

Feistel Cipher Structure.

Feistel cipher is not a specific structure of block cipher.

It is a design model from which many different block ciphers are derived.

DES is just one example of a feistel cipher.

A cryptography system based on feistel cipher structure uses the same algorithm for both encryption and decryption.

In the feistel block cipher each block has to undergo many rounds where each round has the same function.

Function of Feistel structure

The plain text is divided in two equal halves L_0 and R_0 .

The two half of the data pass through n round of processing and then combine to produce the cipher text block.

On the right ^{half} we apply a function and in the function we will use a sub key generated from the master key.

The output of this is XORed with the left half and then the output will be swapped (one single round).

Note: L_n will have (n round) depend upon the algorithm all round will have the same structure.

Note: If any algorithm we divided the plain text in two half and apply the function on right hand side and XOR it with left hand side and the output is swapped, then that algorithm follows feistel structure.

Now,
Block size, key size, subkey generation algo no of rounds and round function.

Block size larger block size means more security.

Key size larger key size means more security (but it may decrease the processing of encryption and decryption)

No of rounds more round more secure.

Subkey generation more complex algorithm difficult for attacker to steal data.

second function more complex function
harder for the cryptanalyst to attack.

Eg $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ encoding matrix

(PRE) (PAR) (EAT) (DAN) (EGO) (LIA)

(16, 8, 5) (16, 1, 18) (5, 27, 20) (15, 27, 14) (15, 3, 15) (20, 9, 1)

$\begin{bmatrix} 5, 17, 15 \end{bmatrix} \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} -96 & 22 & 107 \end{bmatrix}$

$\begin{bmatrix} 20, 9, 17 \end{bmatrix} \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} -183 & 32 & 207 \end{bmatrix}$

decoding matrix is $A^{-1} = \frac{1}{|A|} \text{adj } A$

$$|A| = -3(4-3) + 3(0-4) - 4(0-4) \\ = 1 \neq 0 \quad A^{-1} \text{ exist}$$

$\begin{bmatrix} 16, 18, 5 \end{bmatrix} \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} -122 & 23 & 132 \end{bmatrix}$

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & -3 \\ 4 & -3 & 3 \end{bmatrix} = A^{-1}$$

$\begin{bmatrix} 16, 1, 18 \end{bmatrix} \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} -123 & 19 & 139 \end{bmatrix}$

$\begin{bmatrix} 5, 27, 20 \end{bmatrix} \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} -176 & 47 & 181 \end{bmatrix}$

$\begin{bmatrix} 15, 27, 14 \end{bmatrix} \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} -182 & 41 & 107 \end{bmatrix}$

Components of Block cipher

Modern Block cipher: normally an key substitution cipher in which the key allows only partial mapping from the possible input to the possible output

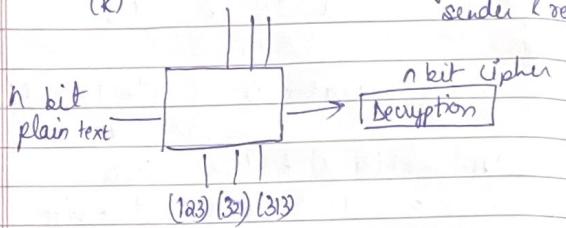
① Modern block cipher mode of combination of transposition (permutations) (P-box or S-box)

Unit of diffusion called S-box

② Substitution (confusion)
also called S-box

A symmetric key modern block cipher encrypt an n bit block of plain text or decrypt n bit of cipher text.

The encryption or decryption algorithm use n bit (will be same for both (K) sender & receiver)



Substitution and Transposition

A modern block cipher can be designed to either act as a substitution cipher or transposition cipher

Traditional cipher unlike here the symbol to be substituted or transposed bit instead of character.

Note Modern Block cipher are designed as substitution cipher.

Substitution Techniques

Caesar Cipher

Playfair cipher

Hill cipher

Caesar Cipher

$$1 \leq K \leq 25$$

- It is also called shift cipher/additive cipher.
- Each letter in the plaintext is replaced by a letter corresponding to a no of shift in the alphabet.
- It is monoalphabetic Caesar cipher
- It is one of the earliest and simplest method of encryption technique.

e.g. He used a key of 3 per communication
plain \rightarrow Meet me at zebra
cipher \rightarrow

$$\text{Encryption} \quad C = E(K, P) = (P+K) \bmod 26$$

$$\text{Decryption} \quad P = D(K, C) = (C-K) \bmod 26$$

Numerical values assigned to each letters
 a b c d e f g h i j k l m - - - x y z
 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

If the cryptanalyst attacker knows a cipher text, then he can apply brute force technique to find the plaintext by using all the possible 25 keys.

Question on Pg (19 - 22) Since it is a part of symmetric encryption since key is used for encryption & decryption

Playfair Cipher (digraph substitution cipher)

- developed by Charles in 1845
- In this we encrypt a pair of alphabets (digraphs) instead of a single alphabet
- fast to use

Key → Information

Plain Text → Attack on Sunday

| | | | | | |
|---|---|---|---|---|---|
| V | J | N | F | O | R |
| M | A | T | B | C | |
| D | E | G | H | K | |
| L | P | Q | S | U | |
| V | W | X | Y | Z | |

at te ck on Su nd ay

T B B T K U R F U L I E B W

Key → Sheep

Plain Text → Communication

| | | | | |
|---|---|---|---|---|
| S | H | E | P | A |
| B | C | D | E | G |
| V | K | L | M | N |
| O | Q | R | T | U |
| V | W | X | Y | Z |

(O N X H E N N I C A T I O N
B Q L Y N T I K X O M V I
G H)

Hill cipher

- Developed by Lester Hill in 1929
- Encrypt a group of letters called polygraph
(like in playfair cipher)

This method makes use of Maths

To encrypt:

$$c = kp \bmod 26$$

Step1- Choose a key (key Matrix must be a square matrix)

eg Key VIEW

$$\begin{bmatrix} V & I \\ E & W \end{bmatrix}$$

$$\begin{bmatrix} 21 & 8 \\ 4 & 22 \end{bmatrix}$$

eg Key = QVICKNESS

$$\begin{bmatrix} Q & V & I \\ C & K & N \\ E & S & S \end{bmatrix}$$

$$\begin{bmatrix} 16 & 20 & 8 \\ 2 & 10 & 13 \\ 4 & 18 & 18 \end{bmatrix}$$

Plain text - Attack

$$\text{Key} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

Plain text

$$\begin{bmatrix} A \\ T \end{bmatrix} \begin{bmatrix} T \\ A \end{bmatrix} \begin{bmatrix} C \\ K \end{bmatrix}$$

① $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix}$

$$\begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$$

② $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

$$\begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} H \\ F \end{bmatrix}$$

③ $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} 38 \\ 66 \end{bmatrix} \bmod 26$
 $\begin{bmatrix} 8 \\ 14 \end{bmatrix} \text{ IG}$

FKMFIO

Since the key is a 2×2 matrix plain text should be converted into vectors of length 2

For decryption

$$D = K^{-1} C \text{ Mod } 26$$

PKHMFIO

$$\text{Key} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

$$\begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix}$$

30-30

DES - Data Encryption Standard / System

Symmetric algo

Block cipher

64-bit plain text

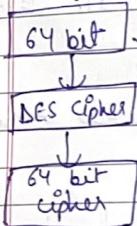
(16-rounds) Feistel structure

Key size - 64 bit Key

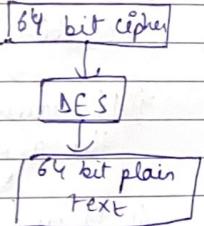
56 bit (take) \rightarrow 48 bits

sub key - 16 sub key

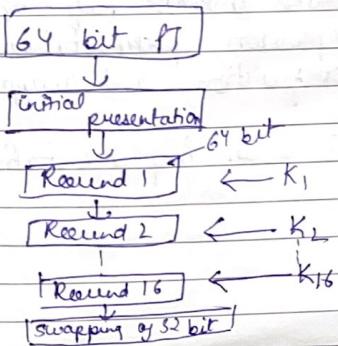
Encryption

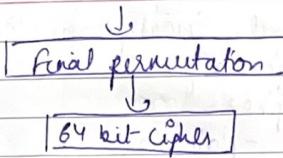


Decryption



DES algo (General Structure)

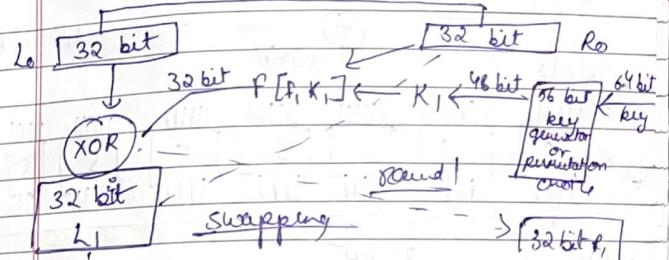




- Note:) DES i.e Data encryption standard, it is a symmetric key block cipher
- 2) Published by NIST i.e National Institute of Standard and Technology.
- 3) DES encrypt 64 bit plain Text to 64-bit cipher text
- 4) 16 round in DES provides strengthness the algorithm. . . . ?
- 5) It uses 16 round feistel structure
- 6) Each round has the same function which involves key transformation expansion, permutation, S-box, P-box, XOR function and swapping
- 7) DES is an implementation of a feistel cipher

Rounds in DES (what function will be applied in round function)

[64 bit PT]



Till swapping it is round 1

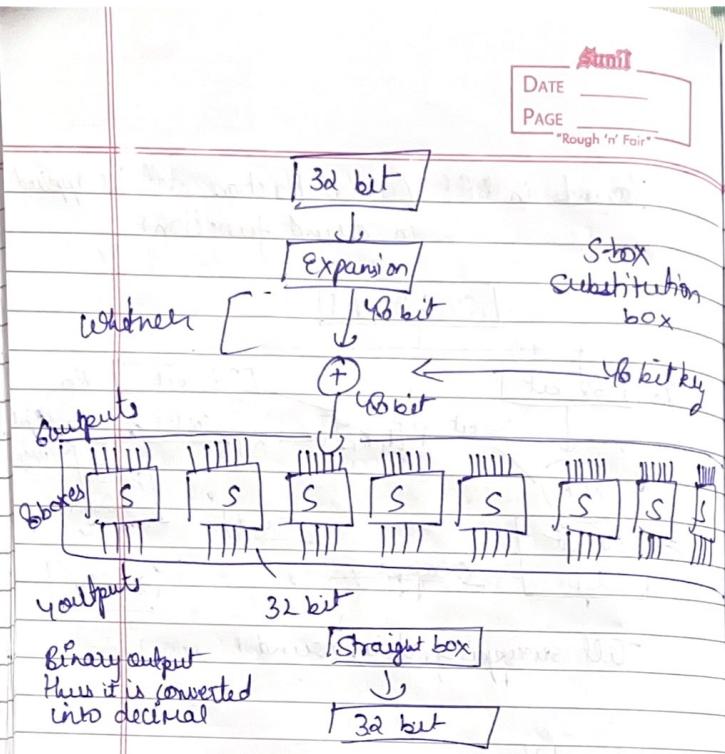
Round 16

DES Function

The heart of the cipher is the DES function (F) which is already defined in DES function or in DES round.

It apply 48 bit key to the rightmost 32 bit to produce 32 bit output

Expansion p-box
Whitener (xored), substitution
group of substitution box (S-box), straight box (P-box)



Shannon's theory of confusion & diffusion

The terms confusion and diffusion were introduced by Claude Shannon

Shannon's concern was to prevent crypt analysis, based on statistical analysis. The reason is as follows

Assume attacker has some knowledge of the statistical characteristics of the plain text (eg in a msg, the frequency distribution of the various letters may be known)

function of Expansion inside the function of DES.

Note - $4 \times 8 = 32$ bit
 $6 \times 8 = 48$ bit

| | | | |
|-------------|-------------|-------------|-------------|
| 0 0 1 1 | 0 1 1 1 | 1 1 1 0 | 1 0 0 1 1 |
| 1 0 0 1 1 0 | 1 0 1 1 1 1 | 1 1 1 1 0 0 | 0 0 0 0 1 1 |

Expansion permutation box

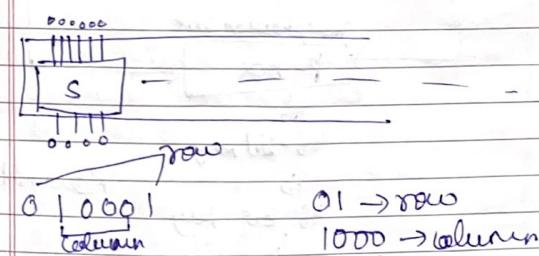
Since right input is 32 bit and secret key is a 48 bit key we must need to... expand right input to 48 bit

Note

whether

XOR operation b/w 48 bit key and 48 bit output from expansion box.

Substitution box



S-box Table 1

| | | | | | | |
|---|----|----|----|---|---|----|
| 0 | 1 | 2 | - | - | - | 15 |
| 0 | 16 | 23 | 19 | - | - | |
| 1 | 2 | 3 | 45 | - | - | |
| 2 | - | - | - | - | - | |
| 3 | - | - | - | - | - | |

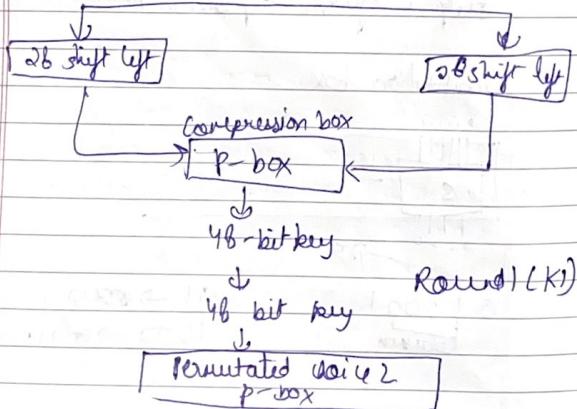
The S-boxes carries out the real mixing (confusion)

DES uses 8 S-boxes each with a six bit input and 4 bit output.

Generation of keys in DES

64 bit key
↓
64 bit

↓ parity or permuted choices 1
↓ 56 bit



Round 1 (k)

↓
48 bit key $\rightarrow k_2$

Q Find out weakness & strength of DES algo

Strengths

a) The use of 56-bit keys : 56 bit key is used in encryption, there are 2⁵⁶ possible keys. A brute force attack on such number of keys is impractical.

b) The nature of algorithm : Cryptanalyst can perform cryptanalysis by exploiting the characteristics of DES's algorithm but no one has succeeded in finding out the weakness.

Weakness

weakness has been found in the design of the cipher

a) Two chosen input to an S-box can create the same output

b) The purpose of initial & final permutation is not clear

How does block cipher work?

Design principle of block cipher
A block cipher is design on the following three principles

- ① No of rounds
- ② Function F design
- ③ Key schedule algorithm

No of rounds

This block cipher design principle indicates the overall strength of the cipher algorithms.

In short the more the no of rounds the greater is the strength of the block cipher making it more difficult to break into or decrypt the algorithm.

Function F design

Based on the Feistel structure the encryption process consist of multiple rounds of plain text processing where the input block of each round is denoted by two half i.e left half and right half.

Function F is essentially an encrypting

function that takes the encryption key (K) and (r) as the input and produce the encrypted output. It is the block cipher design principle that determines security. Function F should be designed in such a way that it cannot be substituted.

function F provide the strength to the algorithm

Key schedule algorithm

The key schedule algorithm calculates the round key

This algorithm defer according to the block scheme / cipher method.

For eg The key schedule algorithm in the DES scheme divide the 56 bit key into two half of 28 bit each then these two go into the p-box and converted into 48 bit key by compression.

Eg : DES, 2DES, 3DES, AES, IDEA, etc.

Mode of operation in Block cipher

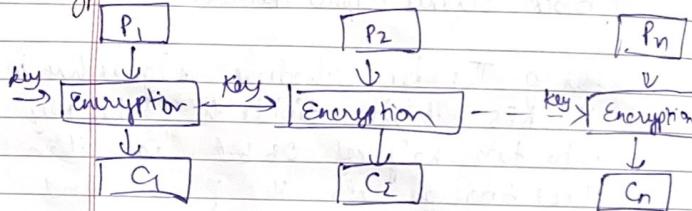
The block cipher operation mode can be divided into five parts and these modes of operation helped in providing security to the algorithm.

These modes are

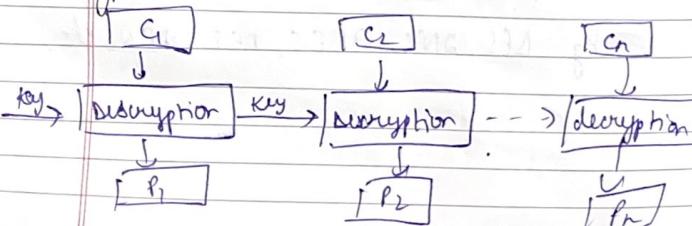
- 1) Electronic code block mode
- 2) Cipher block chaining mode
- 3) Cipher Feedback mode
- 4) Output feedback mode
- 5) Counter mode

[A] Electronic code block (ECB) mode

Encryption



Decryption

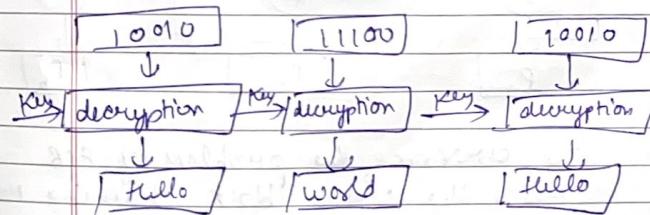
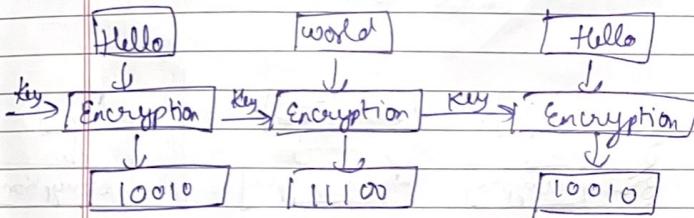


In ECB mode the given plain text message is divided into blocks of 64 bit each and each 64 bit block get encrypted.

The plain text box produced cipher text of same size and encrypt / decrypt the message using same key.

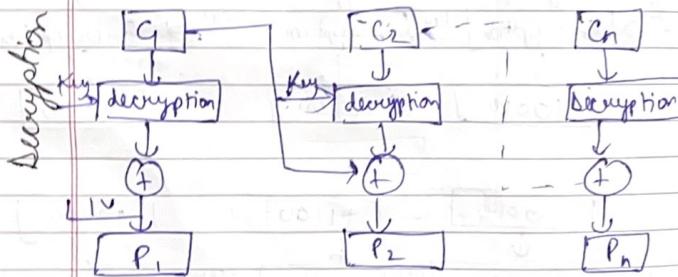
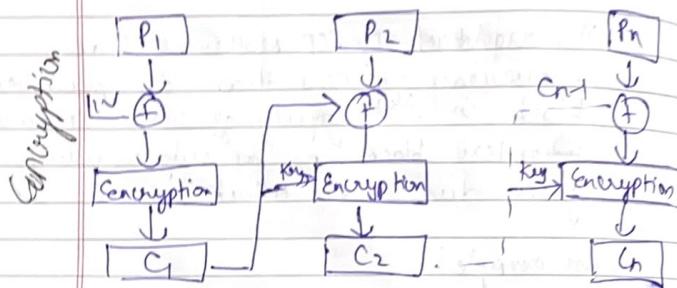
The drawback of ECB mode is that occurrence of more than one plain text block in the input generates the same cipher text block in the output which gives due to the attacker.

For example:



Mostly ECB mode used transmitting single value in secure fashion.
Eg Password

[B] Cipher Block Chaining mode (CBC)



To overcome the problem of ECB mode the cipher block chaining mode is used.

IV vector is data block of same size. Initialization vector is used in 1st encryption and 1st decryption.
IV must be known to both parties but should be unpredictable by the 3rd party.

In this most first block of plain text is XORed with an initialization vector (IV) which is then encrypted using key 'K' and produce cipher text C or block.

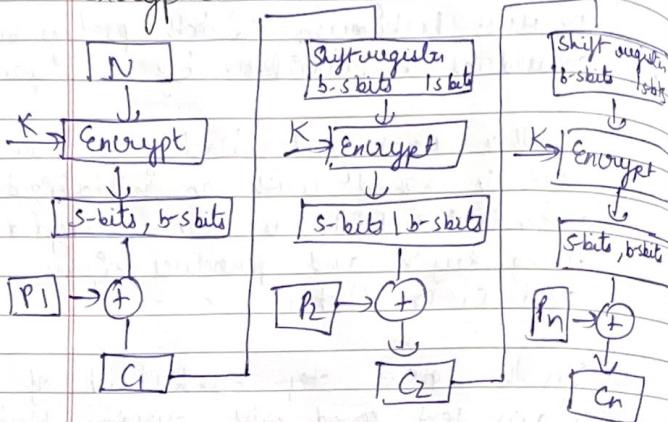
In the next step each block of plain text XORed with previous block of cipher text. The procedure is continue till all plain text block gets encrypted.

CBC mode is applicable whenever large amount of data need to be sent securely.
Eg email, FTP, web, etc.

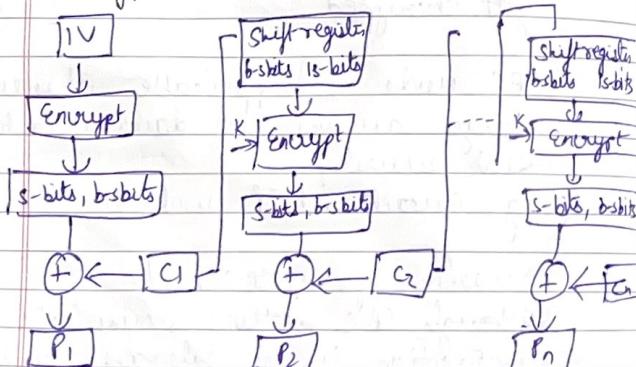
Disadvantages of CBC mode
Although CBC is more secure, its encryption is not tolerant of block losses. This is because blocks depend on their previous blocks for encryption. So if block Bi is lost, the encryption of all subsequent blocks will not be possible.

Cipher Feedback Mode (CFB)

Encryption



Decryption



CFB mode use block cipher but act as stream cipher, it means that is encrypted in smaller unit of (data) block 8 bits rather than predefined size of 64-bit

In CFB encryption process 64 bit IV is used which may keep in 64 bit shift register

The IV is encrypted and produce 8 bits encrypted IV but it is divided in two parts S(8 bits) and b-s (remaining 56 bits)

Now, the leftmost s-bit (size of s-bit) of the encrypted IV are Xored with the first s-bit of plain text p to produce the first b-bit cipher text C which is then transmitted to next step.

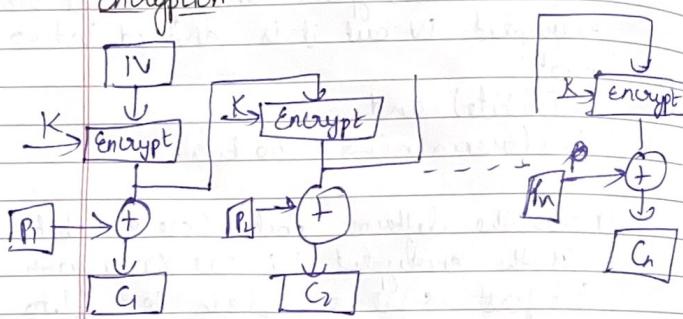
In next step content of the 64 bit shift register are shifted left by 6-s bits and c1 is placed at the eight least s-bit of the shift register and which again undergoes to encryption process

Disadvantages of CFB

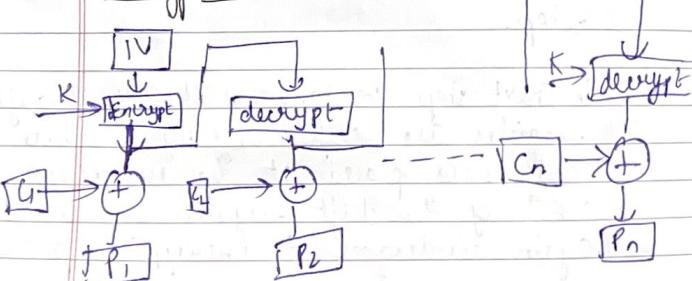
CFB mode is converting a block cipher into a type of stream cipher. This algo mostly used to key-stream generator to produce key stream.

[D] Output Feedback Mode (OFB)

Encryption



Decryption



The output feedback mode is similar to CFB mode in OFB the cipher text unit is feedback to the shift register. In case of OFB difference is that output of encryption process generating text C_i is directly placed in next stage of shift register which performs XOP operation.

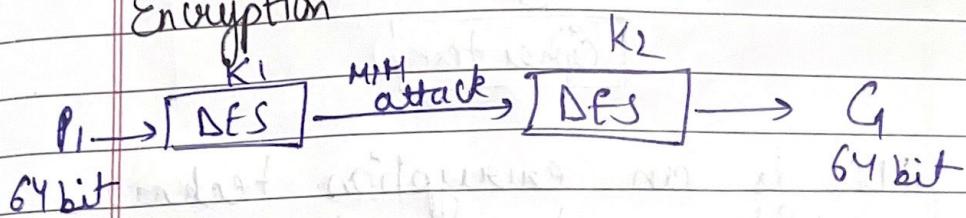
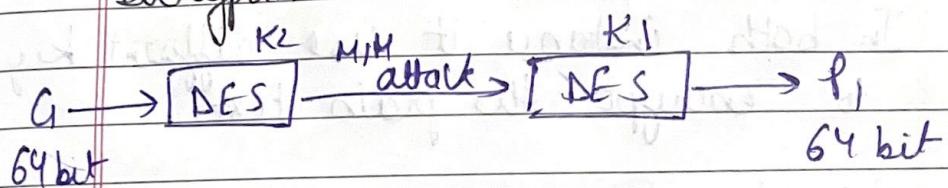
Disadvantages of CFB mode

Message blocks cannot be decrypted from any part or re-encrypted after modification.

Encryption speed is significantly slower.

Double DES

Double DES use two different keys i.e
 $56 + 56 = 112$ Keys
 (Both use 56 bit keys)

EncryptionDecryption

MIM - Meet in the middle attack.

Encryption

$$p \rightarrow E(K_1, p) \\ E(K_2, (K_1, p))$$

Decryption

$$p \leftarrow D(K_1, D(K_2, C))$$

for decryption

- First decryption using key K_2 which produce single encrypted cipher text. This 64 bit middle text is then decrypted using the key K_1 to get plain Text.

64 bit Plain Text



(X)

DES Cipher



64 bit Middle Text



DES Cipher



Cipher Text

Rb (K₂)
but

2DES is an encryption technique which use two instance of DES on same plain text.

In both instance it use different key to encrypt the plain text.

Both keys are required at the time of decryption. The 64 bit plain text goes into first DES instance which then converted into a 64 bit middle text using the first key i.e K₁ and then it goes into second DES instance which gives 64 bit cipher text by using second key i.e K₂.

However double DES uses 112 bit key but give security level by 2^{56} not 2^{112} and this is because of Meet in the middle attack (MIM) attack which can be used to break through 2DES.

Amit
DATE _____
PAGE _____
"Rough 'n' Fair"

Amit
DATE _____
PAGE _____
"Rough 'n' Fair"

As we know DES use 56 bit key to encrypt ~~any~~ any plain text which can be easily cracked by using modern technology to prevent this from happening double DES and 3DES were introduced which are much more secure than the original DES because it uses 112 and 168 bit key. 3DES and 3DES offer much security than DES.

MIM (Meet in the middle attack)

This attack involves encryption from one end and decryption from the other end and then matching the result in the middle.

This attack requires some plain text and cipher text pair.

Let us assume plain text (P) and cipher text (C), this attack proceeds as follow:

- Encrypt P for all 2^56 possible values of K₁ and store the result in a table and sort it.
- Now decrypt C using 2^{56} possible values of K₂. Now check the table for a match.
- When there is a match we have located a possible correct pairs of key.

Some pairs of PT

| PT | CT | match pair | CT | PT |
|----------------|-----|------------------------------------|-----|-----|
| K ₁ | ABC | X42 | X42 | ABC |
| | CDE | AZY | ZWO | CAC |
| | | | | |
| | | (K ₁ , K ₂) | | |

Some pairs of CT

3DES (Triple DES)

3DES is a type of computerised cryptography where block cipher algorithm applied three time to each data block.

The key size is increased in 3DES to ensure additional security through encryption capabilities.

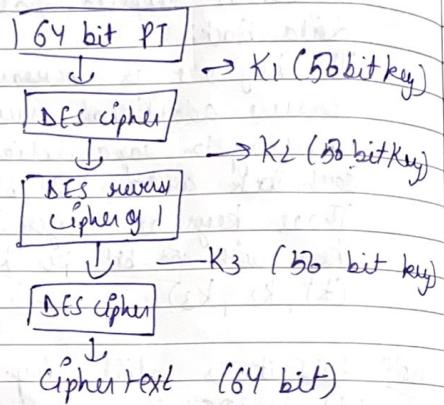
Each block contains 64 bit of data. Three keys are referred to as bundle key with 56 bit per key (K₁, K₂, K₃)

Note DES it is still imp to learn about what 3DES is and how it work. Triple DES was developed as a more secure ~~after~~ alternative because of DES small key length. In 3DES, the algo is run through three times with three key. However it is only considered secure if three separate keys are used.

3DES was one of the most commonly used encryption techniques/scheme before the rise of AES.

Some example of its implementation of 3DES includes Microsoft Office, Firefox etc.

But now many of these platforms no longer use 3DES because there are better alternatives.



- Q Explain purpose of IV vector
- Q Explain drawback of 2DES
- Q Explain working of conventional Encryption Method with the help of diagram
- Q Define cryptanalysis with its types
- Q Define cryptography & cryptosystem

AES (Advance Encryption System)

Advance encryption standard is a symmetric key cryptography algorithm published by NIST.

The algorithm replacement of DES. AES work on block cipher technique size of plain text and cipher text must be same.

In AES, the data length (plain text length) of 128, 192, 256 bit and supporting three different keys length 128 bit, 192 bit, 256 bit respectively.

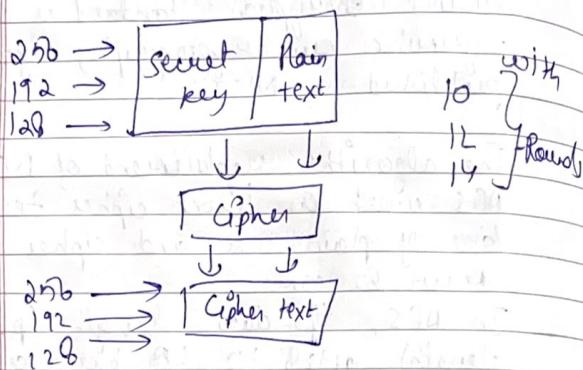
AES consist of multiple rounds of processing different keys bits like 10, 12, 14 respectively.

| PT | KL | rounds |
|-----|-----|--------|
| 128 | 128 | 10 |
| 192 | 192 | 12 |
| 256 | 256 | 14 |

Characteristics

- AES has key of three length 128, 192, 256
- It is flexible and has implementation of software and hardware

Block diagram



Characteristics

It provides high security and can prevent from many attacks.

It doesn't have any copyrights so it can be easily used globally (anywhere).

It consists of 10 rounds of processing for 128 bit key, 12 rounds for 192 bit key and 14 rounds for 256 bit key.

Example

When you store personal info on a website, facebook, twitter, etc and even when your visa or bank card

to make a process AES algo perform or provide security in everywhere

Online govt-sites, passport application, driving license, etc

Plaintext - "AES is used"

Plain text (128 bit) convert into 4×4 Matrix of bytes

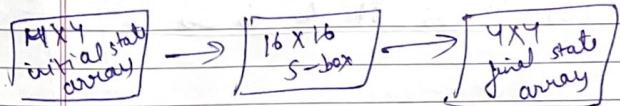
\therefore the first byte of a 128 bit input block occupy first column in the 4×4 matrix of bytes. The next 4 bytes occupy the second column and so on.

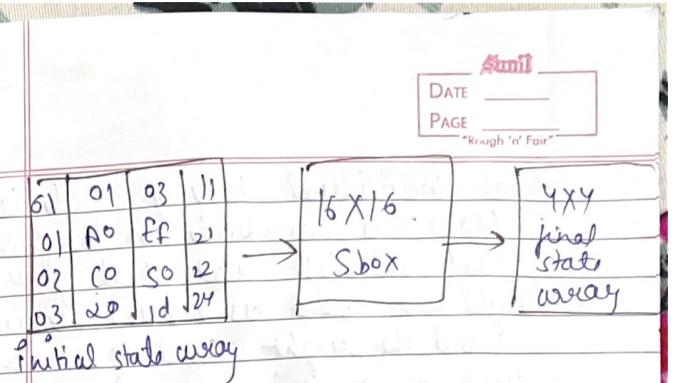
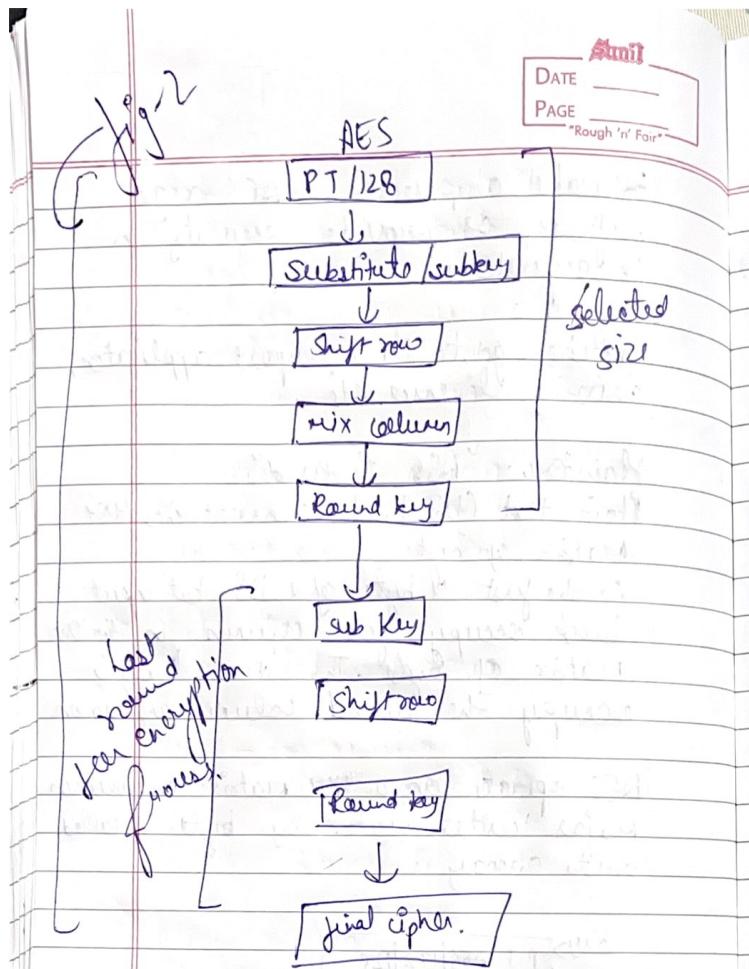
AES operate on a 4×4 matrix or columns major order matrix of bytes is called state array

Key → PT 256/192/128

↓
| Round 1 |
|
| Round 10 |

fig-1





Structure of overall structure of DES encryption process shown in fig-2

for encryption each round consists of the following 4-steps and these steps also called AES transformation system (functions)

1) Substitute 1 sub byte

AES defines a 16×16 matrix of byte values called an S-box that contains a permutation of all possible 256 8 bit values.

Similarly, for 192 and 128

No change.

Diagram illustrating the state transition graph for a 4x4 final state array. The graph has four states: O, A, B, and F.

Graph Structure:

- States: O, A, B, F
- Transitions:
 - O to A: labeled "sbox" (16x16, flatbox)
 - O to B: labeled "AB-->"
 - A to B: labeled "EF"
 - B to F: labeled "CD", "96", "12", "07"
 - B to A: labeled "EF", "05", "H1", "81"
 - F to B: labeled "CD", "96", "12", "07"
 - F to A: labeled "AI", "C1", "22", "11"

Final State Array:

| | 1A | 12 | AE | 23 |
|----------------|----|----|----|----|
| K ₁ | | | | |
| K ₂ | EF | 05 | H1 | 81 |
| R ₃ | CD | 96 | 12 | 07 |
| R ₄ | AI | C1 | 22 | 11 |

Final state array: 4x4

Each individual byte of state is mapped to a new byte in the following way. The left most 4 bit of the byte are used as a new value and the right most 4 bit are used as a column value.

The row and column values serve as index to the S-box to select a unique 8 bit output value.

2) Shift Row

It is called shift row

Rules

Row 1 - no shifting

Row 2 - 1 byte left shift

Row 3 - 2 byte left shift

Row 4 - 3 byte left shift

3) Mix Column

It operates on each column individually. Each byte of a column is mapped to a new value that is a function of all 4 bytes in that column.

Initial state array

| | | | |
|----|----|----|----|
| 01 | 01 | 03 | 11 |
| A1 | A0 | EF | 21 |
| 02 | C0 | 50 | 23 |
| 03 | 2d | 1d | 24 |

Mixed row matrix

| | | | |
|----|----|----|----|
| TA | 12 | AF | 25 |
| EP | 11 | A1 | 91 |
| 01 | 05 | 12 | 32 |
| F6 | 21 | 22 | 11 |

| P1 | P2 | P3 | P4 |
|---|--|--|--|
| $f_1(b) = XA1 + 01 \times EF + 03 \times 01 + 11 \times FG$ | $f_2(A) = XI2 + A0 \times II + EFX05 + 21 \times 21$ | $f_3(0) = 02 \times AF + C0 \times A1 + 50 \times 12 + 23 \times 22$ | $f_4(03 \times 23 + 2d \times 81 + 1d \times 37 + 24 \times 11)$ |

4×4 Matrix

4) Add Round Key

In the forward add round key transformation called add round key, the 128 bit of state array bit are xored with the 128 bit of the round key

In this column wise operation blur the 4 bytes of a state column and one word of the round key, it can be viewed as a wide level operations

D) Comparison b/w DES vs AES