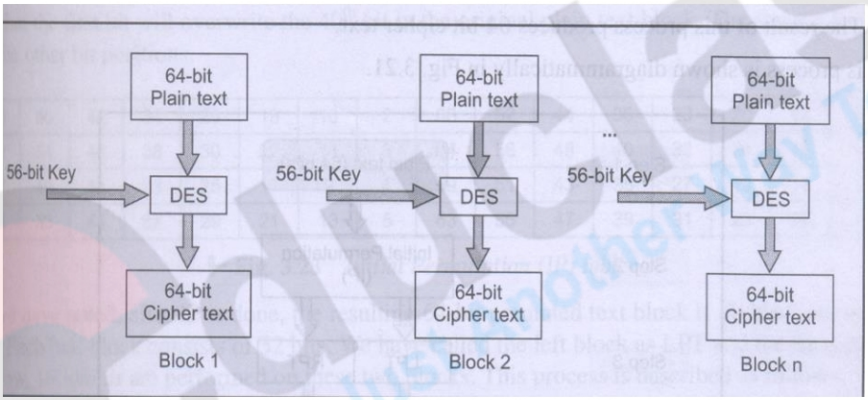
Data Encryption Standard (DES)

- most widely used block cipher in world
- encrypts 64-bit data using 56-bit key
- DES has become widely used, especially in financial applications
- DES uses the two basic techniques of cryptography

  - confusion

  - diffusion

- Diffusion is achieved through numerous permutations and confusions is achieved through the XOR operation and the S-Boxes.
- This is also called an S-P network.



- The basic process in encryption consists of:
  - An initial permutation (IP)
  - 16 rounds of a complex key dependent calculation **f**
  - A final permutation, being the inverse of IP

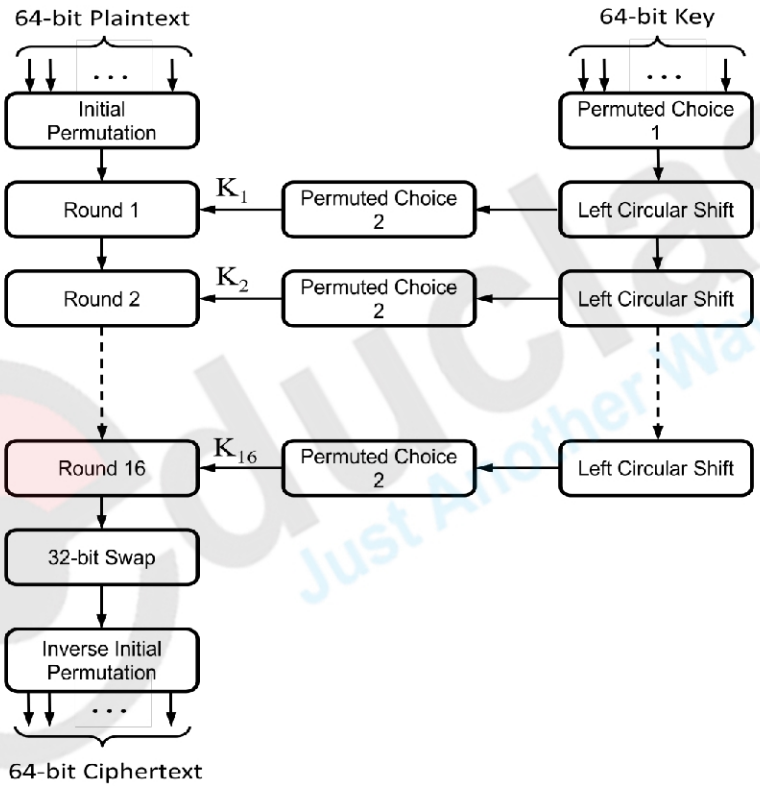
Steps in DES

1. 64 bit plain text is given to IP function
2. IP is performed on plain text
3. IP Produces two halves of permuted block

- LPT
- RPT

4. Each LPT and RPT go through 16 rounds
5. In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed
6. Produces a 64 bit cipher text

DES Encryption Algorithm

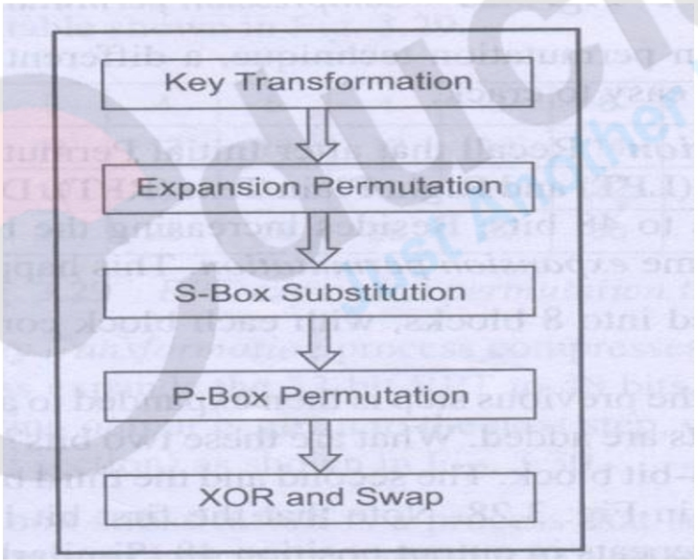


- Initial key consists of 64 bits
- Before the DES process starts every eight bit of the key is discarded
- This will result in a 56 bit key from original 64 bit key

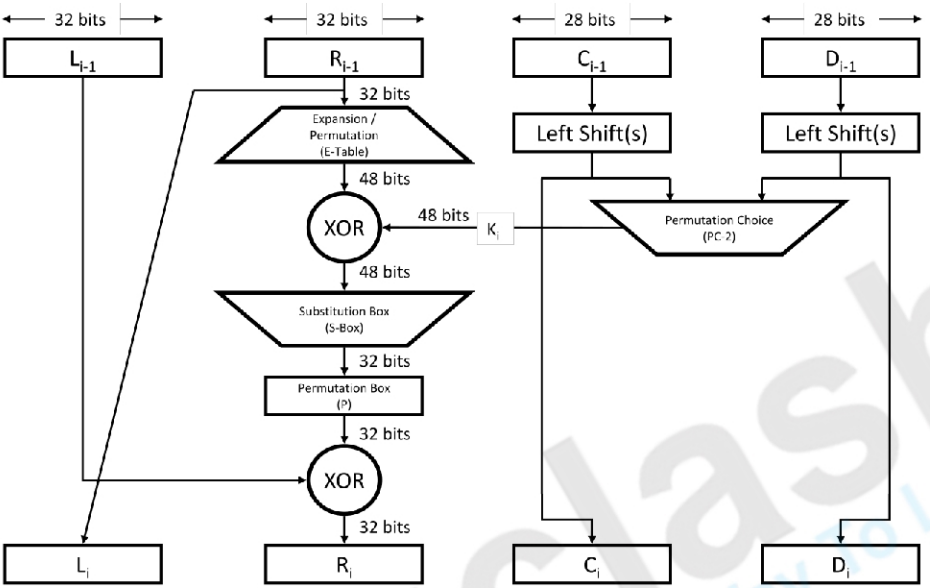
Initial Permutation

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Steps in a single round



Details of a single Round



- The 64 bit data is divided into two 32-bit L & R halves
- As for any Feistel cipher, the overall processing of each round is

$L_i = R_{i-1}$

$R_i = L_{i-1}$ xor F(R_{i-1}, K_i)

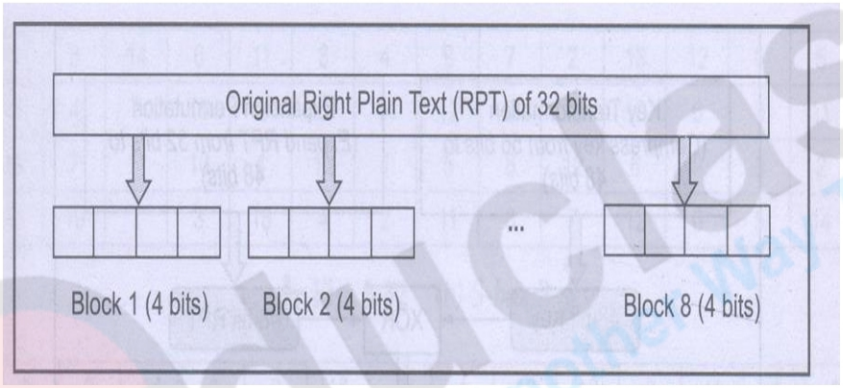
Key transformation

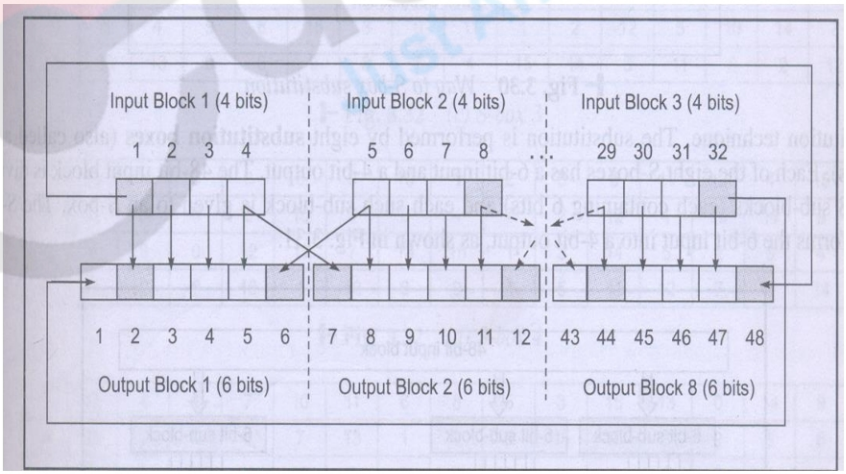
- From 56 bit key, a different 48 bit sub key is generated for all rounds
- This is done using a process called key transformation
- 28 bit data is circularly shifted 1 or 2 positions, depending on the round
- For rounds 1,2,9 or 16 , shift is done by one position

Compression permutation

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Expansion permutation

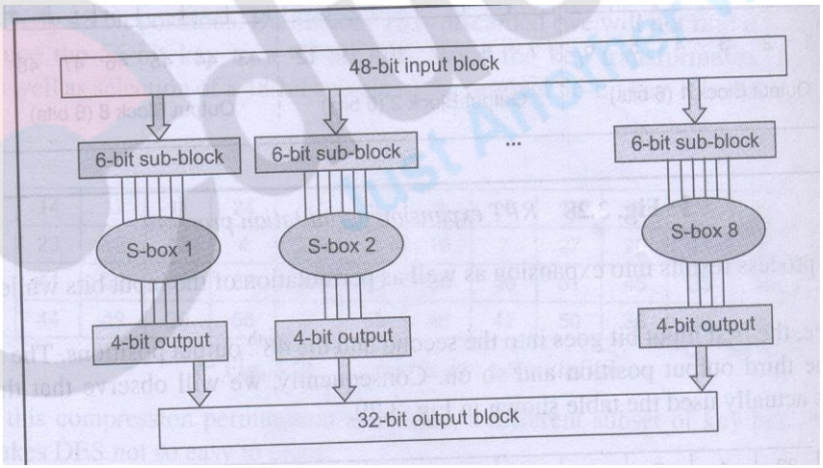


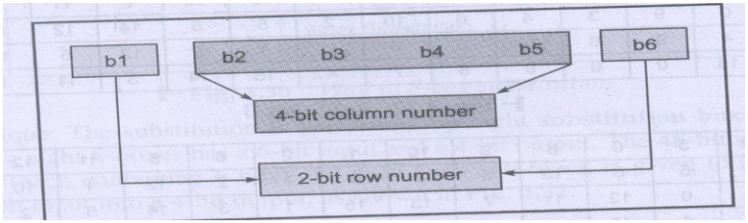


32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Substitution Boxes (S-Boxes)

- S box substitution is a process that accepts the 48 bit input from the XOR operation involving the compressed key and expanded RPT, and produces a 32 bit output using the substitution technique
- An n x m S box has n inputs and m outputs bits
- DES have eight S-boxes
- Each maps 6 x 4 bits





S-box 1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Fig. 3.32 *(b) S-box 2*

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Fig. 3.32 *(c) S-box 3*

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Fig. 3.32 *(d) S-box 4*

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Fig. 3.32 *(e) S-box 5*

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Fig. 3.32 *(f) S-box 6*

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Fig. 3.32 *(g) S-box 7*

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

P-box permutation

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

XOR and Swap

- All operations are performed on the 32 bit RPT
- LPT was untouched
- Now LPT is XORed with the output of P box
- Result of this XOR is the new right half for the next round

Old RPT will become the new LPT

Final permutation

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

DES decryption

- Same algorithm is used for decryption also
- value of tables and operations are shown in such a way that the algorithm is reversible
- Difference is in the reversal of key portions
- For decryption key is used as

  k_{16}, k_{15}, k_{14} ..... k_1

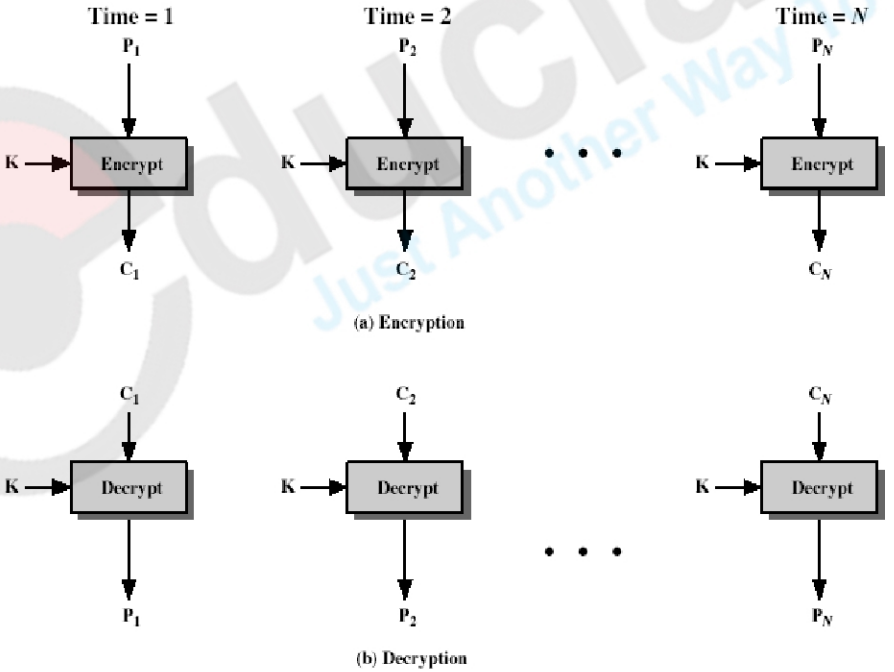
Strength of DES

- Since the inner working of DES algorithm is known to all , its strength lies in its key
- Key must be kept secret
- Since 56 bit key is used, there is 2^{56} possibilities of key

ECB

- It is the simplest mode
- The message is broken into independent 64-bit blocks
- Each block is encrypted using the same key
- For a given key , there is a unique cipher text for every 64 bit plaintext and so it is known as codebook
- If a message is longer than 64 bit, it is broken in to 64 bit blocks
- If necessary last block is padded

- ECB is ideal for short amount of data
- Most significant characteristics of ECB is that if the same 64 bit block of plaintext is used again in the message, it always produces the same cipher text
- For lengthy messages it is not secure
- It is used in secure transmission of single values
- If a message is longer than 64 bit, it is broken in to 64 bit blocks
- If necessary last block is padded
- ECB is ideal for short amount of data
- Most significant characteristics of ECB is that if the same 64 bit block of plaintext is used again in the message, it always produces the same cipher text
- For lengthy messages it is not secure
- It is used in secure transmission of single values



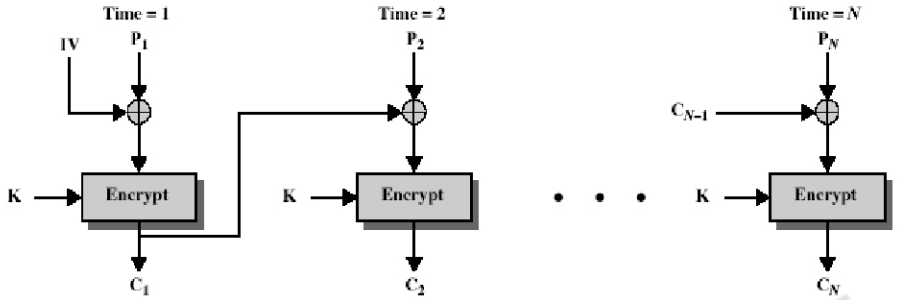
Advantages and Limitations of ECB

- repetitions in message may show in cipher text

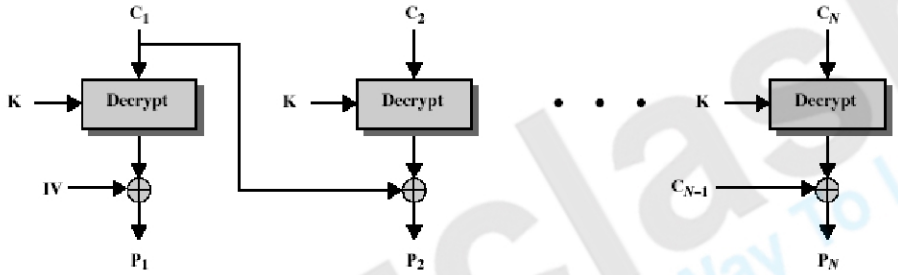
- weakness due to encrypted message blocks being independent
- main use is sending a few blocks of data

CBC

- message is broken into blocks
- but these are linked together in the encryption operation
- each previous cipher blocks is chained with current plaintext block, hence name
- The input to the encryption algorithm is the XOR of the current plaintext block and the preceding cipher text block
- The same key is used with every block
- To produce the first block of ciphertext, an initialization vector (IV) is XORed with the first block of plaintext
- On decryption, the IV is XORed with the output of decryption algorithm to recover the first block of plaintext
- IV must be known to both sender and receiver
- It is used in block oriented transmission and authentication



(a) Encryption



(b) Decryption

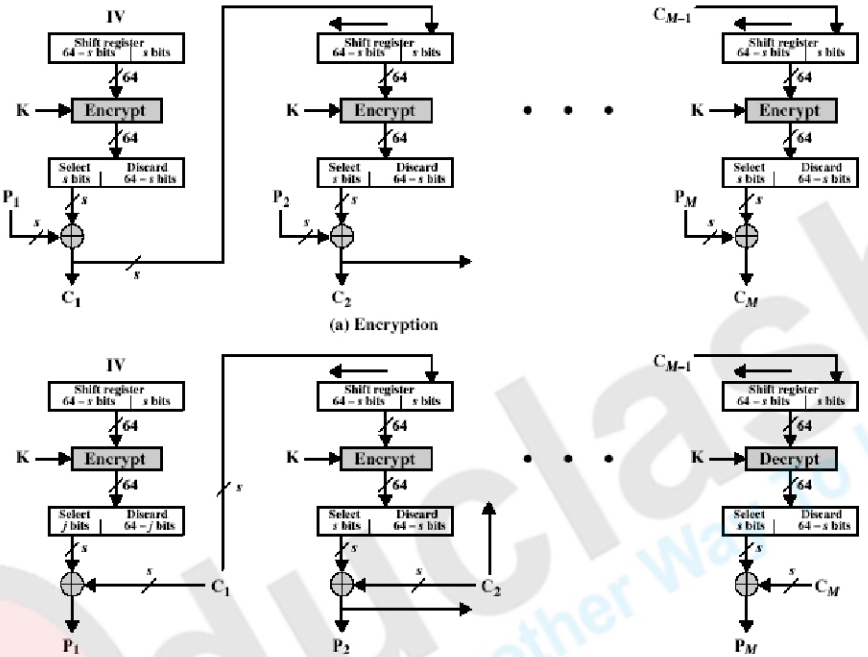
Advantages and Limitations of CBC

- each cipher text block depends on **all** message blocks
- thus a change in the message affects all cipher text blocks after the change as well as the original block
- need **Initial Value** (IV) known to sender & receiver
- If same plaintext block is repeated different cipher text blocks are produced

CFB

- message is treated as a stream of bits
- The input is processed s bits at a time
- It eliminates the need to pad the bits
- Preceding cipher text is used as the input to the encryption algorithm to produce a pseudorandom output

- This output is XORed with plaintext to produce next unit of cipher text
- It is used in stream oriented transmission and authentication



- For Encryption

Initialization vector is given as the input to the shift register

The left most s bits of the encrypted output is XORed with plain text to produce c1

For Decryption

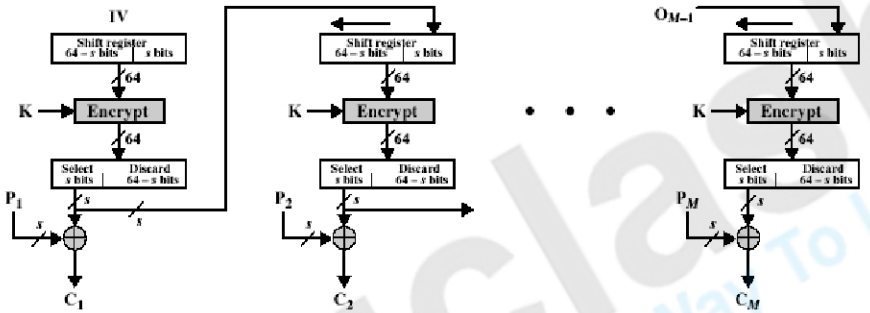
the received ciphertext is XORed with output of the encryption function to produce plaintext unit

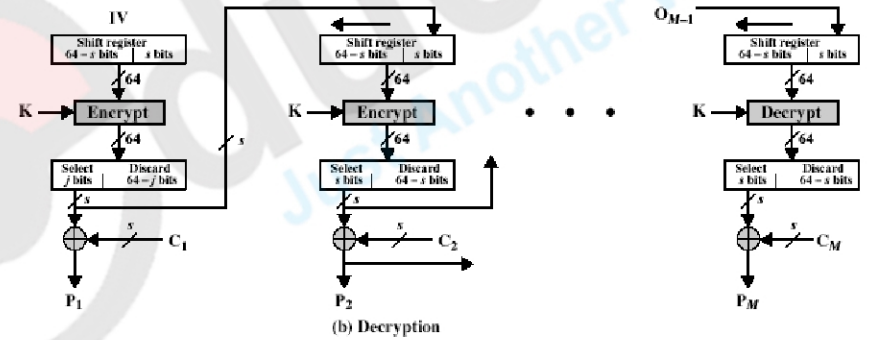
Advantages and Limitations of CFB

- appropriate when data arrives in bits/bytes
- most common stream mode
- Cipher text should be of the same length of plain text, if no transmission capacity is wasted

OFB

- It is similar in structure to that of CFB
- In this the output of the encryption function is given to the next shift register (in CFB cipher text is given)
- message is treated as a stream of bits
- feedback is independent of message
- It is used in stream oriented transmission over noisy channel such as satellite communication





Advantages and Limitations of OFB

- Advantage is that bit errors in transmission is not propagated
- If an error occurs in c1 only the recovered value of p1 is affected
- The disadvantage is that it is more vulnerable to a message stream modification attack
-

Biometrics

- Biometric devices authenticate you according to "something you are"
- It measures your physical characteristics and match them against your profile
- It provides security
- They are too expensive
- A biometric should be

  - universal
  - distinguishing
  - permanent
  - collectable
  - reliable, robust and user-friendly

- A biometric should be

  - universal
  - distinguishing
  - permanent
  - collectable
  - reliable, robust and user-friendly

1. Retinal Scanner

- This is a device that examines the tiny blood vessels in the back of your eye.
- This is distinctive as fingerprint and easier to read
- Not very common as it is expensive

2. Fingerprint readers

- Fingerprint of the user is scanned and stored.
- This has been used as a method of identification for many years
- it uses two approaches

- image based

- minutiae based

- Minutiae refer to specific points in a fingerprint, these are the small details in a fingerprint
- Finger print biometrics works by capturing the image of the fingerprint
- The image is then enhanced using various image processing techniques
- In image based , image of the finger print is taken and stored in the database
- In minutiae based technique, a graph of the individual ridge positions is drawn

3. Face Recognition

- Looking at the digitized picture of a person, a computer can measure facial dimensions and recognize people
- It check and measure the distance between various facial features such as eyes, nose and mouth

4.Iris scanner

- This maps the distinctive layout of the iris of the eye.
- Each person has some unique pattern inside the iris.
- Usually laser beams are used to identify these patterns
- It is reliable
- Iris scan can be done with a camera several feet away

5. Handprint readers

- in this the shape of the hand is measured
- They measure the dimensions of the hand such as finger length, width etc.
- Is easy and quick to measure
- They are not much accurate as finger prints.

6. Voiceprints

- It will do the frequency spectrum analysis of someone's voice and get identification.
- It is identified based on the characteristics of the sound waves of a voice such as pitch and tone.

- It can be defeated with tape recording and it may refuse to some one whose voice is changed due to illness

Behavioral

- The idea is to observe a person to ensure that he is not trying to claim to be someone else.
- It emphasis on checking that a person's behavior is not unusual

1. Signatures

It will record the signature and the actual timing of the movement that go into scribing the signature

- It is now extended by keeping the scanned copy of the signature

2. Keystroke timing

- It depends on the manner and rhythm in which an individual types characters on a keyboard.
- Several characteristics such as speed of typing, strength of keystrokes, time between two keystrokes , error percentage and frequency etc are measured.
- The recorded keystroke timing data is then processed through a unique neural algorithm