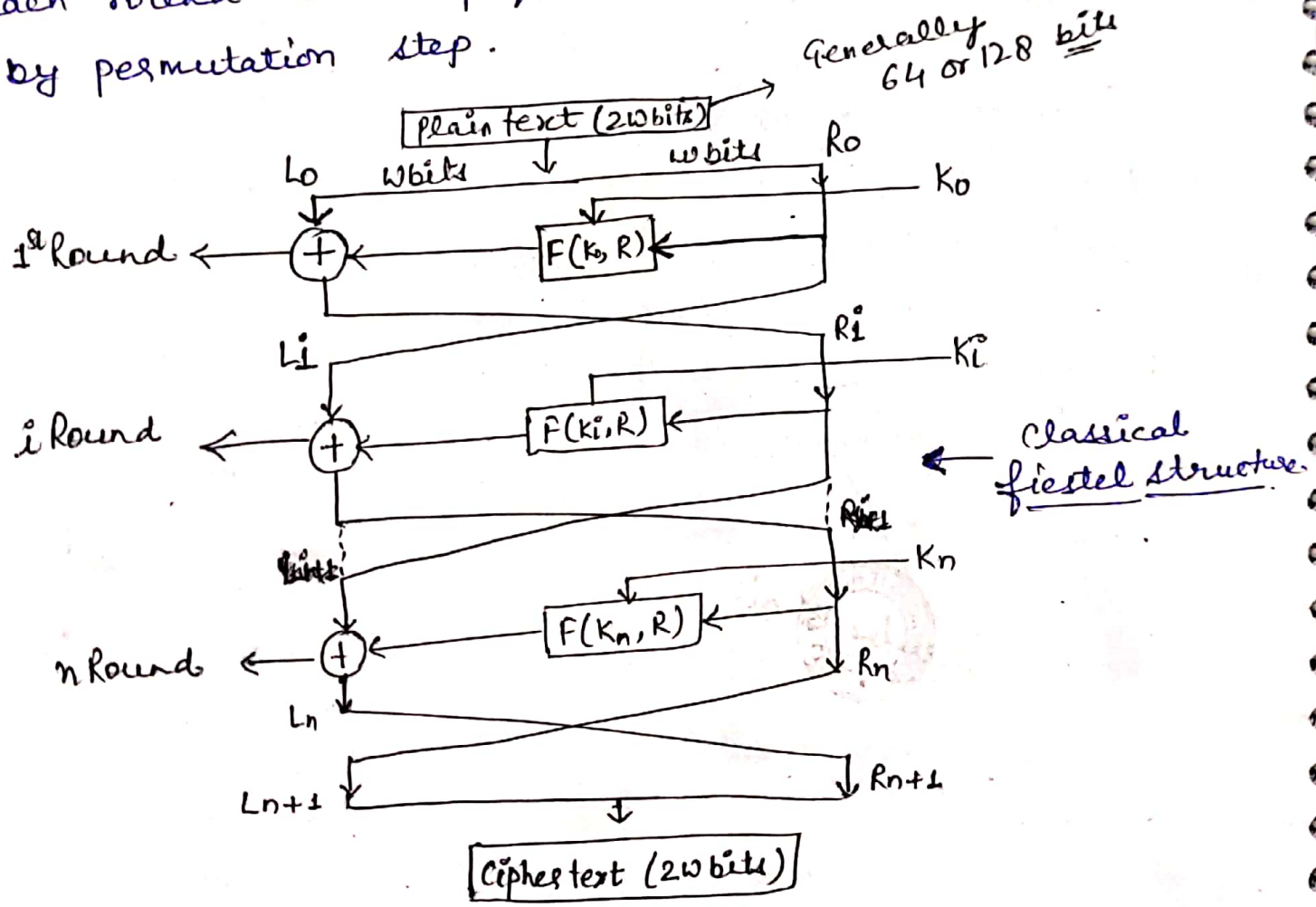
UNIT-II

Block cipher structure :- A block cipher is an encryption/decryption scheme in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

→ Many block ciphers have a fiestel structure.

The fiestel structure – It is not a specific scheme of block cipher. In encryption process uses the fiestel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by permutation step.



Design features →

① Block size – larger block size mean greater security. Traditionally a block size of 64 bits has been considered a resonable tradeoff and was nearly universal in block cipher.

required by the customer.

② - Key Size - Key sizes of 64 bits or less are now widely considered to be inadequate & 128 bits has become a common size.

③ - No. of Rounds - A typical size is 16 rounds.

④ - Subkey generation - Subkeys are derived by original key. for greater complexity.

⑤ - Round function - Difficult part is designing of round function 'F' inorder to unbreakable scheme.

Working of fiestel structure -

- The input block to each round is divided into two halves that can be denoted as L & R.
- In each round, the right half of the block R, goes through

unchanged but, the left L goes through an operation that depends on R and the encryption key. First we apply an encryption function "F" that takes two inputs, the key K & R. the O/P of function XOR with L and form an output.

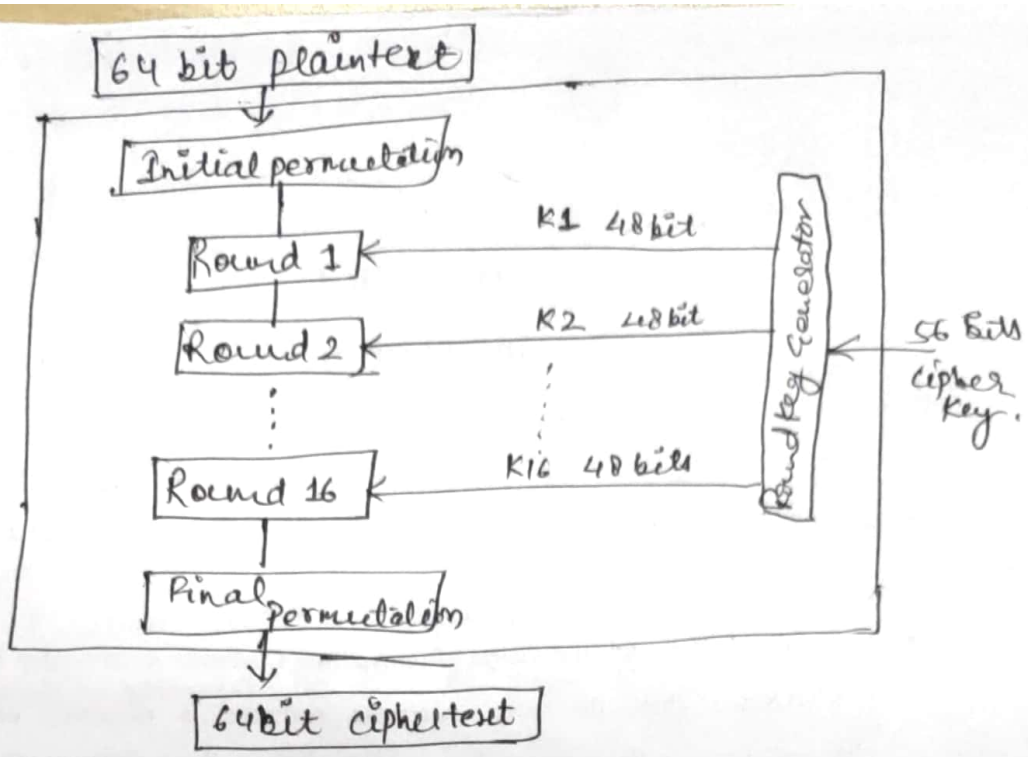
- In DES, each round uses a different key, although all these subkeys are related to the original key.
- The permutation step at the end of each round swaps the modified L and unmodified R. Therefore the L for the next round would be R of the current round and R for the next round be the O/P of L of the current round.
- Above substitution & permutation steps form a 'round'. The no. of rounds are specified by the algorithm.
- Once the last round is completed then the two sub-blocks, R & L are concatenated to form cipher text.

DES (Data Encryption Standard) – DES is a symmetric-key block cipher published by the National Institute of standards & technology (NIST).

DES is an implementation of a fiestel cipher. It uses 16 round fiestel structure. The block size is 64-bit. Though key length is 64 bit, DES has an effective key length of 56 bits. Since 8 bits of the 64 bits of the key are not used by the encryption algo. (f^n as check bits only).

Same key → ENC, DEP.

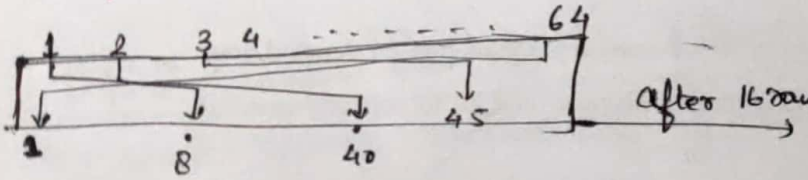
64 bit P.T → DES → 64 bit C.T



DES General structure

Initial Permutation

Occurs only once before the first round.



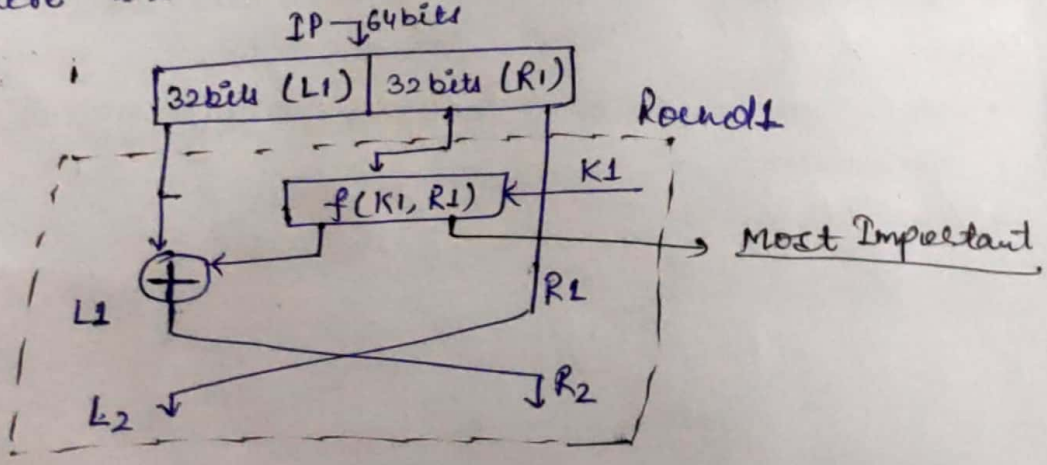
after 16 rounds

Final Permutation:-

Both initial & final permutation are straight P-boxes that are inverses of each other. They have no cryptographic significance in DES.

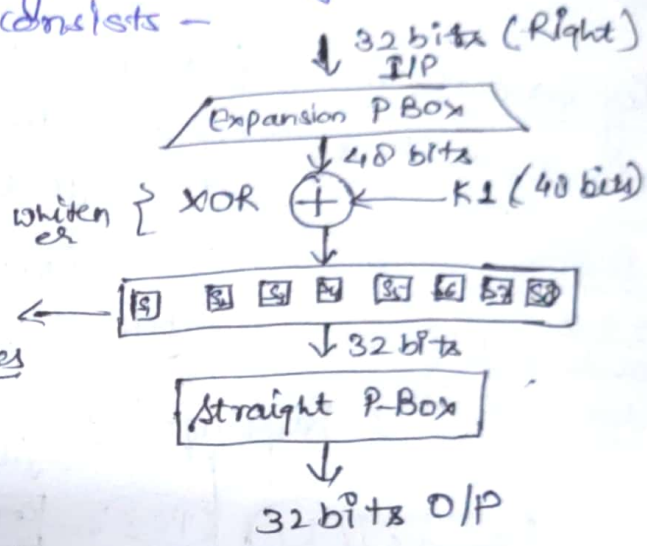
Only reverse 40 bit will be replace by 1st bit.

ROUNDS- There are 16 rounds and each round is a fiestel cipher.



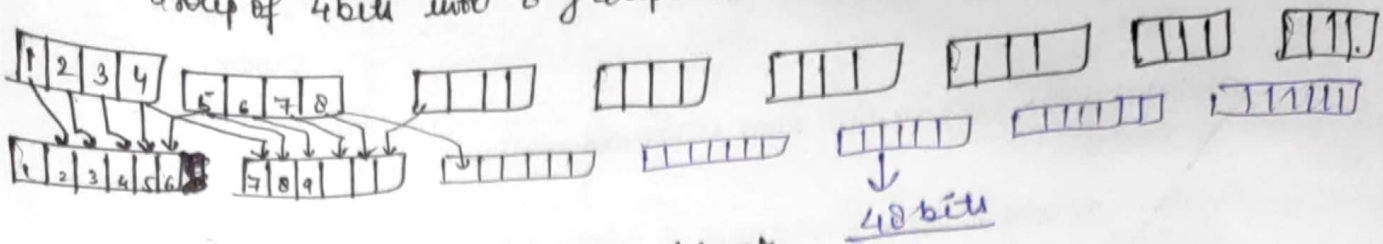
DES function - Applies 48 bit key to the rightmost 32 bits to produce 32-bit output. It consists -

1. - Expansion of P-Box
2. - Whitener
3. - Group of S-boxes
4. - Straight P Box



Expansion P box- (32 bits → 48 bits)

Group of 4 bits into 8 groups to 6 bits -



1 ← 4th bit of previous block.

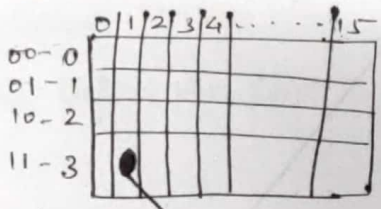
1 → 2
2 → 3
3 → 4
4 → 5

6 → 1 bit of next block

Whitener - XOR operation b/w 48 bits key & 48 bit O/P from expansion P-box.

S-boxes → 8 S boxes are used. - 6 bits I/P & 4 bits O/P

1 S-Box -



Each S-Box has different table.

bit 1 & 6 → Row selection
bit 2, 3, 4, 5 → Column selection

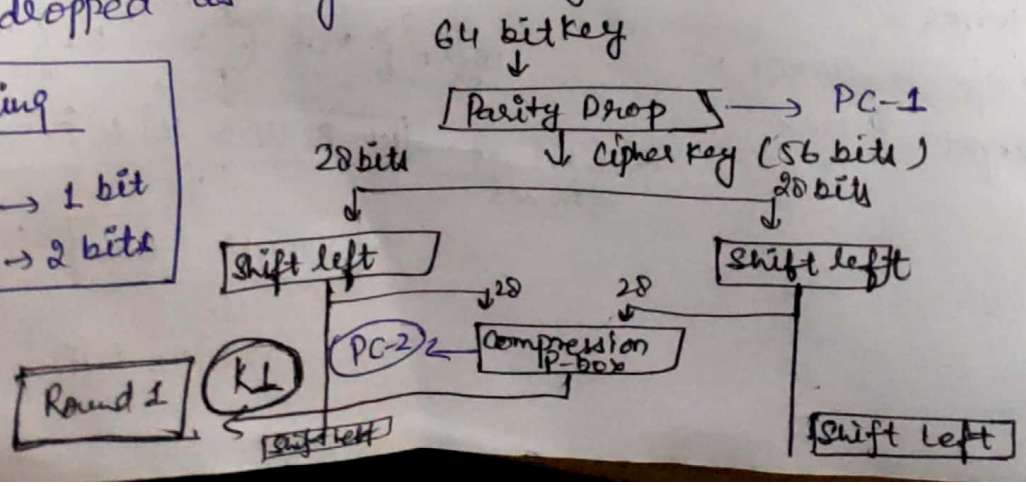
ex- 1 0 0 0 1 1 (column 1, Row 3) → Table entry (Decimal No.) → Convert to 4 bits

So 8 S-Box produce - 8×4 = 32 bits.

Straight Permutation - Again permute them by using P-Box.

Key Generation - 64 bits - each (8, 16, 24, 32, 40, 48, 56, 64) are dropped as they are parity check bits.

Shifting
1, 2, 9, 16 rounds → 1 bit
Other → 2 bits



$\boxed{PC-2}$ - In PC-2, a predefined table is there which selects 48 bits out of 56 bits.

28 - Left half - (9, 18, 22, 25 are missing)
28 - Right half - (35, 38, 43, 54 are missing).
} → 48 bits.

The Strength of DES →

★ The use of 56 bits keys →

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

- In average, only half of the keys have to be tried to break the system.
- In principle, it should take long time to break the system.
- Things are quicker with dedicated h/w.

  In 1998 - a special m/c was built for less than 250000 $ breaking DES in less than 3 days.

  In 2006 - Estimates are that a h/w costing around 20,000 $ may break DES within a day.

★ - Nature of the algorithm →

- There has always been a concern about the design of DES, especially about the design of S-boxes. S-boxes design criteria have been classified inf^n and NSA was involved in the design.
- On the other hand, changing the S-boxes slightly seems to weaken the algorithm.

Advanced Encryption Standard - (1997)

- AES is a block cipher intended to replace DES for commercial applications. It uses a 128-bits block size and a key of 128, 192, 256 bits.
- AES does not use a fiestel structure. Each full round consists of four separate functions: byte substitution, permutation, arithmetic operations over a finite field & XOR with a key.

AES cipher - The Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128, 192 or 256 bits, but limits the block length to 128 bits.

We assume a key length of 128 bits, which is likely to be the one most commonly implemented.

AES parameters →

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plain Text (words/bytes/bits)	4/16/128	4/6/128	4/16/128
Number of Rounds	10	12	14
Round key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240

↳ Symmetric key block cipher

↳ 128 bits data

↳ Stronger & faster than DES

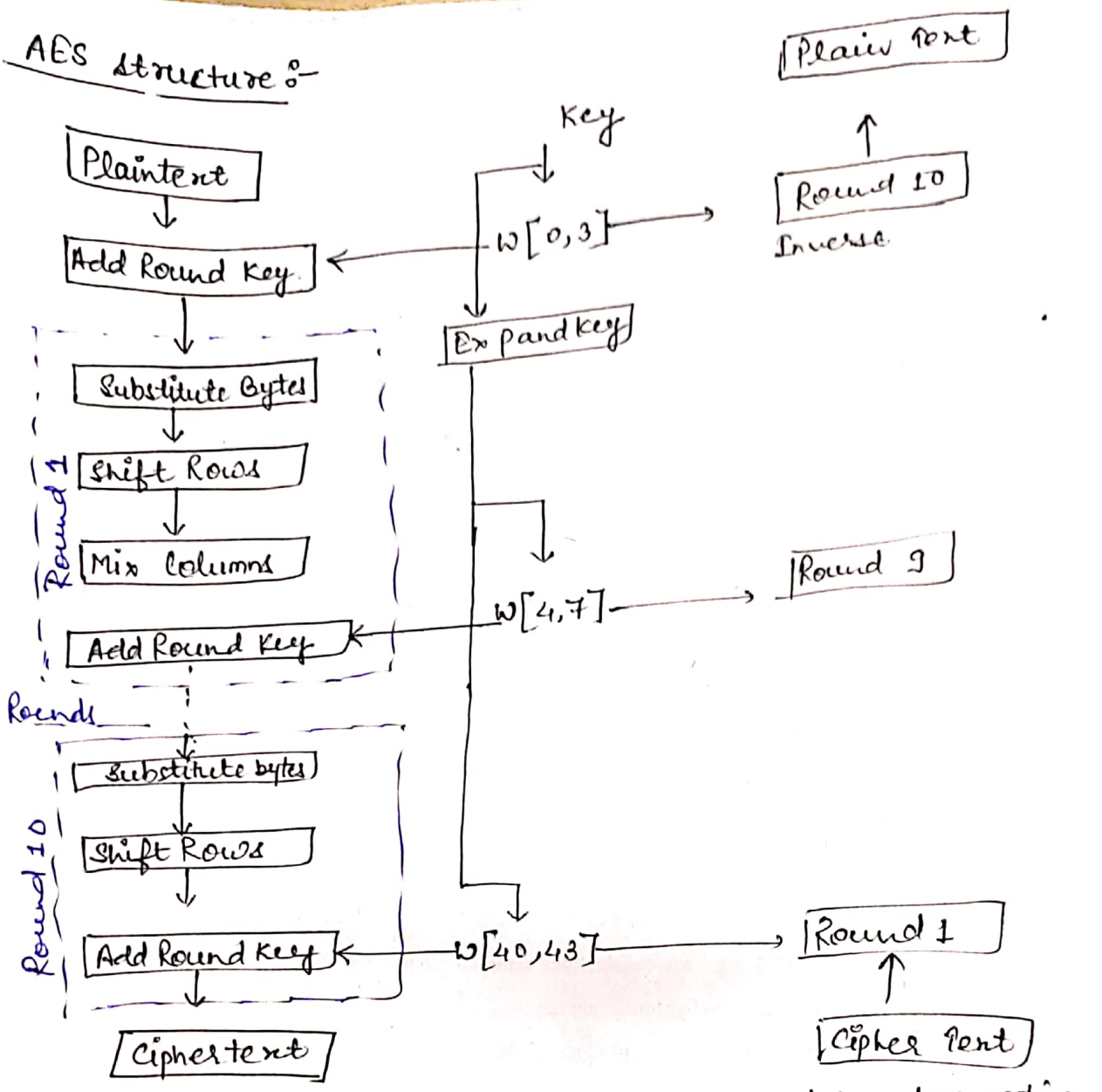
Mix columns → Special math f^n.

Sub bytes - S-Boxes of 4x4 matrix

Shift Rows - rows are left shifted [Row no. shifting]

1	0	3	2	4	3
2	1				

AES structure :-



a) Encryption

b) - decryption.

AES General Structure

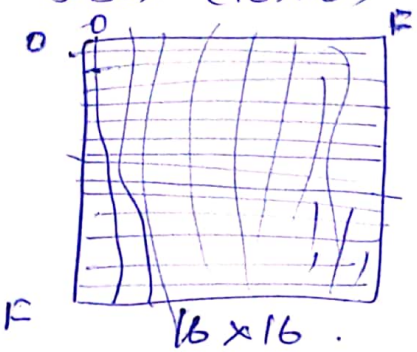
Process in AES - There are mainly two steps in AES to understand - Key Generation, Rounds.

~~Key Generation~~ -

① - Substitute Bytes transformation → AES defines a 16x16 matrix of bytes values called an S-Box, that contain a permutation of all possible 256 8 bit values.

↳ 128 bits ⇒ 16 bytes.

S-Box (16x16)

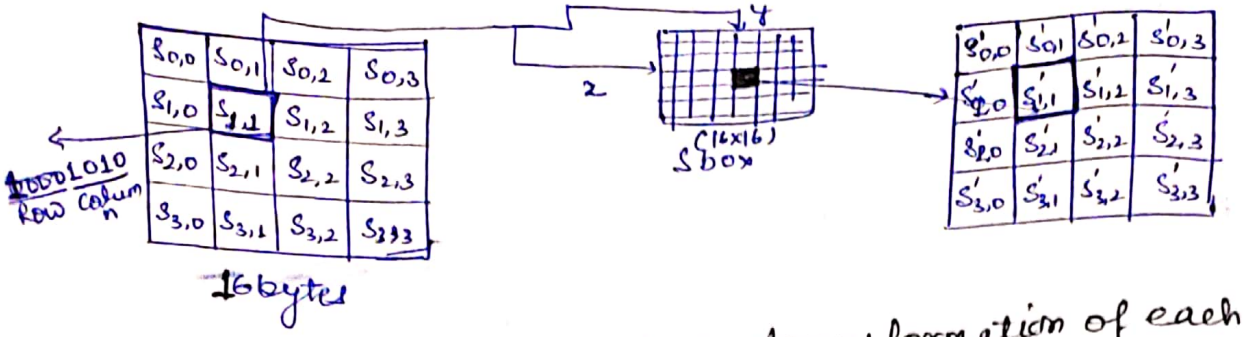


- S-Box & Inverse S-Box

Overall -

144 page No.

of n/w security & Cryptography of William Stallings



Substitute byte transformation of each byte.

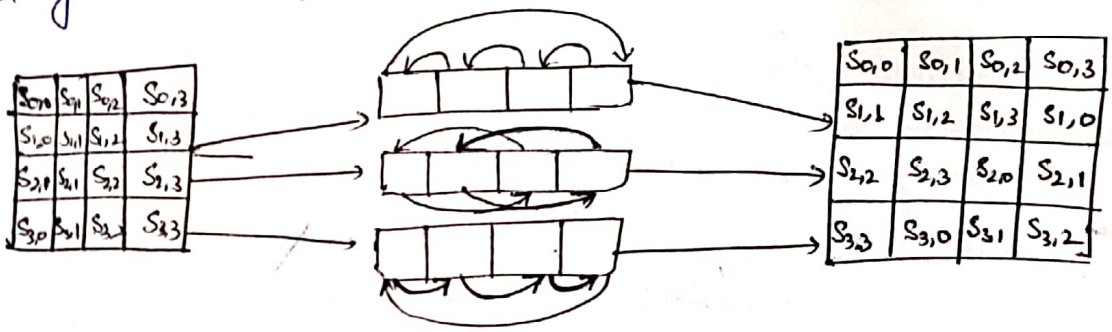
example -

EA	D4	65	85
83	45	98	96
5C	33	5D	B0
F0	2D	A0	C5

S-box →

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

Shift Rows transformation - The forward shift row transformation, The first Row of state is not altered. For the second Row, a 1 byte circular left shift is performed. For third row. 2 byte and for 3rd row 3 bytes circular shift is performed.



Shift row transformation

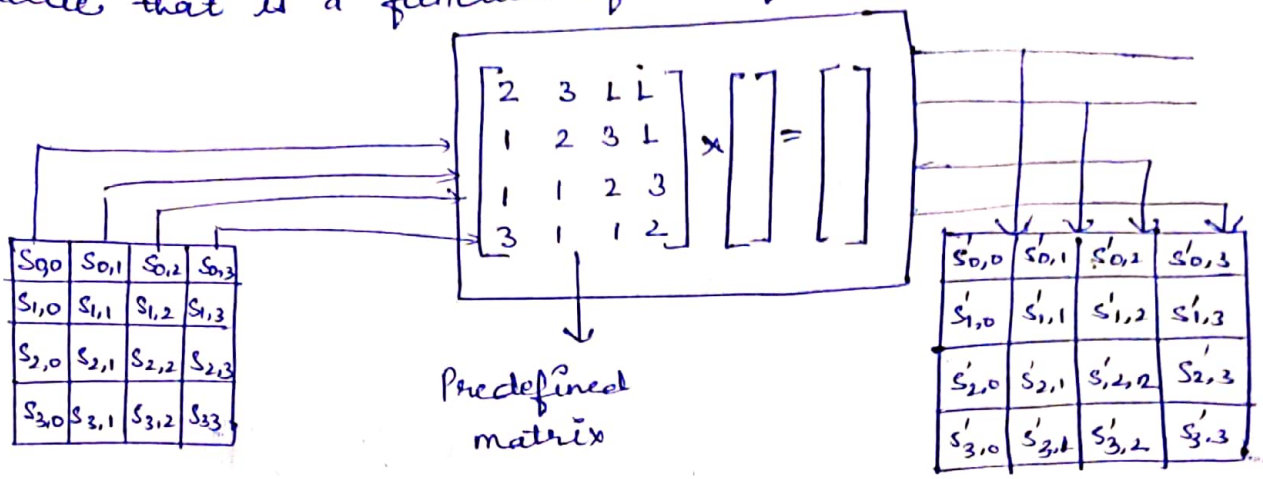
example -

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Mix Column Transformation → In this, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.



mix column :

The mixcolumn transformation on a single column – $j \langle 0 \le j \le 3 \rangle$

$$S'_{0,j} = (2 \cdot S_{0,j}) \oplus (3 \cdot S_{1,j}) \oplus S_{2,j} \oplus S_{3,j}$$

$$S'_{1,j} = S_{0,j} \oplus (2 \cdot S_{1,j}) \oplus (3 \cdot S_{2,j}) \oplus S_{3,j}$$

$$S'_{2,j} = S_{0,j} \oplus S_{1,j} \oplus (2 \cdot S_{2,j}) \oplus (3 \cdot S_{3,j})$$

$$S'_{3,j} = (3 \cdot S_{0,j}) \oplus S_{1,j} \oplus S_{2,j} \oplus (2 \cdot S_{3,j})$$

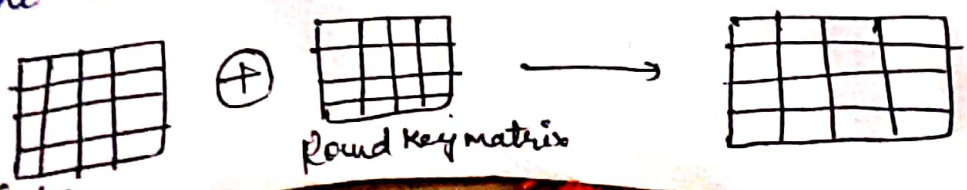
example-

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

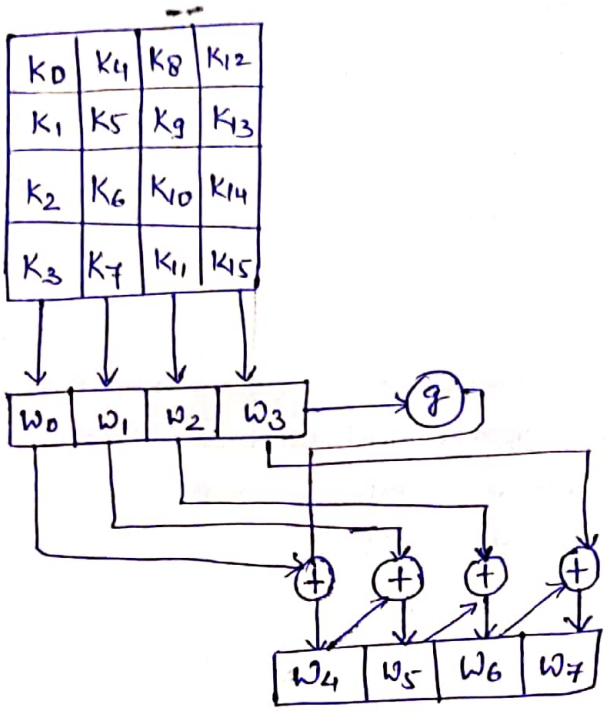
→

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

Add Round Key Transformation :→ The 128 bits of state are bitwise XORed with the 128 bits of the round key. The operation is viewed as a columnwise operation b/w the 4 bytes of a state column and one word of the round key, it can be viewed as a byte-level operation.



AES Key Expansion :- In this, algo takes as input a 4 word (16 byte) key and produces a linear array of 44 words (176 bytes). This is sufficient to provide a 4 word round key for the initial add Round key stage & each of the 10 rounds of the cipher.



'g' is a complex function consists some subfunction :-

1)- RotWord performs a one-byte circular left shift on a word. This means that an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].

2)- SubWord performs a byte substitution on each byte of its input word, using the S-box.

3)- The result of steps 1 and 2 is XORed with a round constant Rcon[j] produce a word (4 bytes).

Round constant table - Rcon[j] = (RC[j], 0, 0, 0)

	01	02	04	08	10	20	40	80	1B	36	6C	D8	AB	4D	9A
Rcon	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

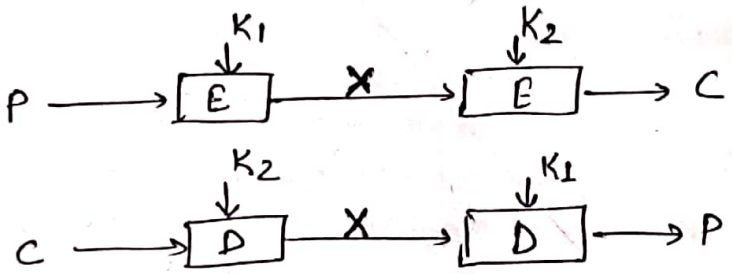
Multiple Encryption:- M.E is a technique in which an encryption algo. used multiple times.

- → Triple DES, makes use of three stages of the DES algorithm using a total of two or three distinct keys.
- → Generating a new algorithm would cost more, hence to preserve the existing investment in s/w and equipment, is to use multiple encryption with DES and multiple keys.

Double DES → In this, two encryption stages and two keys. Given a plaintext P, and two encryption keys K_1 & K_2, generated ciphertext C:

$$C = E[K_2(E(K_1, P))]$$

$$P = D[K_1(D(K_2, C))]$$



Meet in middle Attack → Thus the use of double DES results in a mapping that is not equivalent to a single DES, but there is a way to attack this scheme, one that does not depend on any particular property of DES but that will work against any block encryption cipher.

Thus meet in middle attack is the observation that, if we have-

$$C = E[K_2, (E(K_1, P))]$$

then → $$X = E(K_1, P) = D(K_2, P)$$

- first encrypt P for all 2^{56} possible values of K_1. Store these results in a table and then short the table by

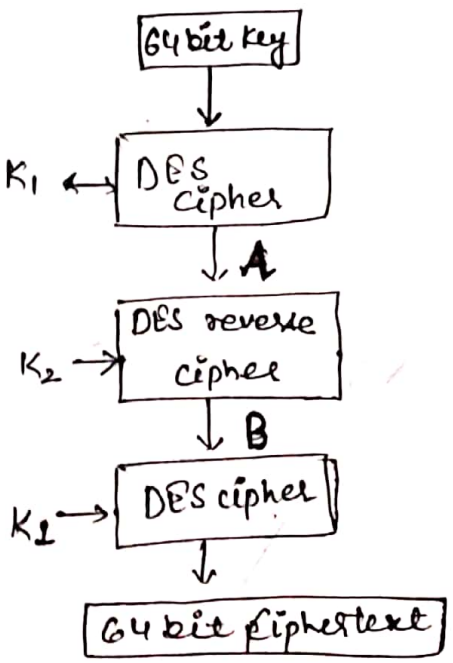
the table by the value of X. 9

- Next decrypt C using all 2^{56} possible values of K_2. check the result against the table for a match. If a match occurs, then test the two resulting keys against a new known plaintext-ciphertext pair. If the two keys produce the correct ciphertext, accept them as the correct keys.

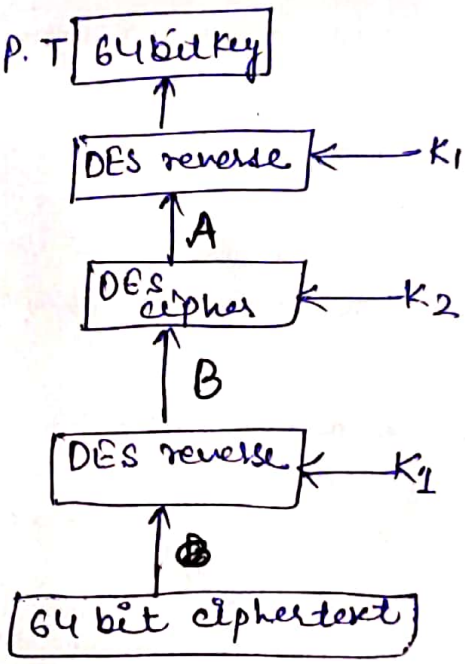
Triple DES with two keys:- An obvious counter to the meet-in-middle attack is to use three stages of encryption with three different keys.
This raises the cost of the known plaintext attack to 2^{112}, which is beyond what is practical now and far into the future.
However, it has a drawback of requiring a key length of 56x3 = 168 bits, which is some what unwidely.

Hence Tuchman proposed triple DES with two keys as EDE -

$$C = E[K_1, D(K_2, E(K_1, P))]$$



3DES 2keys Encryption



Attack - The attack may proceeds as follows:-

1)- Obtain n (P,C) pairs; This is known plaintext. Place these in a table 1 sorted on the value of P.

2)- Pick an arbitrary value 'a' for A and create a second table with entries defined in table 2. For each 2^56 possible keys $K_1 = i$, calculate the plaintext value P_i that produces a :

$$\boxed{P_i = D(i, a)}$$

P_i	C_i
—	—

Table 1 [n known P.T-C.T pairs, sorted on P]

B_j	Key_i
	—

Table 2 [Table of intermediate values & candidate Key]

For each P_i that matches an entry in table 1, create an entry in table 2 consisting of the K_1 value and the value of B that is produced for the (P, C) pair from table 1, assuming the value of K_1:

$$\boxed{B = D(i, C)}$$

At the end of this step, sort table 2 on the value of B.

3)- We now have a number of candidate values of K_1 in table 2 and are in a position to search for a value of K_2. For each of the 2^{56} possible keys $K_2 = j$, calculate the second intermediate value for our chosen value of a:

$$\boxed{B_j = D(j, a)}$$

At each step, look up B_j in table 2. If there is a match, then the corresponding key i from table 2 plus this value of j are candidates values for the unknown keys (K_1, K_2). Why? Because we have found a pair of keys (i, j) that produces a known (P, C) pair.

4)- Test each pair of keys (i, j), on a few other plaintext-ciphertext pairs. If a pair of keys produces the desired ciphertext, the task is complete. If no pair succeeds, repeat from step 1 with a new value of a.

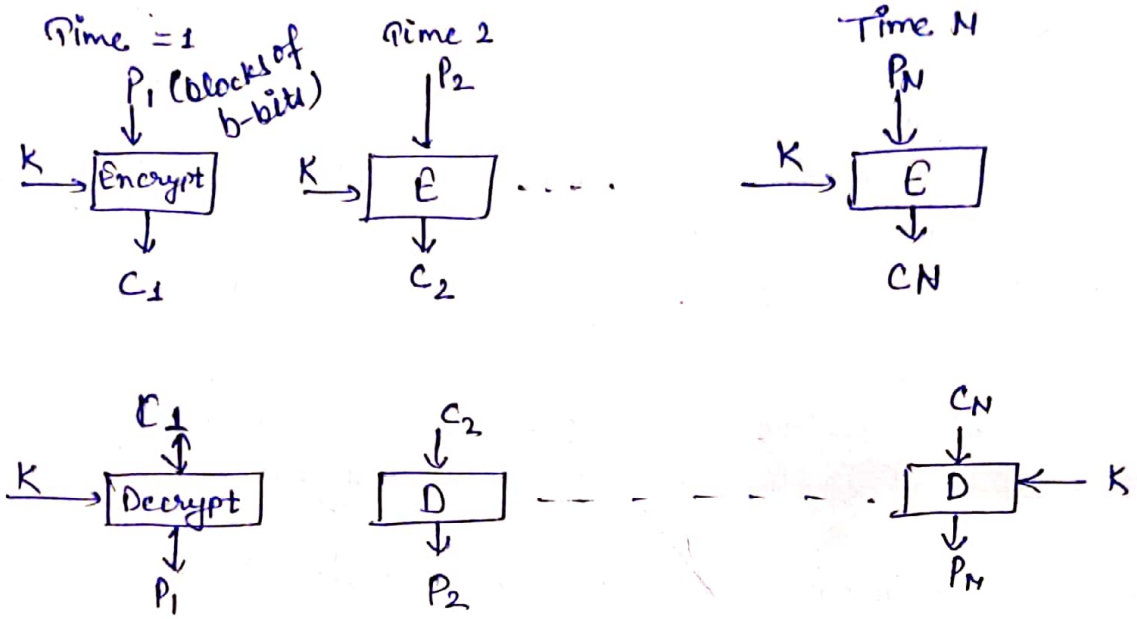
<u>Triple DES with three keys</u>- Although the attack just described appear impractical, anyone using 2-key 3DES may feel some concern. Many researchers now feel that three key 3DES is the preffered alternative. 3-keys 3DES uses 168 bits effective

$$C = E[K_3, D(K_2, E(K_1, P))]$$

A no. of Internet based applications have adopted three-key 3DES, including PGP and S/MIME.

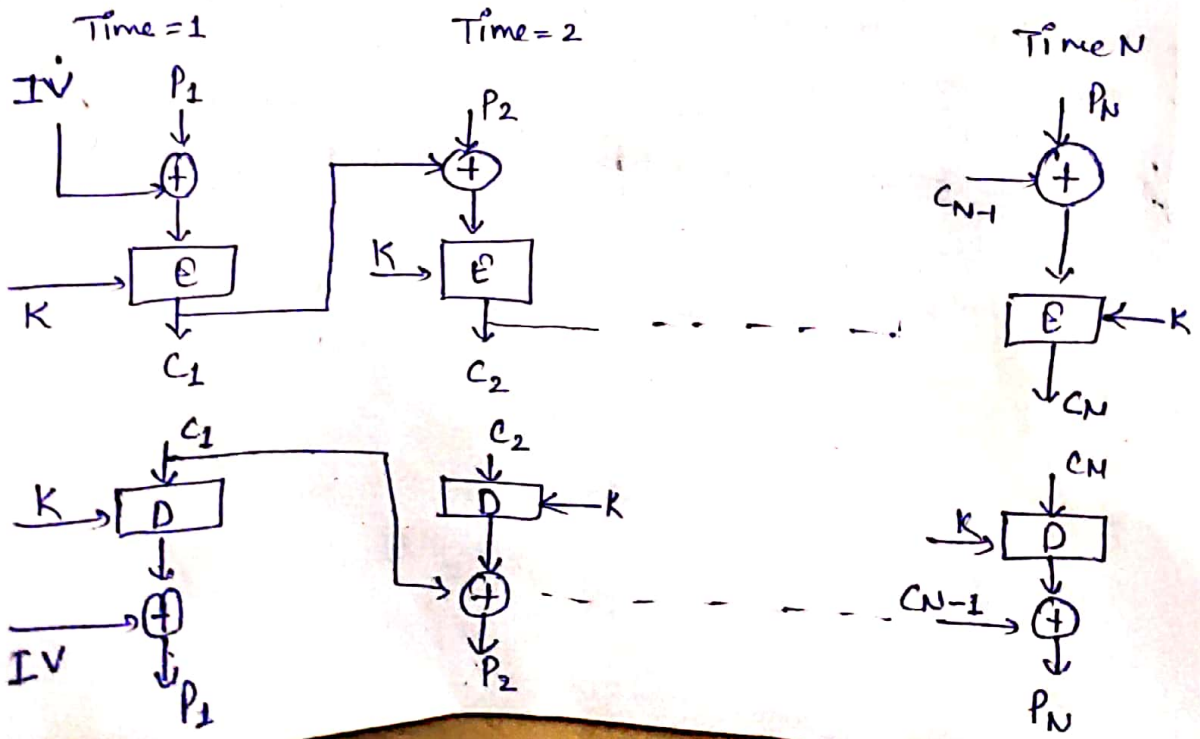
Block Cipher modes of Operation:- Mode of operation is a technique for enhancing the effect of a cryptographic algorithm, such as applying a block cipher to a sequence of data blocks or a data stream.

1)- Electronic Codebook Mode →

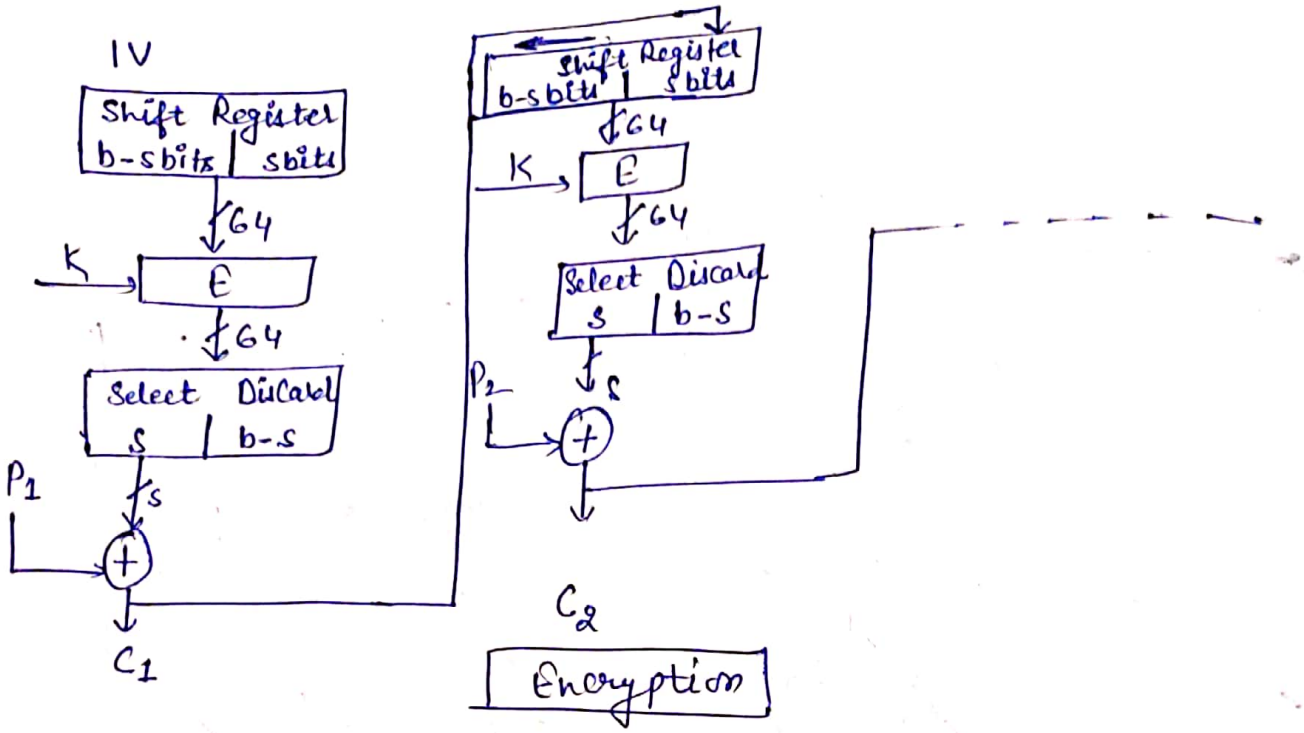


ECB method is ideal for a short amount of data, such as an encryption of Key. If you want to transmit a DES Key, then ECB is the appropriate mode of use.

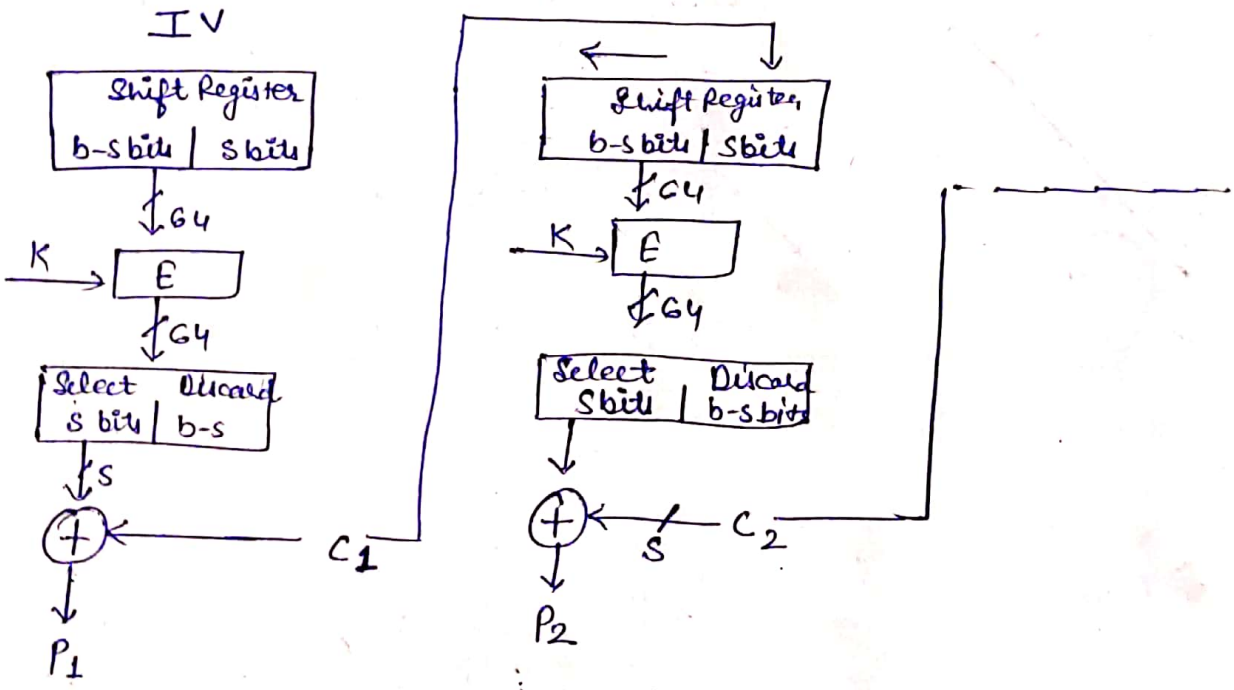
2)- Cipher Block Chaining Mode → (Initialization Vector)



3)- Cipher feedback mode →



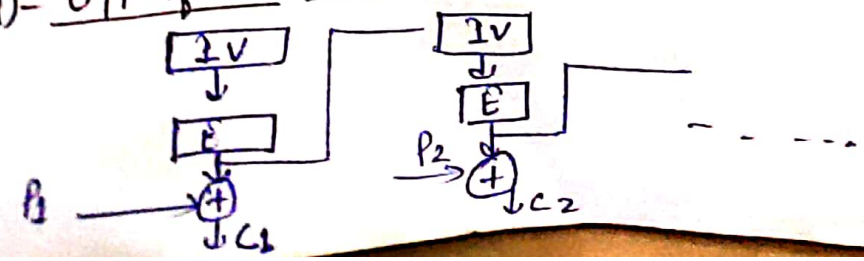
Encryption

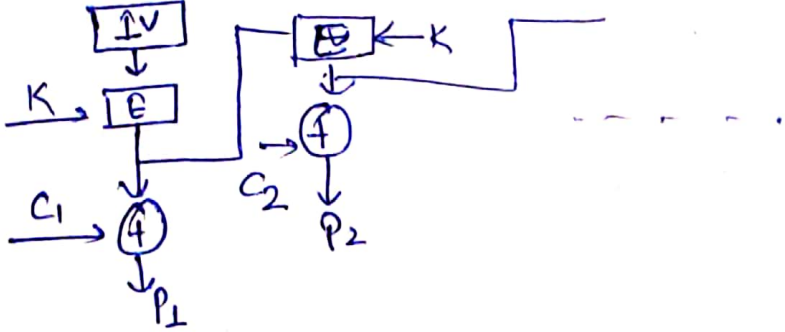


Decryption

Since, there is some data loss due to use of shift register, thus it is difficult for applying cryptanalysis.

4)- O/P feedback mode -





So here are some reasons to use Salesforce-

- **Salesforce Improves Customer Data Quality & Management** – One of the core functions of all CRMs is data management about customers. Salesforce delivers in this crucial, core service by providing companies with a host of easy-to-use options to input and manage their customer data. Adding, removing, updating and sharing customer data is a breeze with Salesforce CRM.

- **Salesforce Improves Customer Service and Support** – Another core function of any good CRM is that it will provide companies with an easy, sustainable way to improve their customer service and support options. Fundamentally, CRMs are all about improving and managing the customer-business relationship and Salesforce delivers by increasing the efficiency, automation, and quality of customer interactions.

- **Helps Acquire New Customers** – For a business to grow it must continually increase its customer base. Salesforce makes this possible by providing useful, informative reports and data about existing customers and by facilitating new sales and marketing campaigns. Salesforce even has options in place that are designed to slowly nurture a non-paying, lead relationship into a happy, satisfied, and paying customer relationship.

- **Increases Efficacy of Marketing Campaigns** – Thanks to the reports and data that Salesforce delivers about marketing campaigns, as well as the many useful marketing and tracking apps available on the AppExchange, and how easily Salesforce integrates with a host of other platforms, services, and programs, Salesforce dramatically increases the efficacy, and the ease, of marketing campaigns.

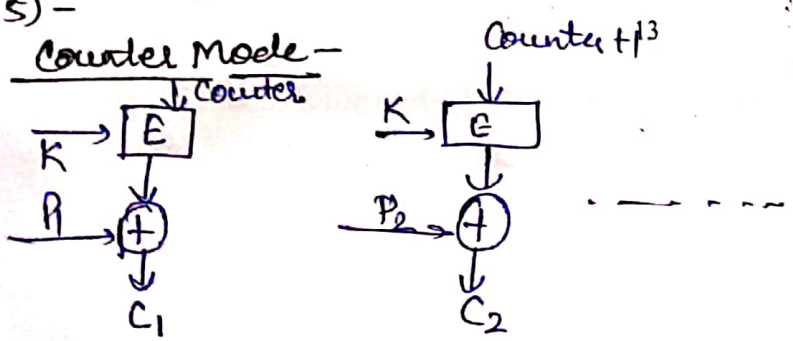
- **Enhances Cross Selling and Up-Selling Opportunities** – The traditional drawback to attempts made at cross selling and up-selling is that depending on how it is done and who the customers are, businesses run the risk of alienating existing customer relationships by appearing to be engaging in high-pressure sales that are intimidating or unwanted to customers. However, with Salesforce the data and reports delivered about customer demographics, past experiences, and other statistics, make it easy to see which customers will respond favorably to cross selling and up-selling and even appreciate the opportunity to be made aware of new goods and services.

- **Reduces Costs Associated with Sales, Services, and Marketing** – Salesforce makes it easy to track which marketing campaigns are working and which ones aren't. This means that costly, useless or near-useless campaigns can be jettisoned in favor of more lucrative approaches. By the same token the reduced effort and manpower associated with executing and tracking these campaigns will also save the company money and improve productivity.

- **Scalable As Business Size Changes** – One challenge that many companies face as they grow their business, is that techniques that worked well for a small to mid-size company are not suitable for larger businesses. Fortunately all of the services and benefits of Salesforce are

5) –

Counter Mode –



Decryption –