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 feistal cipher structure ~~ad~~ use the same algorithm for both encryption and decryption.

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

Function of Feistal 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 ~~data~~ 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: We 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 will left hand side and the output is swapped. Then that algorithm follow feistal 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.

round function more complex function harder for the crypt analyser to attack.

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

(PRE) (PAR) (E27t) (027N) (EGO) (LIA)

[16,8,5] [16,1,18] (5,27,20) (15,27,14) [5,7,15] (20,9,1)

[16,8,5] $\begin{bmatrix} -3 & -3 & -4 \\ 6 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-122 23 132]

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

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

[15,27,14] $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-182 41 191]

[5,17,15] $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-96 22 101]

[20,9,1] $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-183 32 203]

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

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

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

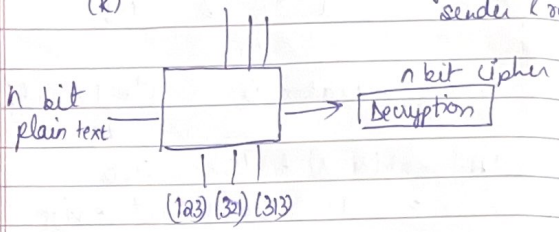
Components of Block ciphes
Modern Block cipher normally are key substitution cipher in which the key allow only partial mapping from the possible input to the possible output

① Modern Block cipher made of combination of transposition (permutations) (pbox or dbox) unit of diffusion called D-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 (K) (will be same for both sender & receiver)



Substitution and Transposition
A modern block cipher can be design 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 Technique
Ceaser Cipher
Playfair cipher
Hill Cipher

Ceaser 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 shifts in the alphabet.
- It is monoalphabetic ceaser cipher
- It is one of the earliest and simplest method of encryption technique.

Eg He used a key of 3 for communication
plain → Meet Me | Zebra
Cipher →

Encryption $C = E(K, P) = (P + K) \bmod 26$ (message)

Decryption $P = D(K, C) = (C - K) \bmod 26$ (cipher text)

Numerical values assigned to each letters

a	b	c	d	- - -	x	y	z
0	1	2	3	- - -	23	24	25

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

Question on Pg. (19 - 22) Since it is a part of symmetric encryption same key is used for encrypt & decrypt

Sunil
DATE
PAGE
"Rough 'n' Fair"

Playfair cipher (digraph substitution cipher) created

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

Key → Sheep
Plain text → Communication

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

CO MX MU NI CA TI ON
BQ LY NT IK GH OM VI

Sunil
DATE
PAGE
"Rough 'n' Fair"

Key → Information
Plain Text → Attack on Sunday

I/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 ta ck on Su nd ay

TB BT KU RF UL IE BW

Sunil
DATE
PAGE
"Rough 'n' Fair"

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 = QUICKNESS

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

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

Sunil
DATE
PAGE
"Rough 'n' Fair"

Plain text - Attack

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

Since the key is a 2x2 matrix plain text should be converted into vectors of length 2

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

$\begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 \quad \begin{bmatrix} M \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$

③ $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26$

$\begin{bmatrix} 8 \\ 14 \end{bmatrix}$ I O

FKMFIO

For decryption

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

FKMFIO

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

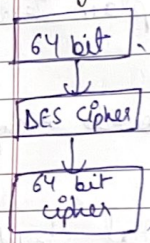
$$\begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$$

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

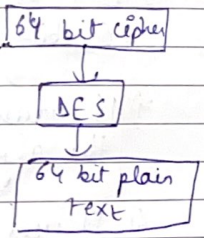
30 - 30

DES - Data Encryption Standard System
Symmetric algo
Block cipher
64-bit - plain text
(16- rounds) Fiestal structure
Key size - 64 bit Key
56 bit (take) → 48 bits
↓
sub key - 16 sub key

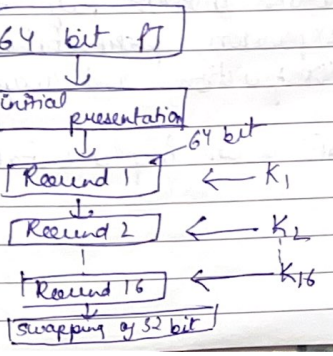
Encryption



Decryption



DES algo (General Structure)



Sunil
DATE
PAGE
"Rough 'n' Fair"

↓

Final permutation

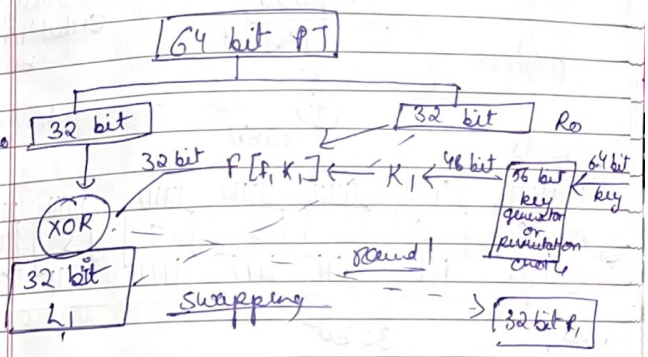
↓

64 bit cipher

Note:
1) DES i.e Data encryption standard, it is a symmetric key block ciphes
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 provide strengthness the algorithm...!
6) It uses 16 round feistal structure
7) Each round has the same function which involve key transformation expension, permutation, s-box, p-box XOR function and swapping
5) DES is an implementation of a feistal cipher

Sunil
DATE
PAGE
"Rough 'n' Fair"

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



Till swapping it is round 1

Round 16

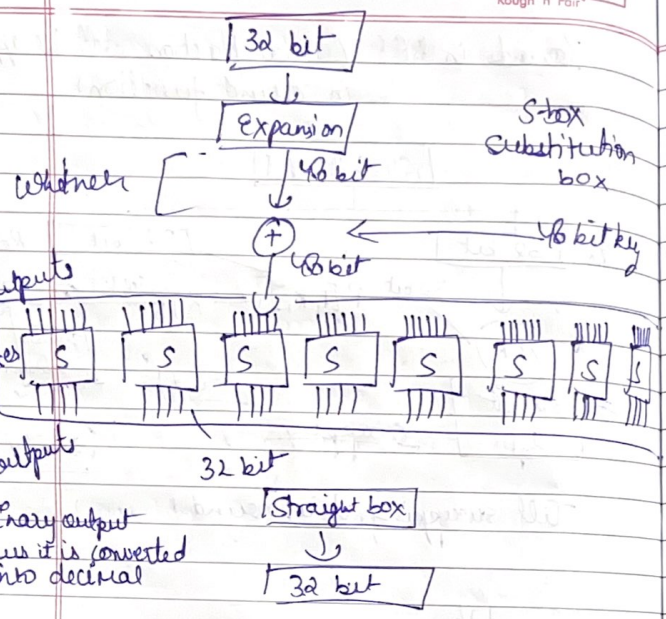
DES Function
The heart of the cipher is the DES function (F) which is already defined in DES function or in DES round.

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)

Sunil
DATE
PAGE
"Rough 'n' Fair"



Shannon's theory of confusion & diffusion

The terms confusion and diffusions were introduced by claude Shannon

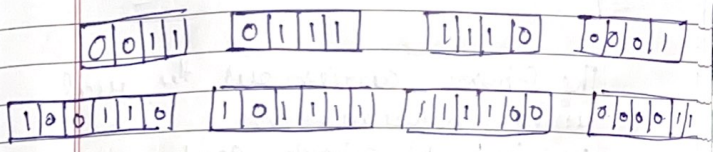
Shannon's concern was to prevent crypt analysis, based on statistical analysis. The reason is as follows

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)

Sunil
DATE
PAGE
"Rough 'n' Fair"

function of Expansion inside the function of DES.

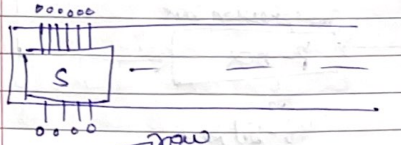
Note - $4 \times 8 = 32$ bit
$6 \times 8 = 48$ bit



Expansion permutation box
since right input is 32 bit and second key is a 48 bit key we must need to expand right input to 48 bit

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

Substitution box



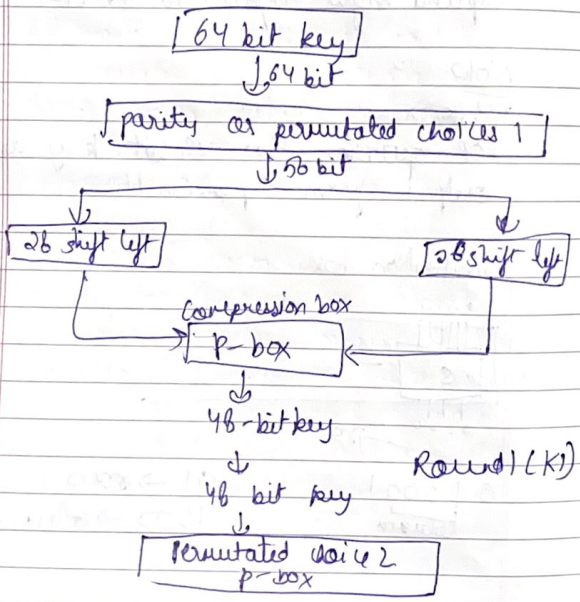
01 → row
1000 → column

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



48 bit key → K2

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 2^{56} 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 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

Sunil
DATE
PAGE
"Rough 'n' Fair"

How does block cipher work?

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

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

No of rounds
This block ciphers design principle indicates the overall strength of the ciphers 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 feistal 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 determine security. Function f should be designed in such a way that it cannot be substituted.

function F provide the strength to the algorithms

Key schedule algorithm
The key schedule algorithms 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.

Sunil
DATE
PAGE
"Rough 'n' Fair"

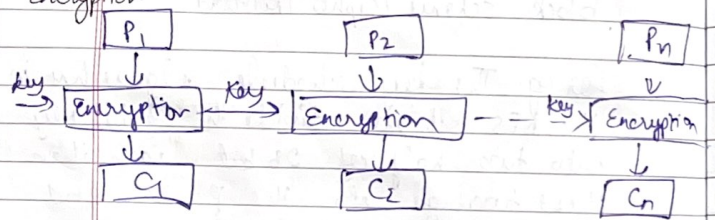
Mode of operation in Block cipher

The block cipher operation mode are divided into five parts and these modes of operation helped in provide security to the algorithms.

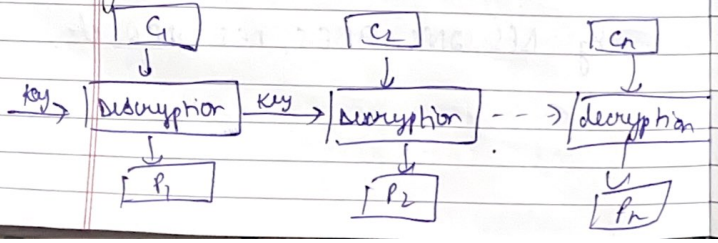
These modes are
1) Electronic code blok mode
2) Cipher block chaining mode
3) Cipher Feedback mode
4) output feedback mode
5) counter mode

[A] Electronic code Block (ECB) mode

Encryption



Decryption

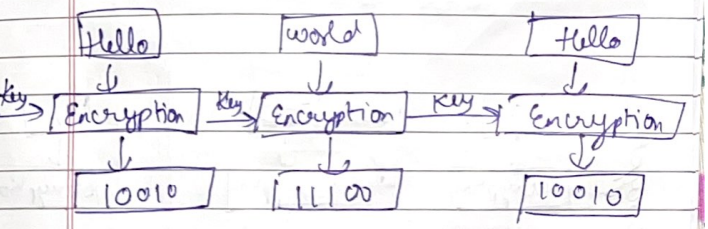


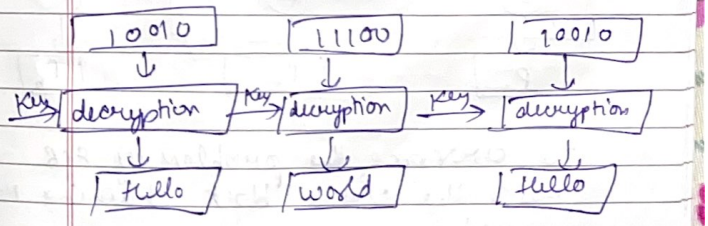
In ECB mode the given plain text message is divided into blocks of 64 bit each and each 64 bit block get encrypted.

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 generate the same cipher text block in the output which gives clue to the attacker.

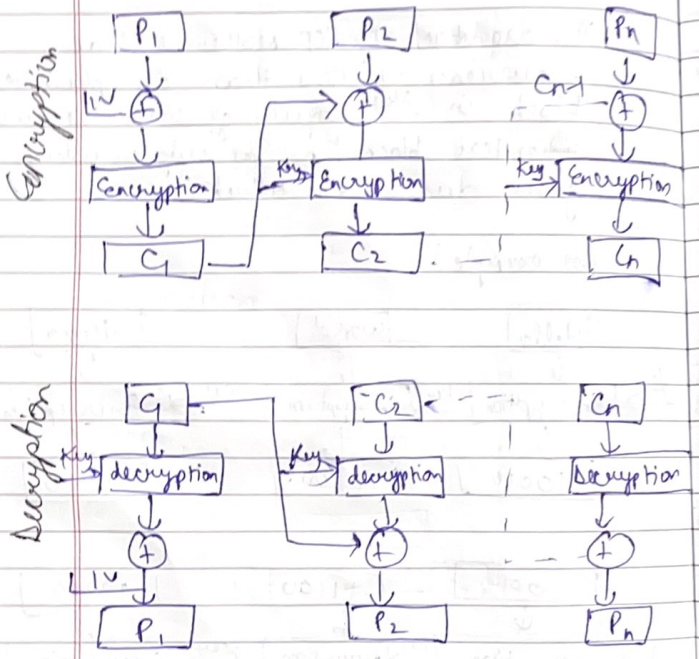
for example





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_1 or block.

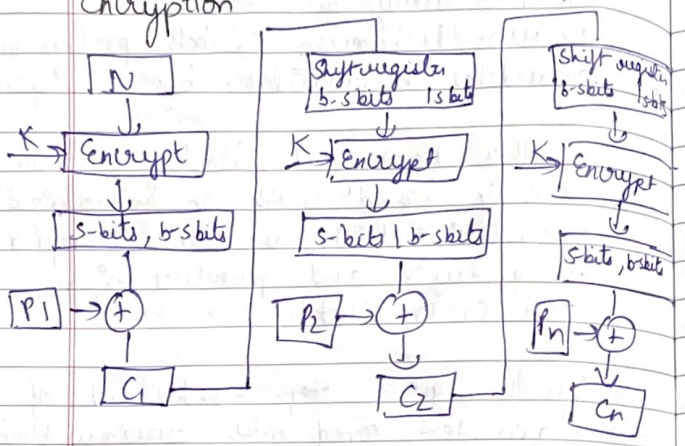
In the next step each block of plain text xored with previous block of cipher text. The procedure is continue till all plain text block gets encrypted.

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

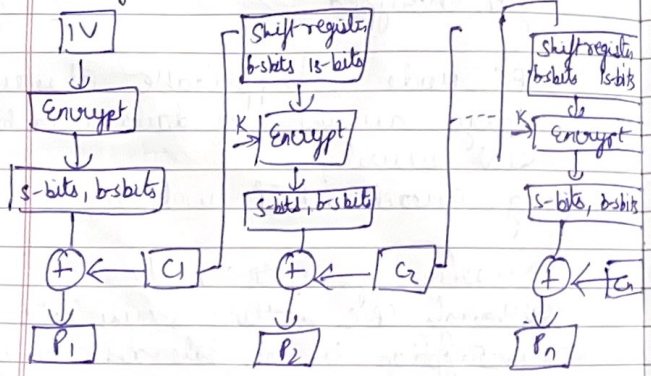
Disadvantages of CBC mode
Although CBC is more secure, its encryption is not tolerant of block losses. This is because blocks depend on their previous blocks for encryption. So if block B_i is lost, the encryption of all subsequent blocks will not be possible

[C] Cipher Feedback Mode (CFB)

Encryption



Decryption



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

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

The IV is encrypted and produces 64 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 8-bit) of the encrypted IV are XORed with the first s-bit of plain text P1 to produce the first 8-bit cipher text C1 which is then to transmitted to next step.

In next step content of the 64 bit shift register are shifted left by b-s bits and C1 is placed at the rightmost s-bit of the shift register and which again undergoes to encryption process

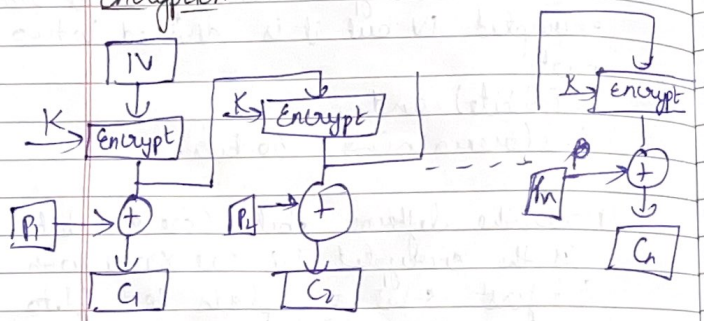
Disadvantages of CFB

CFB mode is converting a block cipher into a type of stream cipher

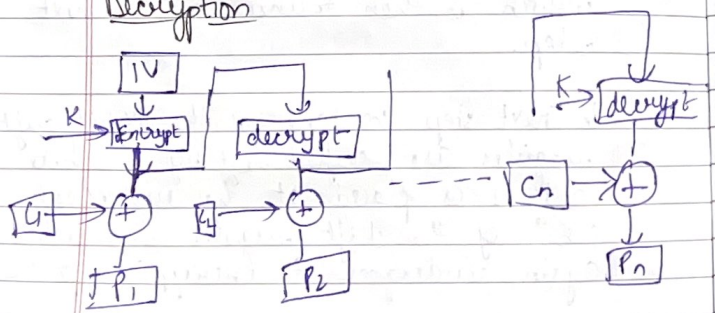
This algo mostly used to key-stream generator to produce key stream

[D] Output Feedback Mode (OFB)

Encryption



Decryption



The output feedback mode is similar to CFB mode in CFB the cipher text unit is fedback to the shift register. In case of OFB difference is that output of encryption process generating text C_1 is directly placed in next stage of shift register which perform XOR operation.

Disadvantages of OFB mode

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

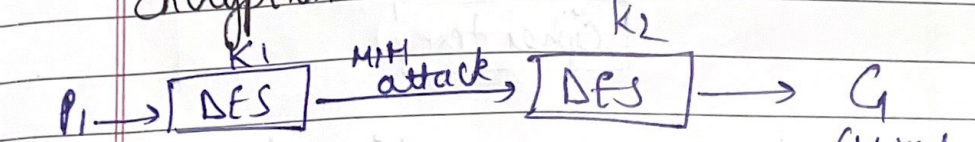
encryption speed is significantly slower

Sunil
DATE
PAGE
"Rough 'n' Fair"

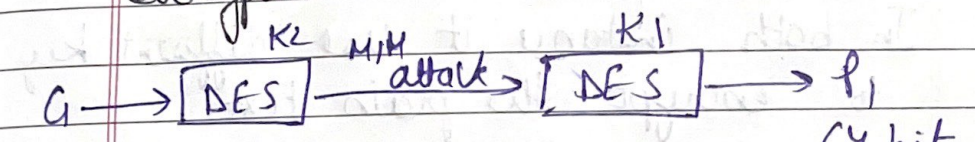
Double DES

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

Encryption



Decryption



M/M - 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
↓

(X1) DES Cipher

↓

64 Middle Text

↓

56 bit (K2) DES Cipher

↓

Cipher text

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)

As we know DES use 56 bit key to encrypt any plain text which can be easily tracked 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. 2DES 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 follows

→ 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.

Sunil
DATE
PAGE
"Rough 'n' Fair"

Some pair of PT | Some pair of CT

	PT	CT	match pair	CT	PT
K_1	ABC	X42	✓ K_2	X42	ABC
	CAE	AZY		2W0	CAE
	↓	↓		↓	↓
	↓	↓	(K1, K2)	↓	↓

Sunil
DATE
PAGE
"Rough 'n' Fair"

3DES (Triple DES)

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

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

Each ~~block~~ contain 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.

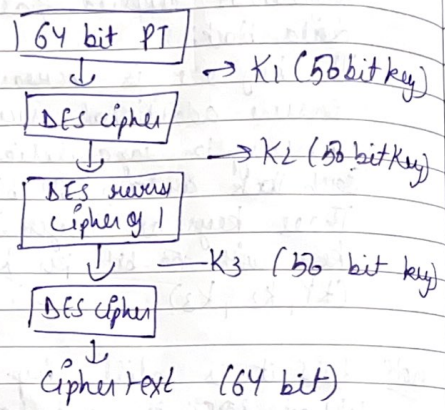
Triple DES was developed as a more secure ~~after~~ alternative because of DES small key length. In 3DES, the algo is run through three times with three key However it is only considered secure if three separate keys are used.

3DES was one of the most commonly used encryption technique/scheme before the use of AES

Some example of its implementation of 3DES includes. Microsoft office, firfox etc

Sunil
DATE
PAGE
"Rough 'n' Fair"

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



1. Explain purpose of IV vector
2. Explain drawback of 2DES
3. Explain working of conventional Encryption Method with the help of diag
4. Define cryptanalysis with its types
5. Define cryptography & cryptosystem

Sunil
DATE
PAGE
"Rough 'n' Fair"

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

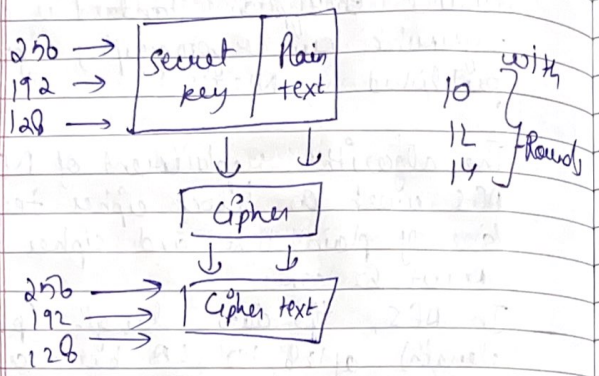
PT	KL	Rounds
128	128	10
192	192	12
256	256	14

Characteristics

→ AES has key of three length 128, 192, 256

→ It is flexible and has implementation of softwares and hardware

Block diagram



Characteristics
It provide high security and can prevent from many attacks.

It doesn't have any copyrights so it can be easily used globally (Douglas) FOSS tool

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

Examples
When you store personal info on a website facebook, twitter, etc and even when your use of bank card to make a purchase AES algo perform or provide security is everywhere

Online govt-site, passport application, driving license etc

Plaintext - "AES is used"
Plain text (128 bit) convert into 4x4 Matrix of byte
∴ the first 4 byte of a 128 bit input block occupy first column in the 4x4 matrix of byte. The next 4 byte occupy the second column and so on.

AES operate on a 4x4 matrix or column major order matrix of byte is called state array

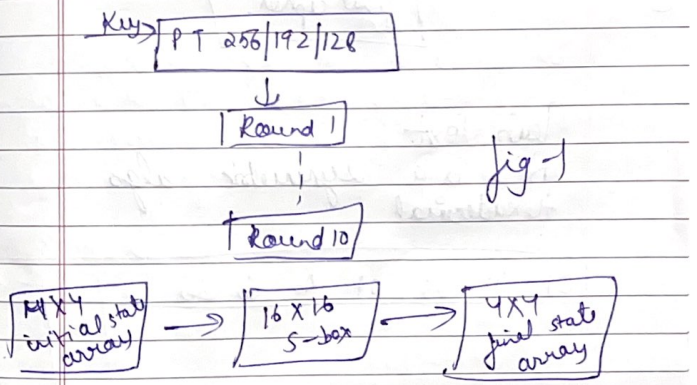
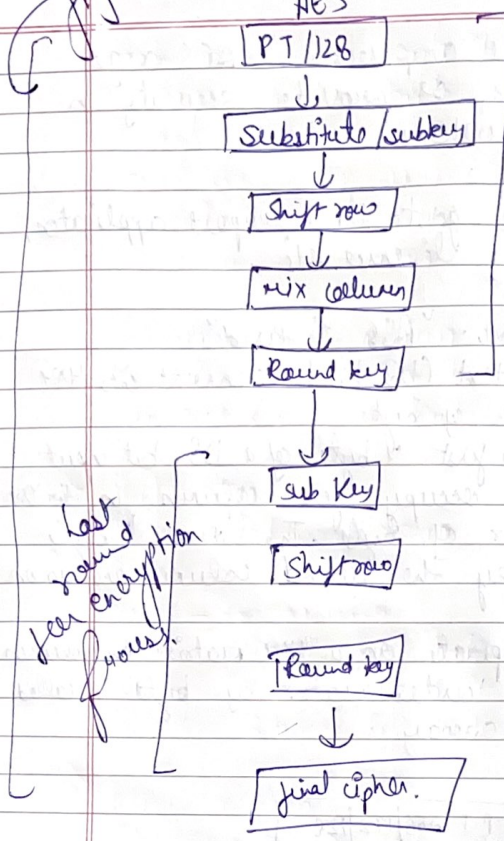


fig-1

Sunil
DATE
PAGE
"Rough 'n' Fair"

fig-2



Plain Text
AES is a symmetric algo
Hexadecimal

01	02	03	01	40	C0	20	—	—

Sunil
DATE
PAGE
"Rough 'n' Fair"

61	01	03	11
01	A0	ff	21
02	C0	50	22
03	20	1d	24

→ 16X16 Sbox → 4X4 final state array

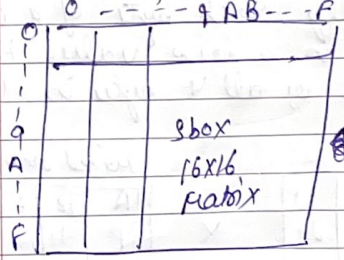
Initial state array

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

For encryption each round consist of the following 4-steps and those steps also called AES transformation system (functions)

1) Substitute / sub byte
AES defines a 16X16 matrix of byte values called an sbox that contains a permutation of all possible 256 8 bit values

Similarly, for 192 and 128 bit keys.



K1	1A	12	AE	23
K2	EF	05	11	81
K3	CB	96	12	62
K4	A1	C1	22	11

4X4 final state array

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

The row and column values serves as index X 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 maped in 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

X

Mixed row matrix

TA	12	AF	25
EP	11	A1	81
01	05	12	37
F6	21	22	11

P1	f1 b1XA1 + 01XEf + 03X01 + 11XF6
P2	f2 A1X12 + A0X11 + EFX05 + 21X21
P3	f3 02XAF + C0XA1 + 50X12 + 23X22
P4	f4 03X28 + 2dX81 + 1dX37 + 24X11

4 X 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 btw the 4 byte of a state column and one word of the round key, it can also be viewed as a wide level operations

Q Comparision btw DES v/s AES.