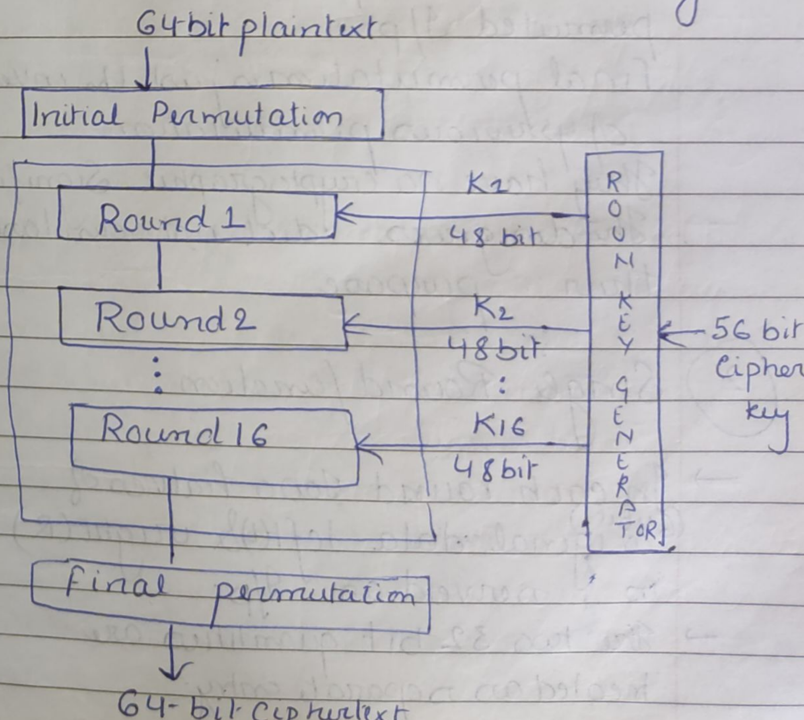
4- ~~Subkey Generation algo~~ **ROUND FUNCTION**
Greater complexity means greater resistence to cryptanalysis.

5- ~~Round function~~
SUBKEY GENERATION ALGO
Greater complexity in this algo should lead to greater difficulty of cryptanalysis.

Data Encryption Standard.

→ DES was developed in 1970's
→ It was based on IBM Lucifer Cipher
→ ~~A~~ It was used as standard in 1977 by Federal Information Processing standard (FIPS)
→ DES is a symmetric key block cipher
→ DES is an Implementation of feistal cipher.

→ It has 16 Rounds, block size is 64 bit, 56 bit ~~eff~~ key, & 48 bit of key is used in each round as subkey.



DES mechanism can be explain under in three parts

1. Initial & Final Permutation
2. Round function
3. Key generation

(1) → Initial & Final permutation

First 64-bit plaintext passes through an Initial permutation that rearranges the bits to produce the permuted I/p.
Final permutation is just the inverse of previous permutation.
They have no cryptographic significance. The designers did not disclose their purpose.

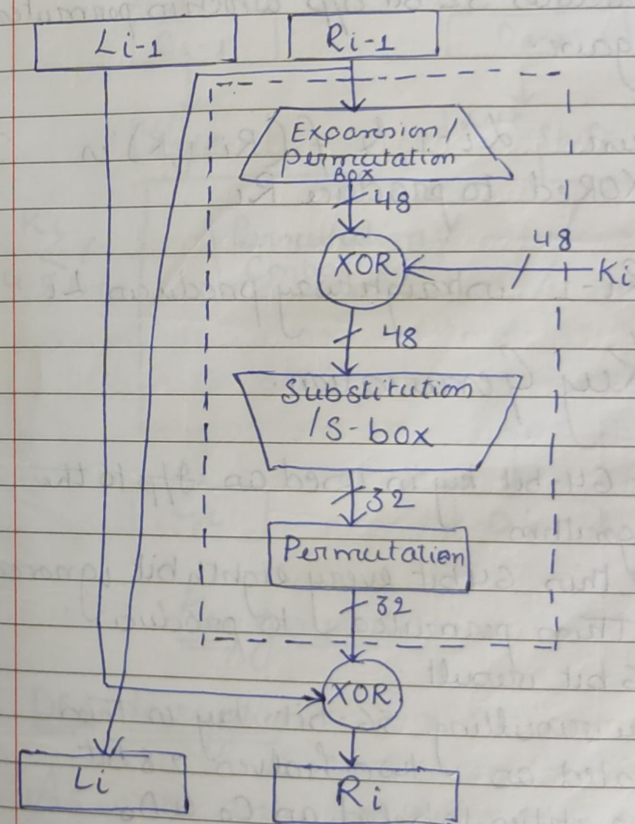
(2) Single Round function:

→ In each round two halves of (64bit) original data left(L) & right(R) is served as I/p.
→ The two 32-bit quantities are treated as separate entry.

→ The overall processing at each round can be summarized in the following formulas:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \times F(R_{i-1}, K)$$

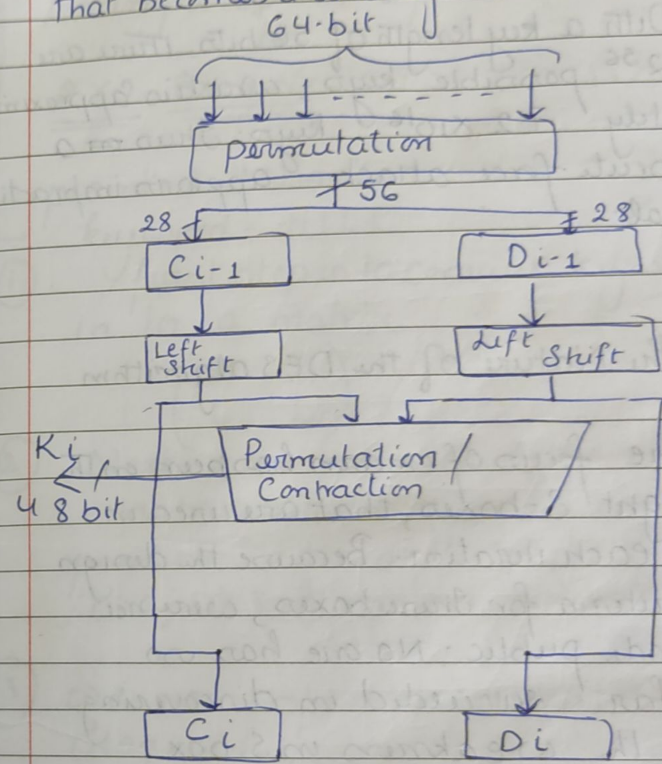


Single Round of DES.

- The key K_i is 48 bits. The R input is 32 bits. This R I/p is first expanded so that size becomes equal to key size.
- The Resulting 48 bit is XORed with K_i. This 48 bit result passes through a substitution function that produces 32-bit O/p which is permuted again.
- Then L_{i-1} & $f(R_{i-1}, K)$ is XORed to produce R_i
- R_{i-1} straightway produces L_i

(3) Key Generation.

- A 64-bit key is used as I/p to the algorithm
- In this 64 bit every eighth bit ignored & then permuted to produce 56 bit result.
- The resulting 56-bit key is then treated as two halves 28 bit quantities labeled as C_0 & D_0
- at each round C_{i-1} & D_{i-1} are separately subjected to circular shift.
- These shifted values serve as I/p to next round. They also serve as I/p to permuted Choice Two, which produces a 48 bit O/p that becomes a subkey.



Key generation.

DES decryption

As with any Feistal cipher, decryption uses the same algorithm as encryption, except that the application of subkeys is reversed.

Strength of DES

① **The Use of 56-bit Keys**

With a key length of 56 bits, there are 2^{56} possible keys, which is approximately 7.2×10^{16} keys. Thus a brute force attack appears impractical.

② **The Nature of the DES algorithm**

The focus of concern has been on the eight S-boxes, that are used in each iteration. Because the design criteria for these boxes, were not made public. No one has so far succeeded in discovering the weakness in S box.

③ **Timing Attacks**

Timing attack is one in which Information about the key or the plaintext is obtained by observing how long it takes a given implementation to perform decryption on various ciphertext.

DES appears to be fairly resistance to successful timing attacks.

Example of hill cipher.

2×2 Example.

→ plaintext = "shor"
→ keyword = HILL

① first step is to convert keyword in to a matrix

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}$$

② Next we convert each letter in above matrix into a number by its position in the alphabet (like A = 0, B = 1, C = 2, D = 3 & so on Z = 25) $= \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$

③ We now split the plaintext into diagraph

$$\begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} O \\ R \end{pmatrix}$$

④ Convert these matrix into column vectors

$$\begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix}$$

⑤ Now to convert plaintext into cipher text

C = KP mod 26 [ENCRYPTION]

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 182 \\ 275 \end{pmatrix} \bmod 26 = \begin{pmatrix} 0 \\ 15 \end{pmatrix}$$

Block cipher mode of operation

$= \begin{pmatrix} A \\ P \end{pmatrix}$

SH is encrypted as AP.

similarly

$\begin{pmatrix} O \\ R \end{pmatrix}$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix}$$

$$= \begin{pmatrix} 234 \\ 341 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 0 \\ 3 \end{pmatrix} = \begin{pmatrix} A \\ D \end{pmatrix}$$

OR is encrypted as AD.

⑥ DECRYPTION

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

To decrypt a ciphertext we must find inverse of matrix

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

step 1 for finding inverse

(a) find the multiplicative inverse of the determinant

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = 7 \times 11 - 8 \times 11$$

$$= -11$$

$-11 \bmod 26$

#

$\Rightarrow 26 - 11$

$= 15 \bmod 26$

$= 15$

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

$15 \times \frac{1}{15} = 1$

$15 \times ? = 1 \bmod 26$

$15 \times 7 = 105 \equiv 1 \bmod 26$

so multiplicative Inverse of determinant modulo 26 is 7

~~&~~ (b) find adj Matrix.

$$adj \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$adj \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} = \begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix}$$

Again, we need to modulus 26 of above matrix

$$\begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$$

$$7 \times \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 105 & 49 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

If $K = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$ then $K^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} A \\ P \end{pmatrix}$$

$$= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 0 \\ 15 \end{pmatrix}$$

$$= \begin{pmatrix} 330 \\ 345 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} S \\ h \end{pmatrix}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} A \\ D \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

$$= \begin{pmatrix} 66 \\ 69 \end{pmatrix}$$

$$= \begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} O \\ R \end{pmatrix}$$

Block cipher modes of operation

- A block cipher algorithm is a basic building block for providing data security
- To apply a block cipher in a variety of applications, four "modes of operation" have been defined by NIST (FIPS 81)

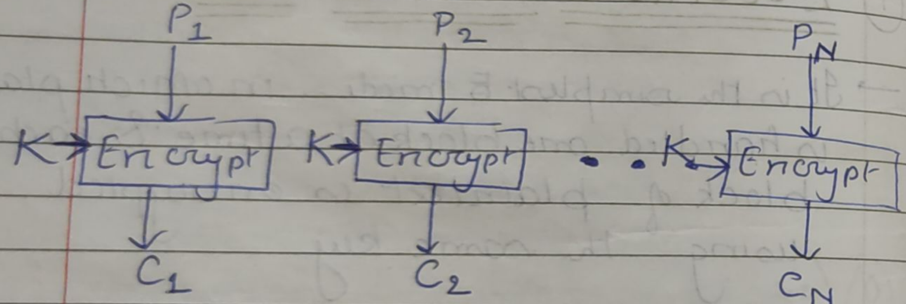
(1) ELECTRONIC CODEBOOK MODE

- It is the simplest mode, in which plaintext is handled one block at a time & each block of plaintext is encrypted using the same key
- The term codebook is used because, for a given key, there is unique ciphertext for every b-bit block of plaintext
- For a msg longer than b bits, the procedure is simply to break the msg into b-bit blocks, padding the last block if necessary. Decryption is performed one block at a time, always using the same key.

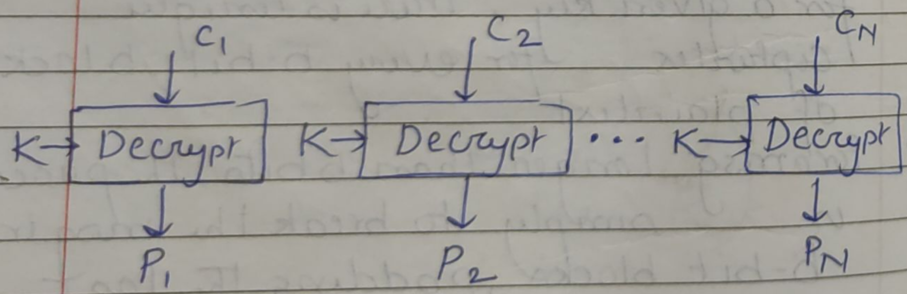
→ The ECB method is ideal for short amount of data, such as an encryption key

→ In ECB if the same b-bit block of plaintext, appears again then ECB always produces same ciphertext

→ for lengthy msg ECB is not secure



(a) ENCRYPTION



(b) Decryption

Cipher block chaining Mode (CBC)

→ CBC is an improvement over ECB, if same plaintext block is repeated in CBC, a different ciphertext block is produced.

→ The I/p to Encryption algo is XOR of the current plaintext block & the preceding ciphertext block, the same key is used for each block.

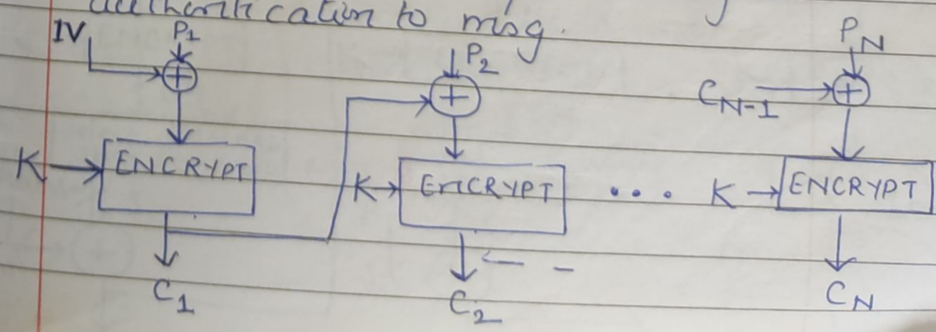
→ To produce 1st cipher block, an Initialization Vector is XORed with first block of plaintext

→ On decryption, the IV is XORed with o/p of the decryption algorithm to recover the first block of plaintext.

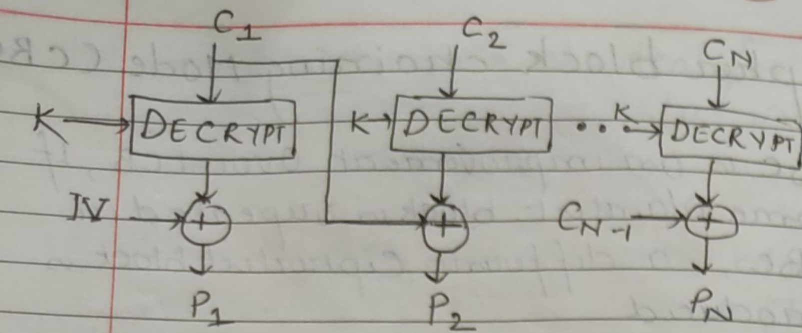
→ IV must be known to both the sender & Receiver but unpredictable by a third party.

→ It is an appropriate technique of encryption for lengthy msg

→ It provides both confidentiality & authentication to msg.



ENCRYPTION



DECRYPTION

(3) Cipher feedback Mode

operation of CBC mode are
→ Load the n-bit Initialization Vector in the top register
→ XOR the n-bit plaintext block with data value in the top register

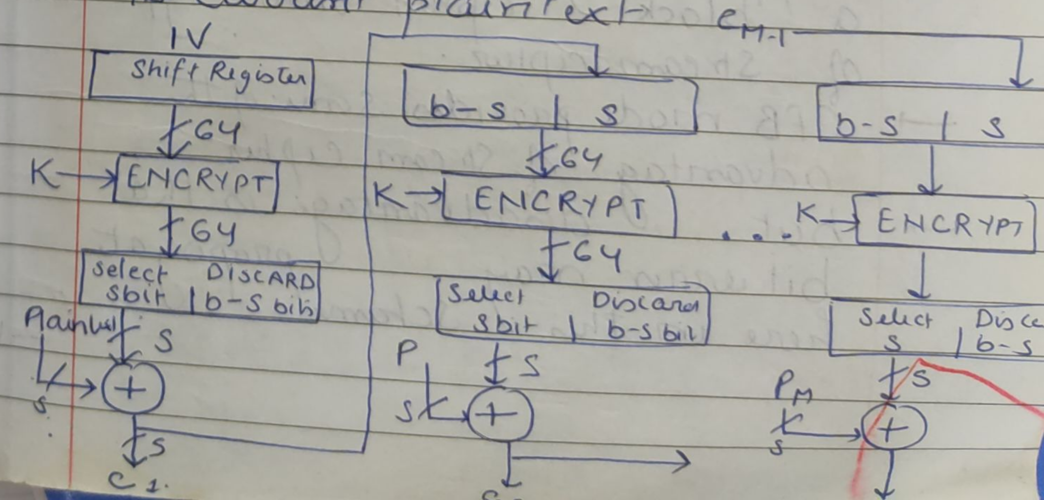
Operation of CFB mode is
→ Load the IV in the top register with underlying block cipher with key K

(3) Cipher Feed back Mode

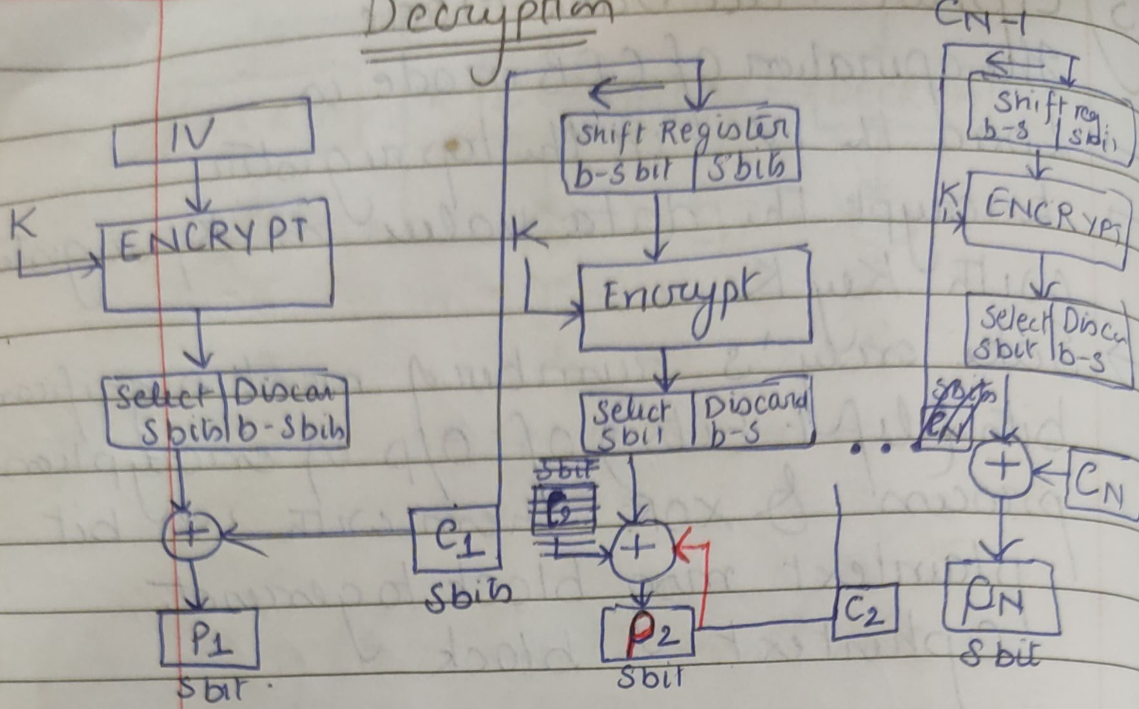
The operation of CFB mode is
→ Load the IV in the top register
→ Encrypt the data value in top register with key K
→ Take only 's' number of most significant bits (left bits) of o/p of encryption process & XOR them with 's' bit plaintext msg block to generate ciphertext block

→ Feed cipher block into top register by shifting already present data to the left & continue the operation till all plaintext blocks are processed

→ Essentially, the previous ciphertext block is encrypted with key & then the result is XORed to the current plaintext



Decryption



→ CFB has a very strange feature. In this mode user decrypts the Ciphertext using only the Encryption process of block cipher. The decryption algo of underlying block Cipher is never used.

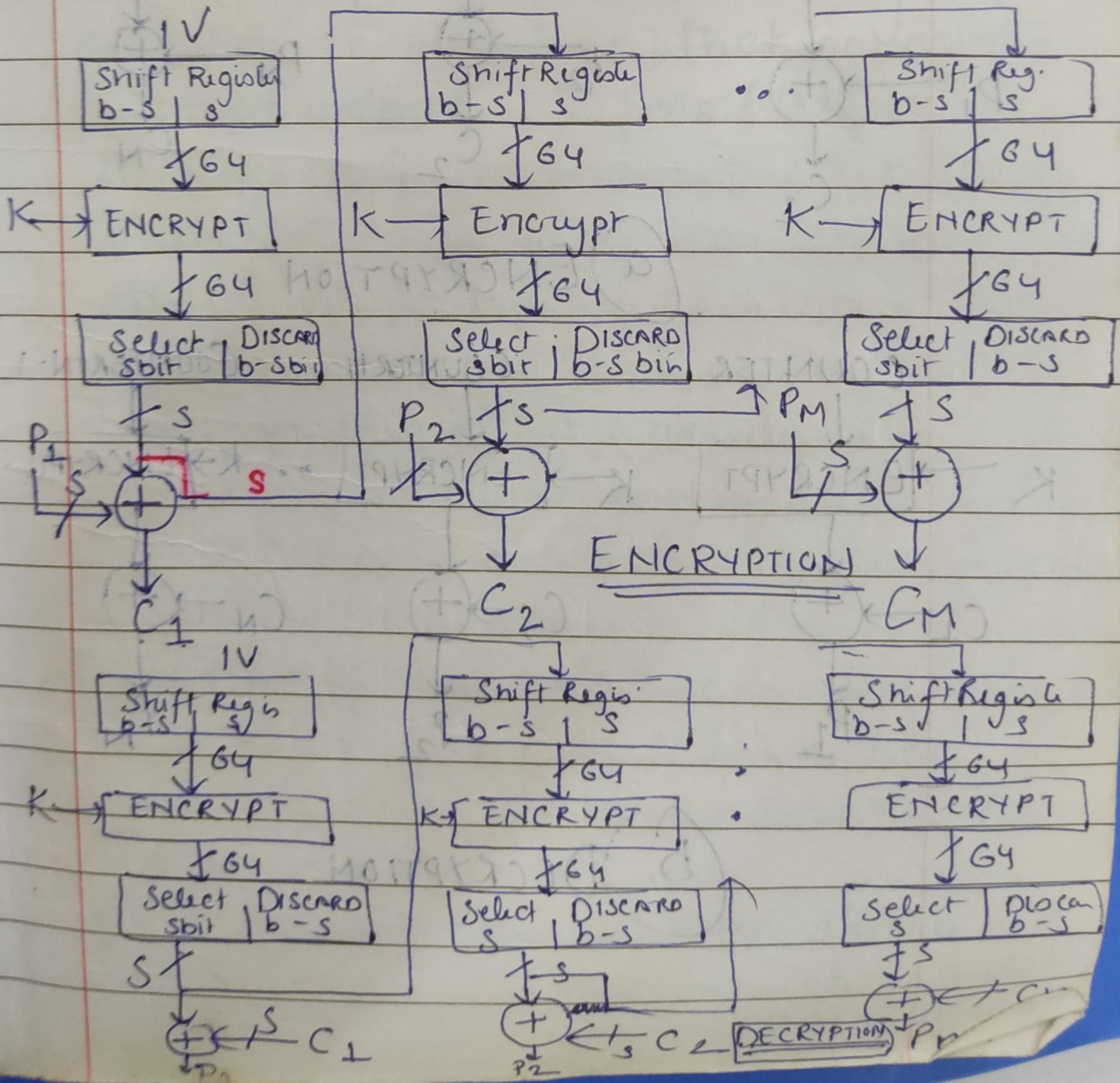
→ Apparently CFB mode is converting a block cipher into a type of Stream cipher.

→ CFB mode provides some of the advantage of Stream cipher

→ but disadvantage is that bit error may propogate here in this Scheme

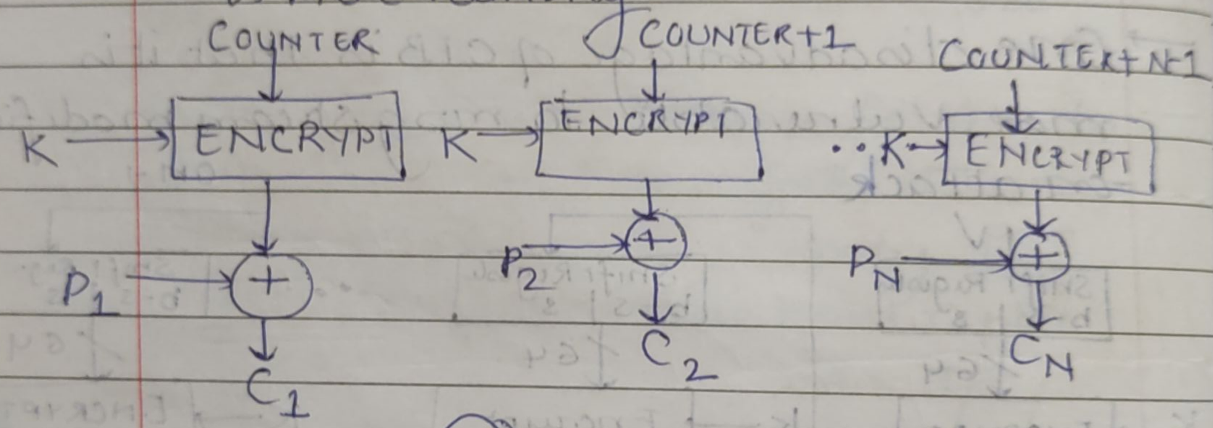
Output Feed back mode (OFB)

- OFB mode is similar in structure to that of CFB.
- here output of Encryption function is fed back to the Shift register.
- an advantage OFB method is that bit error in transmission do not propagate.
- One disadvantage of OFB is That it is more vulnerable to msg stream modification attack

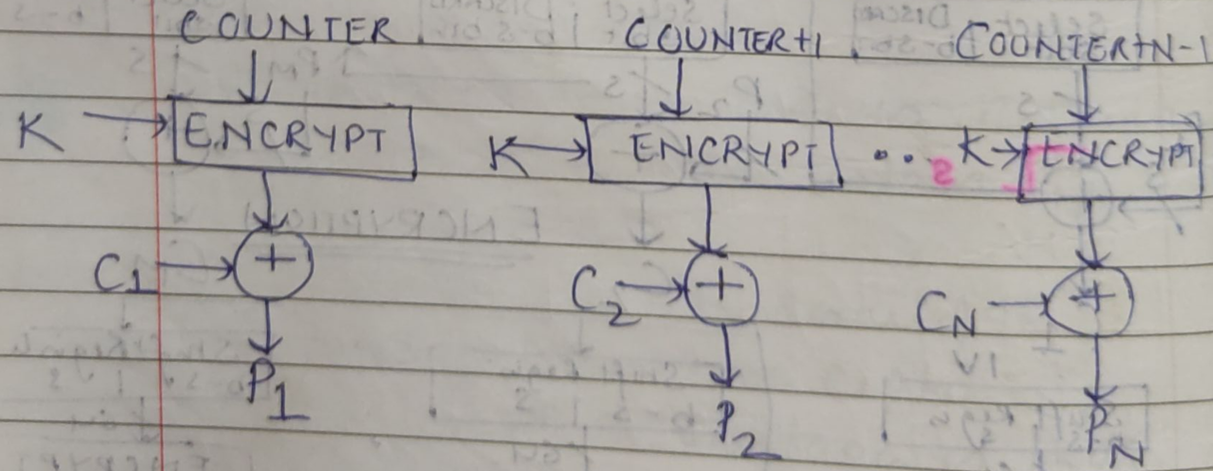


(5) COUNTER MODE

- Typically the counter is initialized to some value & then incremented by 1 for each subsequent block
- For encryption, the counter is encrypted & then XORed with the plaintext block to produce ciphertext block; there is no chaining



(a) ENCRYPTION



(b) DECRYPTION