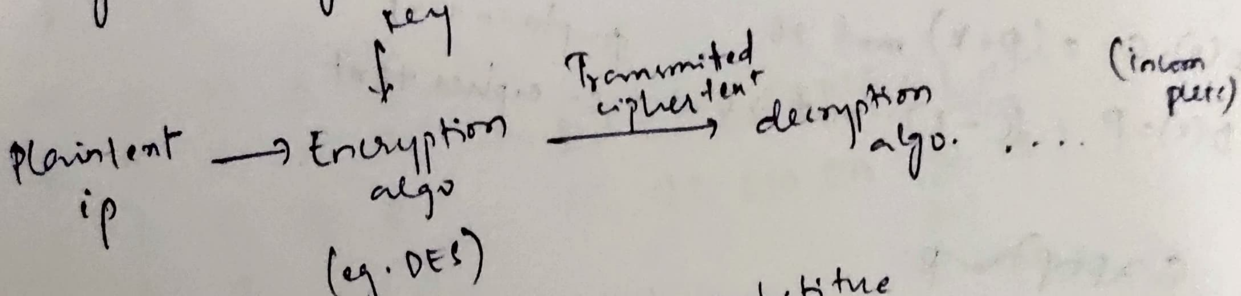
12/9 Symmetric Encryption

Basic Terminology:

- plaintext, cyphertext, cipher, key.
  encipher (encrypt), decipher (decrypt)
  cryptography
  cryptanalysis (code breaking)
  cryptology.

→ Symmetric cypher model



→ Requirement:

1. a strong encryption algo < substitue / transposition
2. a secret key known only to sender/receiver.

$Y = E_K(X)$ → encryption, X → plain text, K → key, Y → cipher text

$X = D_K(Y)$. → decryption.

Cryptography:

- characterize cryptographic system by:
  - type of encryption operations used ↳ substitution/transposition/product
  - no. of keys used → single key or private / two-key or public
  - way in which plaintext is processed
    ↳ block/stream.

Substitution Techniques

Cryptanalysis :

- objective to recover key not just

- Classical Substitution Ciphers :

Caesar Cipher

- replaces each letter by 3rd letter on
  i.e., 3 shifts ahead.

$E(P) = C = (p+k) \bmod 26$ p - plain text

$D(C) = P = (C-k) \bmod 26$ c - cipher text

~~$C = E(p) \to p$.~~

- only have 26 possible ciphers.
- a brute force search
- easy to break.

Monoalphabetic Cipher :

- rather that just shifting the alphabet, could shuffle the letters arbitarily
- the key here is now a permutatn.
  hence key is 26 letters long.

now we have $26! = 4 \times 1026$ keys

- with so many keys, might think is secure
  - but might be wrong.
  - problem is language characteristics.

Cryptanalysis of this cipher

Playfair Cipher

Playfair key Matrix:

- a 5×5 matrix of letters based on a keyword.
- fill in letters of keyword
- fill rest of matrix with other letters.
- only One cell can contain two letters as there are 26 alpha & 25 cells.

rules for encrypting & decrypting — ppt

Eg: keyword - 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

NITWARANGALX

AG QZ RM RA IN SU

JN

- same filler letter for entire msg.

Given matrix - ppt

tm

filler ~~cipher~~ letter - M

plaintext :

I only regret that I have but one life to give formycountry.

MA PA ZO QH GJ HB IG HT IG XC JZ ML QC AT

GK

KZ

JF ML AH XC SM OB VF RS P I OZ

FF

16/9/22

Polyalphabetic Ciphers

vigenere cipher

{key} cipher $(S+T) \bmod 26$

Autokey cipher:

keyword is prefixed to message as key.

One-Time Pad:

- ~~a~~ one key will be used only for one message.
- if a truly random key as long as the message is used, the cipher will be secure.
- since for any plaintext & any ciphertext there exists a key mapping one to another, sharing each key is a problem

Hill cipher:

- The encryption algorithm takes m successive plain text & substitute for them m cipher text letters.

key K

$$K^{-1} = (\det K)^{-1} (-1)^{i+j} (D_{ij})$$

where D is the subdeterminent formed by deleting i^{th} row & j^{th} column of K.

- block cipher

~~roa~~ Key matrix size = block size.

$$C = KP \bmod 26$$

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

For K^{-1} we need $\left[\frac{1}{\det(K)} \right]$ i.e., multiplicative inverse of $\det(K) \bmod 26$.

Ex:-

P = EG

$K = \begin{bmatrix} 3 & 2 \\ 3 & 5 \end{bmatrix}$ $K^{-1} = \begin{bmatrix} 5 & -2 \\ -3 & 3 \end{bmatrix} \times \cancel{9} \times 3 = \begin{bmatrix} 15 & -6 \\ -9 & 9 \end{bmatrix}$

15 − 6 = 9 det(K) = 9

$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 24 \\ 16 \end{bmatrix}$ det inverse = 3

$9 \times \boxed{3} \bmod 26 = 1$

$P = \begin{bmatrix} 15 & -6 \\ -9 & 9 \end{bmatrix} \begin{bmatrix} 24 \\ 16 \end{bmatrix} \bmod 26 =$ [illegible]

Transposition Ciphers :

Rail Fence cipher

- write message letters out diagonally over a number of rows.
- then read off cipher row by row.

Ex:- m e m a t r h t g p r y
e t e f e t e o a a t

cipher:- mematrhtgpryetefeteoaat.

Row Transposition ciphers :

- write letters of message out in rows over a specified no. of cols.
- then reorder the cols, according to some key before reading off the rows.

20/9/22

Block ciphers Modes of operation

1. Electronic Code Book (ECB):

key is same for whole message

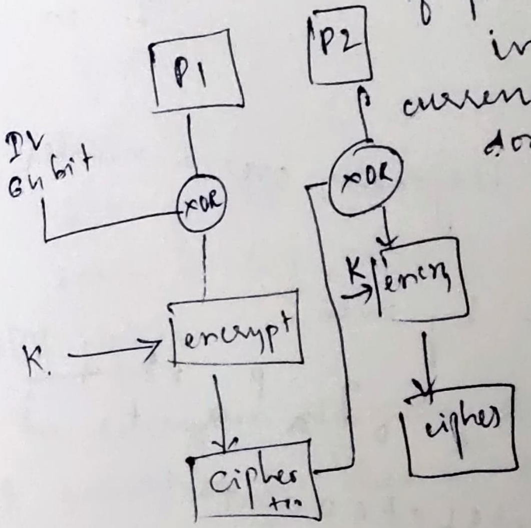
Each block encrypted at a time.

2. cipher block chaining mode (CBC):

Initialization vector (IV) - randomly generated

size same as plain text block size.

B1 64bit

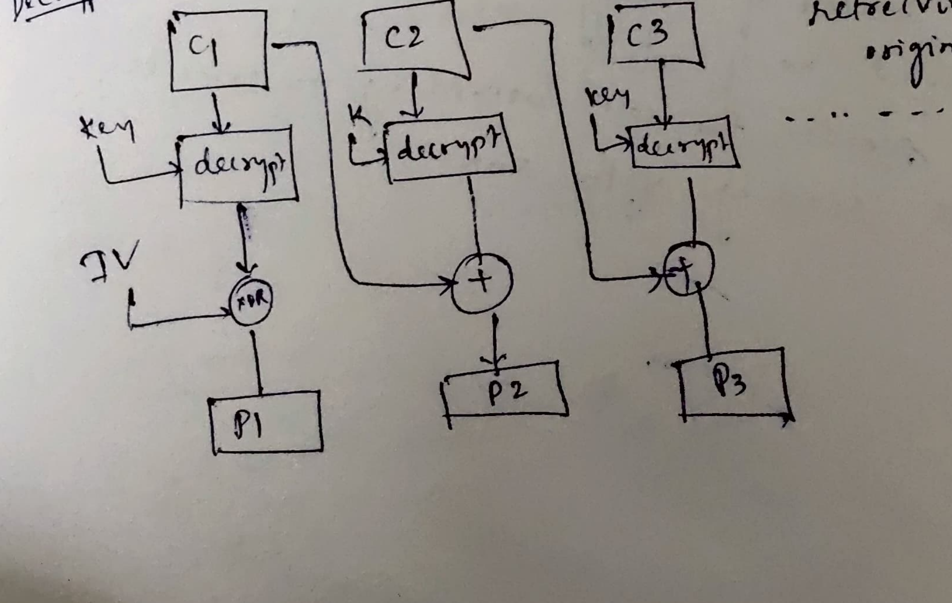


from second block, the cipher text of prev Block is used as initialization vector for current block & encryption is done using the same key for all blocks.

→ In this scheme, ~~the~~ the ip to the encryption algo is the XOR of the current plaintext block & previous ciphertext block.

- Apart from the key, the IV has also to be shared between both parties. (using a trusted third party)

Decryption:

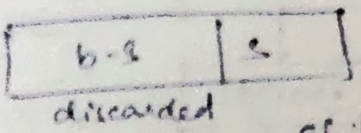


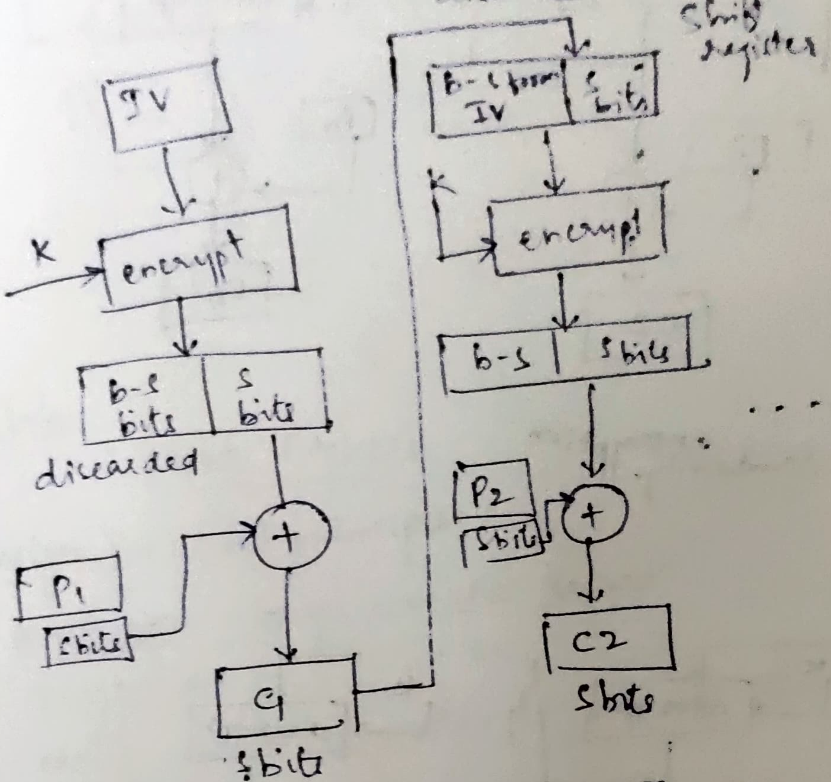
retreiving original msg on receiver side.

5. Cipher Feedback Mode (CFB):

input is processed s bits at a time

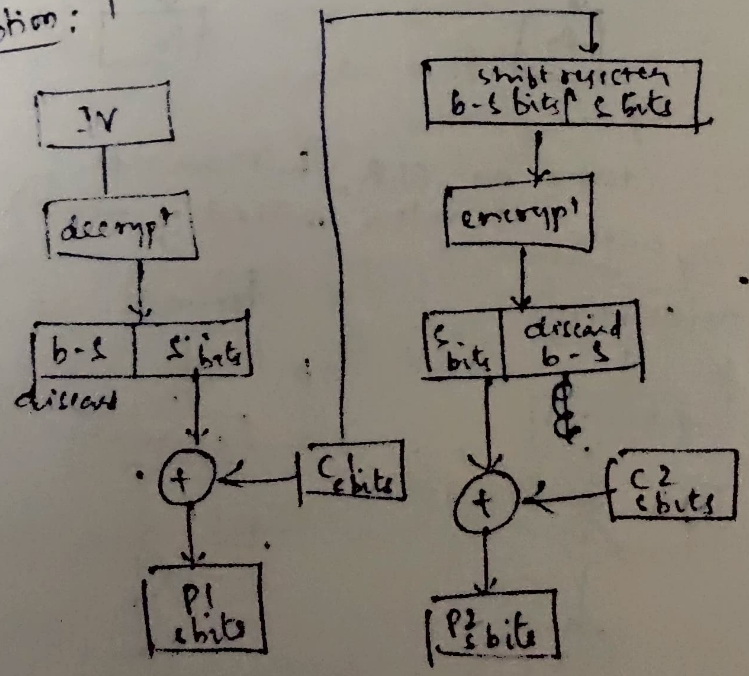
b. block size.



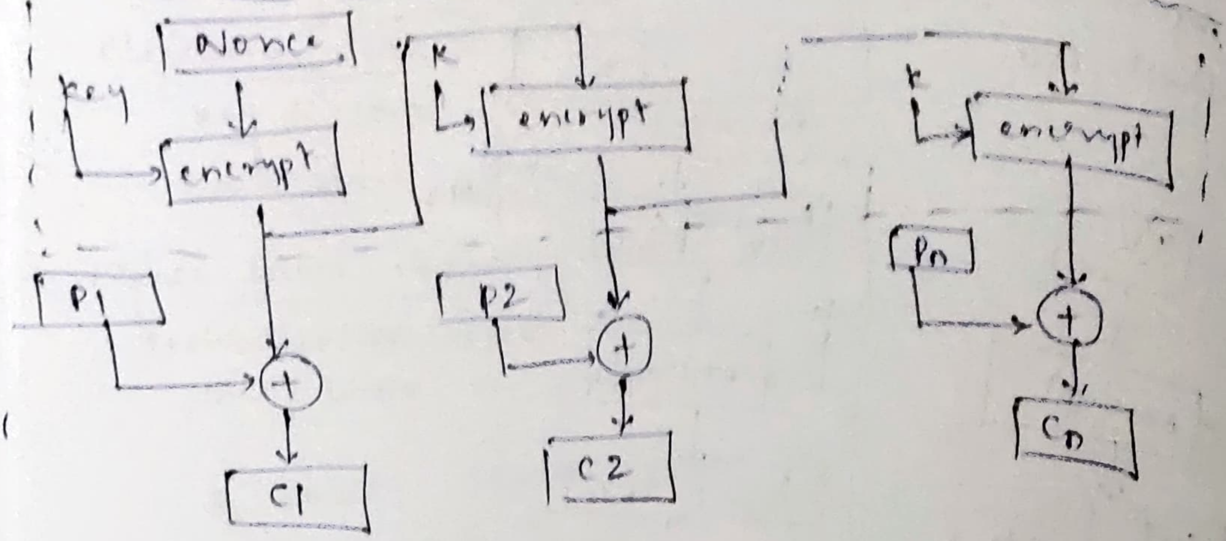


The ip is processed s bits at a time. The preceding ciphertext is used as ip to the encryption algorithm to produce.. ~~pseu~~

Decryption:

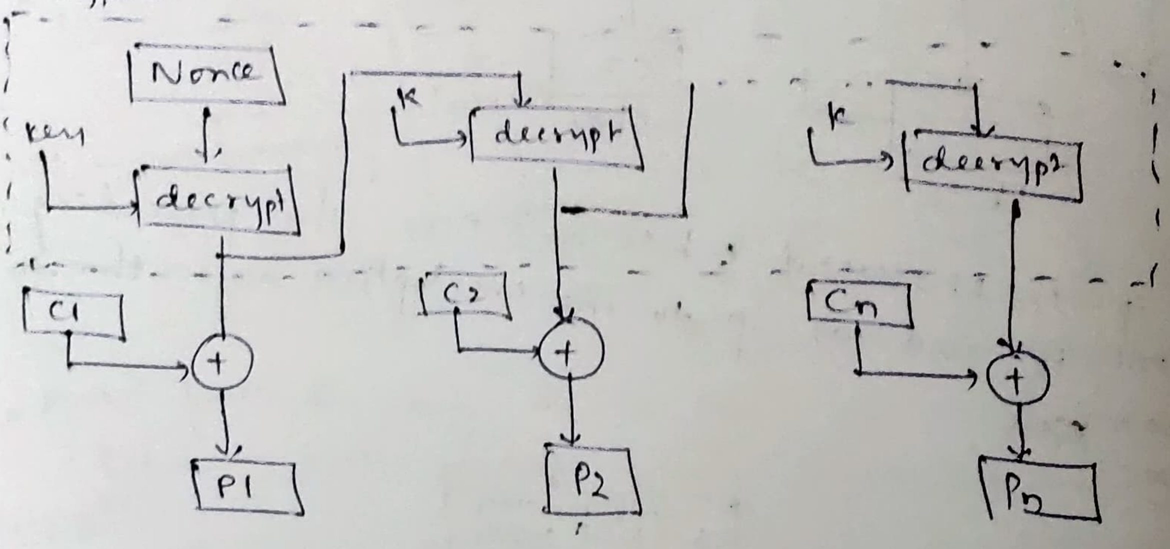


4. Output feedback mode (OFB):



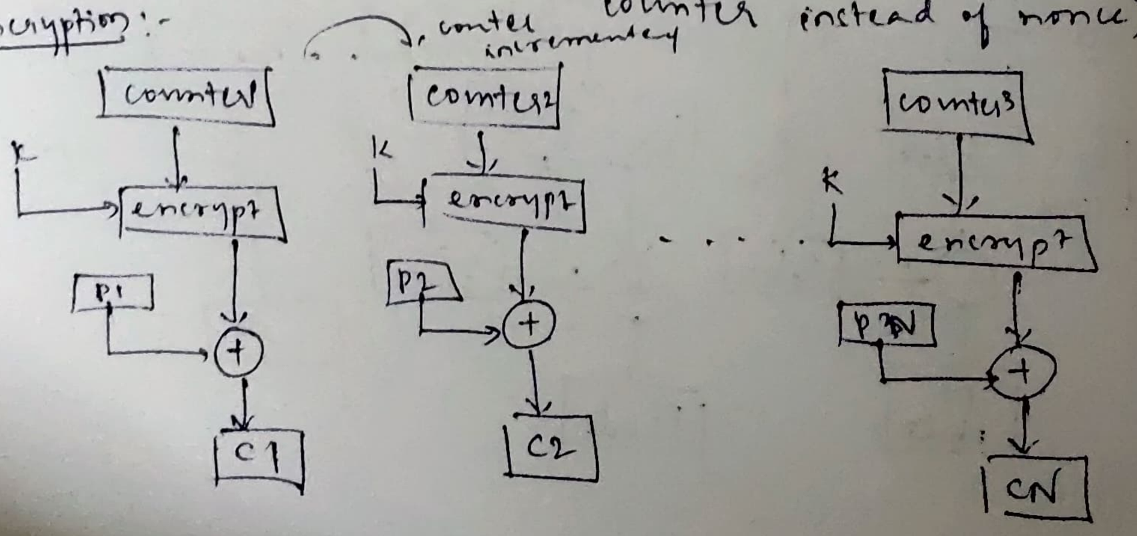
nonce-generated encryption randomity.

Decryption:-

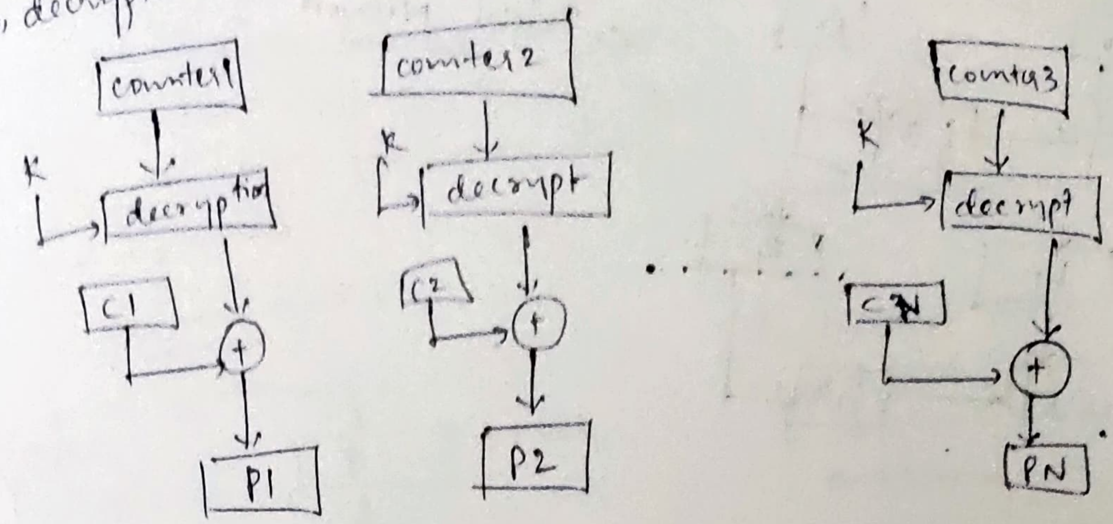


5. Counter mode: (same as OFB, but we use counter instead of nonce)

Encryption:-



b) decryption



22/9/22

Block Ciphers

Design features/ principles :

1. Block size : larger - more secure
2. key size : "
3. No. of rounds : multiple rounds increasing security.
4. Encryption modes

Feistel Network :

- A feistel network is fully specified, given ;
  - the block size : 2W   W: window.
  - no. of rounds : d
  - d round functions $f_1 \dots f_d : \{0,1\}^w \rightarrow \{0,1\}^w$.

Encryption :-

L: - left half
R: - right half.

- $L_1 = R_0 \quad R_1 = L_0 \oplus f_1(R_0)$
- $L_2 = R_1 \quad R_2 = L_1 \oplus f_2(R_1)$

$\vdots$

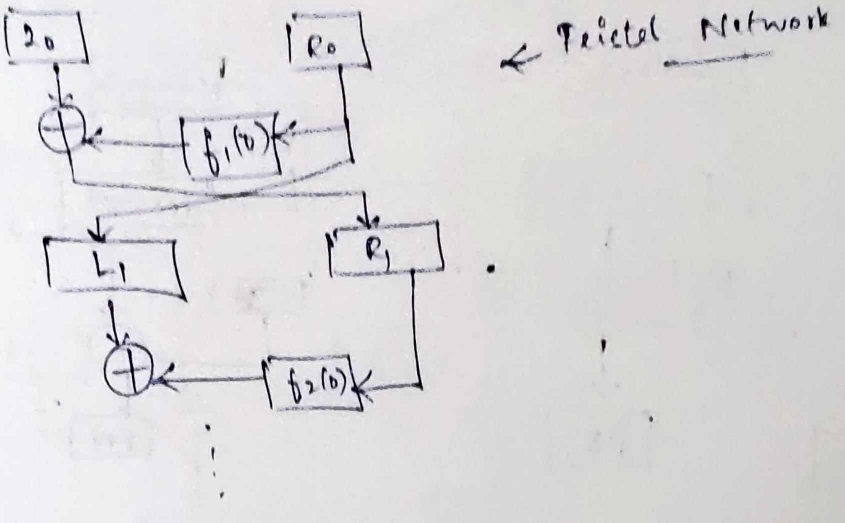
- $L_d = R_{d-1} \quad R_d = L_{d-1} \oplus f_d(R_{d-1})$

Decryption :-

- $R_{d-1} = L_d \quad L_{d-1} = R_d \oplus f_d(L_d)$

$\vdots$

- $R_0 = L_1 ; \quad L_0 = R_1 \oplus f_1(L_1)$.



DES Features : (Data Encryption Standard)

- features:
  - Block size = 64 bits
  - key size = 56 bits (in reality, 64 bits, but 8 are used as parity-check bits for error control, see next XOR of all 7 bits slide).
  - No. of rounds = 16
  - 16 intermediary keys, each 48 bits

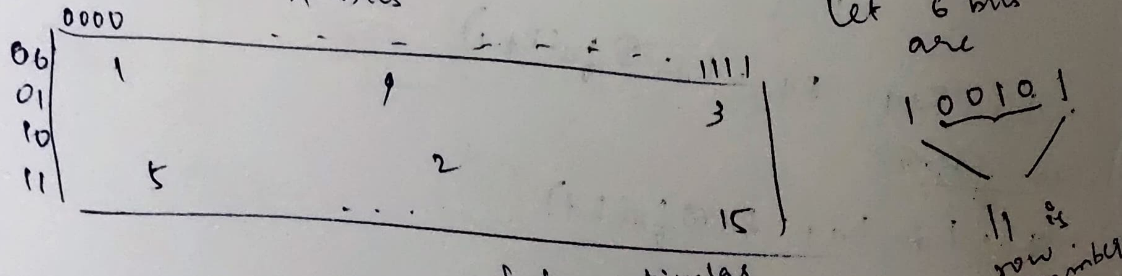
→ every 8th bit is a parity bit i.e., XOR of all 7 bits ahead of it.

— incomplete.

DES "f(0)" function :

- Expansion function — 32 bit ip to 48 bit so as to match the key size.
- Substitution fn : (S-box)
  ↳ 48 bit to 32 bit

6 bits at a time considered, reduced to 4 bits



11 is row number

0010 is col no.

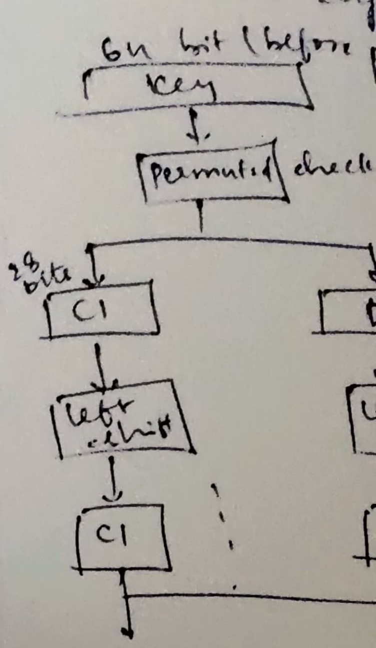
that particular entry is used to reduce the 6bit to 4bit

- DES key generat

- how a 56 b

How key

64 bit (before



- DES Weak key

Weak keys : k

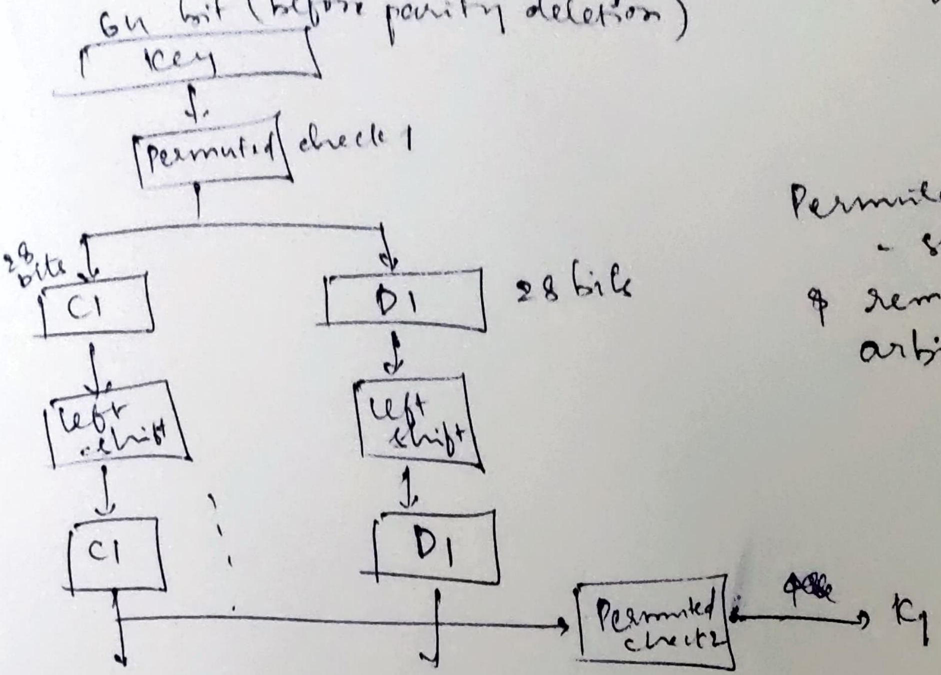
generated in mo

- DES has 4 w

- DES key generation (K_1 - K_{16})

- how a 56 bit key is reduced to 48 bit?

How key for every round is diff.



Permuted check
- some permutation
& removing 8 bits arbitarily.

- DES weak keys.

Weak keys : keys make the same sub-key to be generated in more than one round.

- DES has 4 weak keys.