Unit-2

* Attack: It is defined as gaining, accessing the data, modifying or destroying the data that is been accessed by unauthorized person or user.

There are two types of attacks:

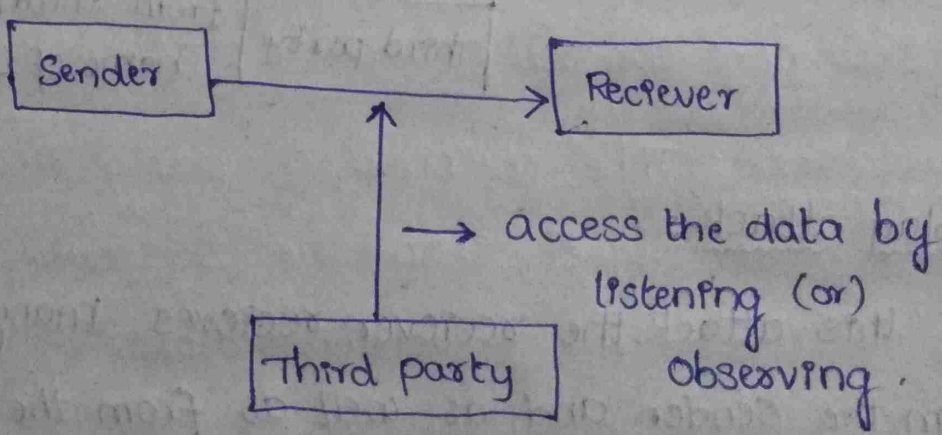
1. passive attack
2. Active attack

* passive attack: In this attack the data is been viewed by unauthorized person but no modifaction is done.
* Active attack: In this attack the modification is done by unauthorized person when data is sent between sender and recievet.
* In passive attack there are two types of methodologies

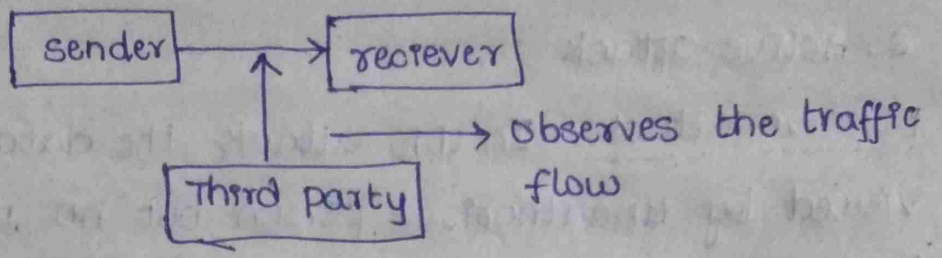
1. Release the content or Eewe dropping
2. Traffic analysis.

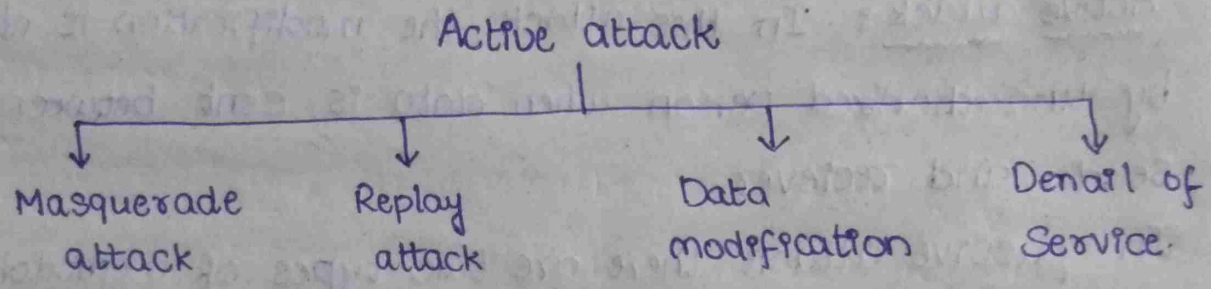
* Release the content (Eewe dropping):

In this methodology the third party person access the data by observing or listening the content but no modification is done.

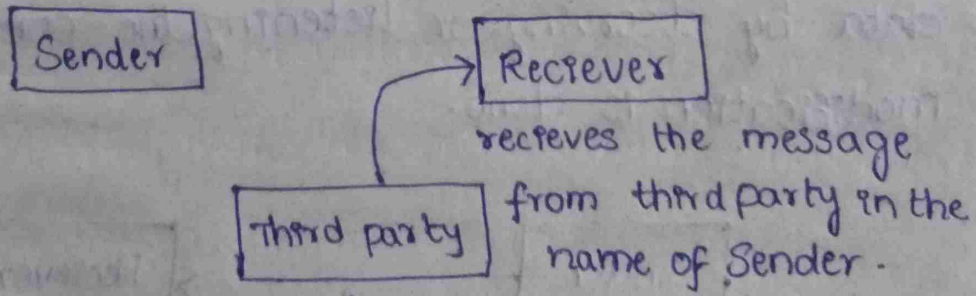


→ Traffic analysis: In this methodology the third party person observes the traffic flow that is been established between sender and reciever here traffic indicates the data sent by sender and recieved by reciever.



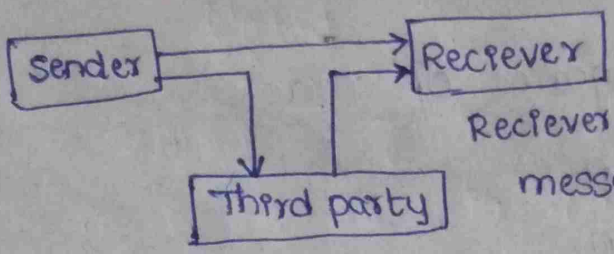


→ Masquerade attack: In this attack the reciever recieves the message from third party who is unauthorized person and reciever does not know who has sent the data.



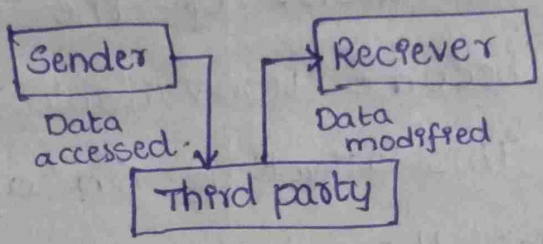
→ Replay attack:

In this attack the reciever recieves many messages from the sender and as well as from the third party.



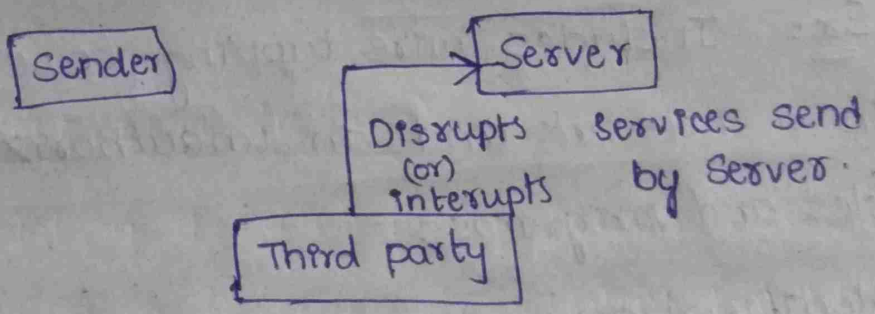
Recievер recieves twice message from Sender

→ Data modification : The sender sends, the data will be modified by the third party in small chunks and recievер recieves the message in the name of Sender.



→ Denail of Service:

In this attack the services sent by the server are interrupted by the third party which is done in the name of the sender.



→ Features of attacks:

1. Interruption.
2. Interception
3. Modification.
4. Fabrication.

* General Categories of attack

1. Interruption
2. Interception
3. Modification
4. Fabrication

* Interruption: An assist of the system is destroyed or become unavailable is known as interruption. This attack is on availability.

Ex: It includes the destruction of piece of hardware.

* Interception: An unauthorized party gains access to an assist. this attack is on confidentiality.

Ex: Includes wire tapping to capture the data in a network and an unauthorized copying of files and programs.

* Modification: An unauthorized party not only gains the access but modifies with that data.

Ex: changing the values in a data file.

* Fabrication: The authorized party inserts counter feit object into the system.

This attack is on authentication.

Ex: Includes the insertion of superious messages in a network or addition of records to a file.

* Security Services:

The message sent to reciever from Sender to that particular data Security is provided.

Types of security services:

1. Access control
2. Authentication
3. Confidentiality
4. Integrity
5. non-repudation

1) Access Control:

The access should be given to authorized persons and prevent unauthorized access to resources.

2) Authentication:

Verifying the identity of sender and the recievev whether it is authorized or unauthorized.

3) Confidentiality:

In this we provide security to the data which is sent by Sender.

4) Integrity:

There is no modification during transmission of data between Sender and reciever.

5) Non-repudation:

To prevent the data from denail of Service attack.

* Difference between authorization and authentication

Authorization	Authentication.
1. What user wants to do	1. who is doing the work
2. The access permissions given to the user whether he has to access it or not verifying the user permissions that are allocated to the user. Ex:- Having ATM Card of a bank because he is a authorized person to use the services of the bank.	2. The user identity is being verified. Ex:- Having a pin number to that particular ATM Card that is being allocated to that person or user is known as authentication.

* Security mechanism:

Security mechanism

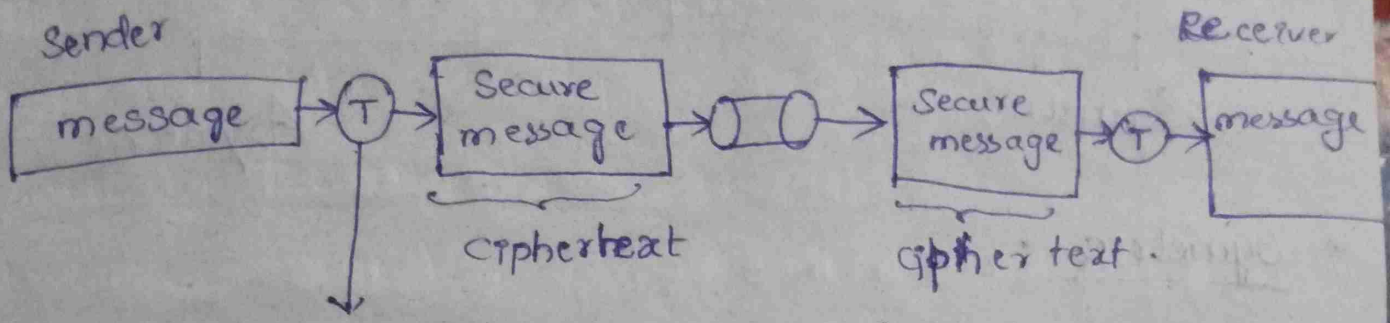
Specific Security

1) Encipherment
2) Digital signature
3) Access Control
4) Data integrity
5) Authentication exchange
6) Traffic padding
7) Routing Control
8) Notarization

pervasive security

1) Trusted functionality
2) Security label
3) Event detection
4) Security Audit trail
5) Security recovery.

Models of Network Security



1. encryption
2. Decryption

encryption: Converting plain text into cipher text using some algorithms and Secret key.

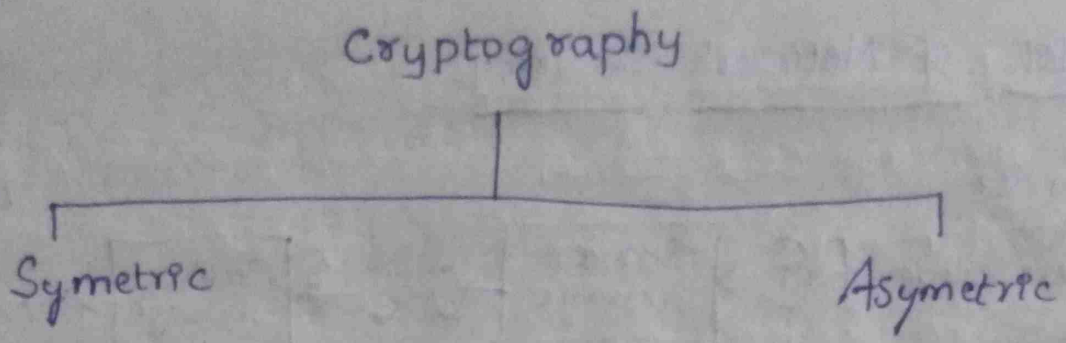
Decryption: Converting cipher text into plain text using some algorithms and Secret key.

* Cryptography:

→ It is a process of encryption and decryption

→ It is a study of Secure communication technique. and method of protecting information.

→ Cryptography is a technique that makes to convert information into an unreadable format this Conversation is done using some mathematical algorithms.



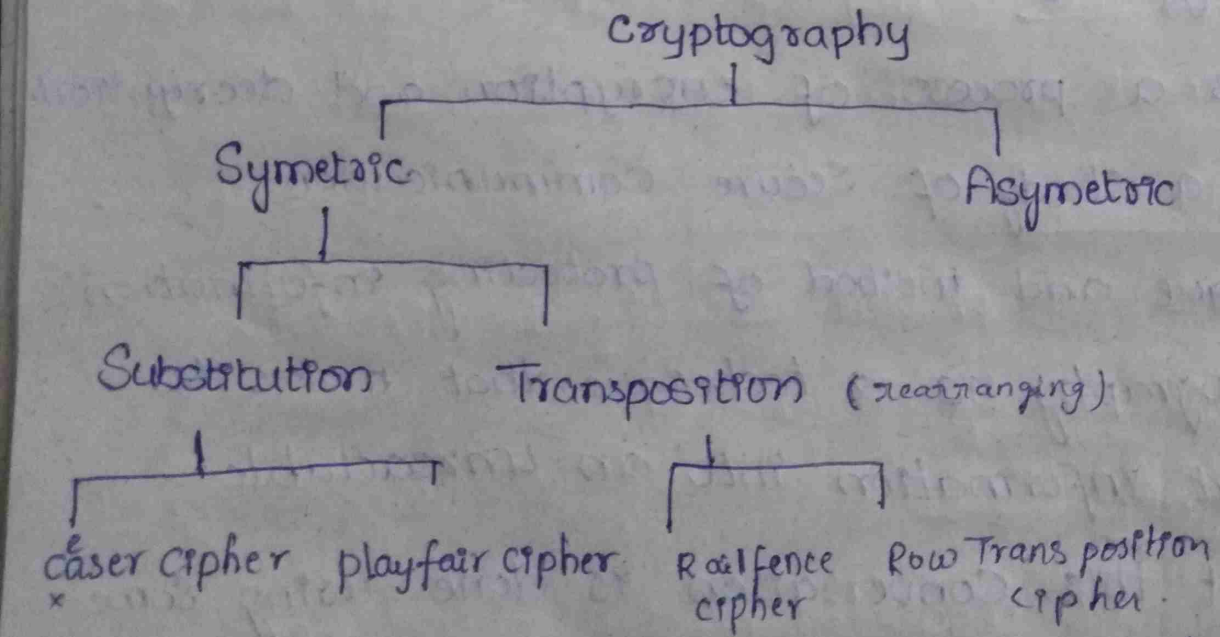
* Symetric :

Same key is been used in order to encrypt and decrypt the message.

* Asymmetric:

In this technique two different keys are used in order to encrypt and decrypt the message

1. public key
2. private key.



Substitution: plain text is replaced by other text.

Ceaser Cipher:

1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I
10	11	12	13	14	15	16	17	18
J	K	L	M	N	O	P	Q	R
19	20	21	22	23	24	25	26	
S	T	U	V	W	X	Y	Z	

* plain text to cipher text (Encryption):

plain text : HELLO → LIPPS

cipher text : $(p+k) \bmod 26$. k - key.

$1 \leq k \leq 26$ $k = 4$

$C(H) = (8+4) \bmod 26$

$= 12 \bmod 26$

$= 12 = L$

$C(E) = (5+4) \bmod 26$

$= 9 \bmod 26$

$= 9 = I$

$C(L) = (12+4) \bmod 26$

$= 16 \bmod 26$

$= 16 = P$

$C(O) = (15+4) \bmod 26$

$= 19 \bmod 26$

$= 19 = S$.

* Cipher text to plain text (Decryption)

plain text = $(C-k) \bmod 26$

$P(L) = (12-4) \bmod 26$

$= 8 \bmod 26$

$= 8 = H$.

$P(I) = (9-4) \bmod 26$

$= 5 \bmod 26$

$= 5 = E$

$P(P) = (16-4) \bmod 26$

$= 12 \bmod 26$

$= 12 = L$

$P(P) = (16-4) \bmod 26$

$= 12 \bmod 26$

$= 12 = L$

$P(S) = (19-4) \bmod 26$

$= 15 \bmod 26$

$= 15 = O$.

→ BALLOON → FEPPSSR

k=4

Encryption:

cipher text : (P+k) mod 26

C(B) = (2+4) mod 26
= 6 mod 26
= 6 = F

C(A) = (1+4) mod 26
= 5 mod 26
= 5 = E

C(L) = (12+4) mod 26
= 16 mod 26
= 16 = P

C(O) = (15 + 4) mod 26
= 19 mod 26 = 19
= S

C(N) = (14 + 4) mod 26
= 18 mod 26
= 18
= R

Decryption:

cipher text : FEPPSSR

plain text : (P-k) mod 26

P(F) = (6-4) mod 26
= 2 mod 26 = 2 = B

P(E) = (5-4) mod 26
= 1 mod 26 = 1 = A

P(P) = (16-4) mod 26
= 12 mod 26 = 12 = L

P(P) = (16-4) mod 26
= 12 mod 26 = 12 = L

P(S) = (19-4) mod 26
= 15 mod 26 = 15 = O

P(S) = (19-4) mod 26
= 15 mod 26 = 15 = O

P(R) = (18-4) mod 26
= 14 mod 26 = 14 = N

* Play-fair cipher:

plain text : HELLO

Secret key : NETWORK.

1. Divide the plain text into pair of letters.
2. Differentiate repeated letter in the pair with dummy letter.

3. If pair of plain text letters are in same row replace them with right most letter.

4. If the plain text letter are in same column then replace with down letters.

5. If the plain text letter are in different rows or columns replace with diagonal letter.

1) plain Text : HELLO

Secret key : NETWORK

HE | LX | LO

FW | PU | NS

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

2) plain text : ZOO

Security key : GATE

ZO | OX

~~CU | RO~~ BU | MZ

~~US | UR~~.

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

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

3) plain text: WELCOME

Secret key: NETWORK

WE | LC | OM | EX.

OT | RS | ES | VT

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

* Transposition Technique:

~~Rail~~ → Rearrange order of plain text in a bit position

→ There is no replacement or Substitution.

* Railfence cipher:

plain text: welcome to my class

Secret key: No key.

w	l	o	e	o	y	l	s		
e	c	m	t	m	c	a	s		

cipher text:

WLOEOYLSECMTMCAS

* plain text: what is your name

Secret key: No Secret key

cipher text wa?yunmhtSorae

w	a	?	y	u	n	m			
h	t	s	o	r	a	e			

* Row Transposition Cipher:

plain text : welcome to my class

Secret key : 3 2 4 5 1 (5×5 matrix)

(The unique key without repetation) between 1 and 9 and no ascending or descending order for key.

Dummy letter : wxyz

3	2	4	5	1
w	e	l	c	o
m	e	t	o	m
y	c	l	a	s
s	w	x	y	z

cipher text: omszeecwwmysltlxcoay

plain text : what is your name

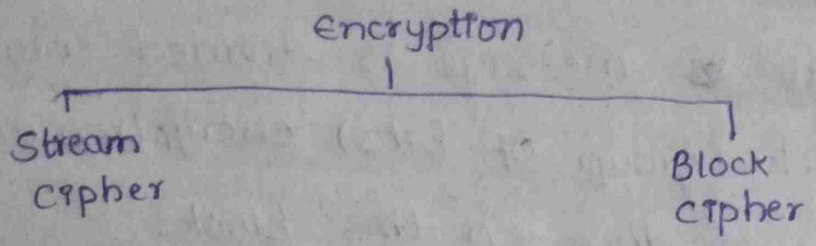
Secret key : 3 2 4 5 1 (5×5 matrix)

Dummy letter : z

3	2	4	5	1
w	h	a	t	i
s	y	o	u	r
n	a	m	e	z

cipher text: irzhyawsnaomtue.

* Cipher Algorithms:



Stream Cipher

Encryption: $C_i = P_i \oplus k_i$

Decryption: $P_i = C_i \oplus k_i$

* Cipher Algorithms:

Encryption is done on two methodologies

1. Stream cipher
2. Block cipher

Stream cipher: In this technique Only one bit at atime is been processed.

Encryption : $C_i = P_i \oplus k_i$ → exclusive OR.

Decryption : $P_i = C_i \oplus k_i$

C_i = cipher text

k = Secret key

P = plain text

Advantages:

1. High speed transformation
2. Low error propagation

Disadvantages:

1. Low diffusion
2. Less-Secure

* Block cipher:

Plain text message is divided into fixed sized blocks (group of bits) encryption and decryption is done on this block.

→ Advantages:

1. High diffusion
2. More Secure.

→ Disadvantages:

1. Encryption process is slower.
2. Error propagation.

* Block cipher modes of operation:

→ ECB (Electronic Code Book)

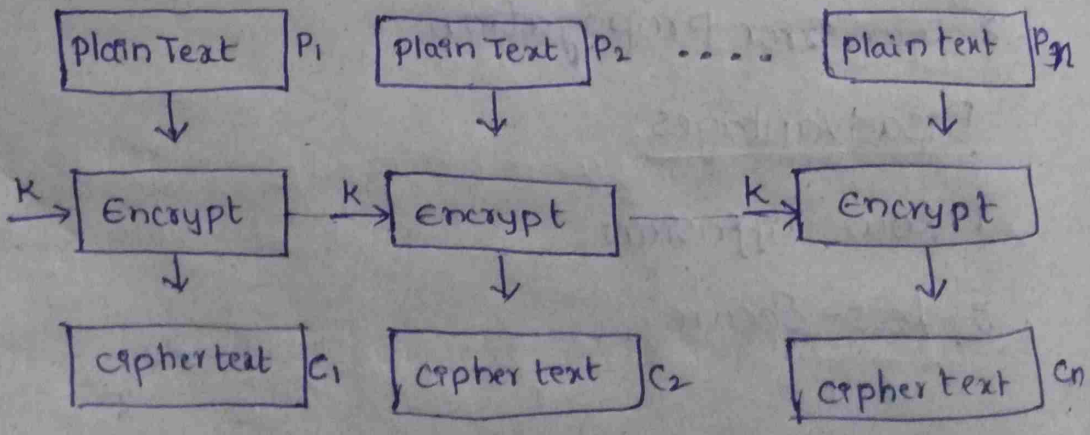
→ CBC (Cipher Block chain)

→ OFB (output feedback mode)

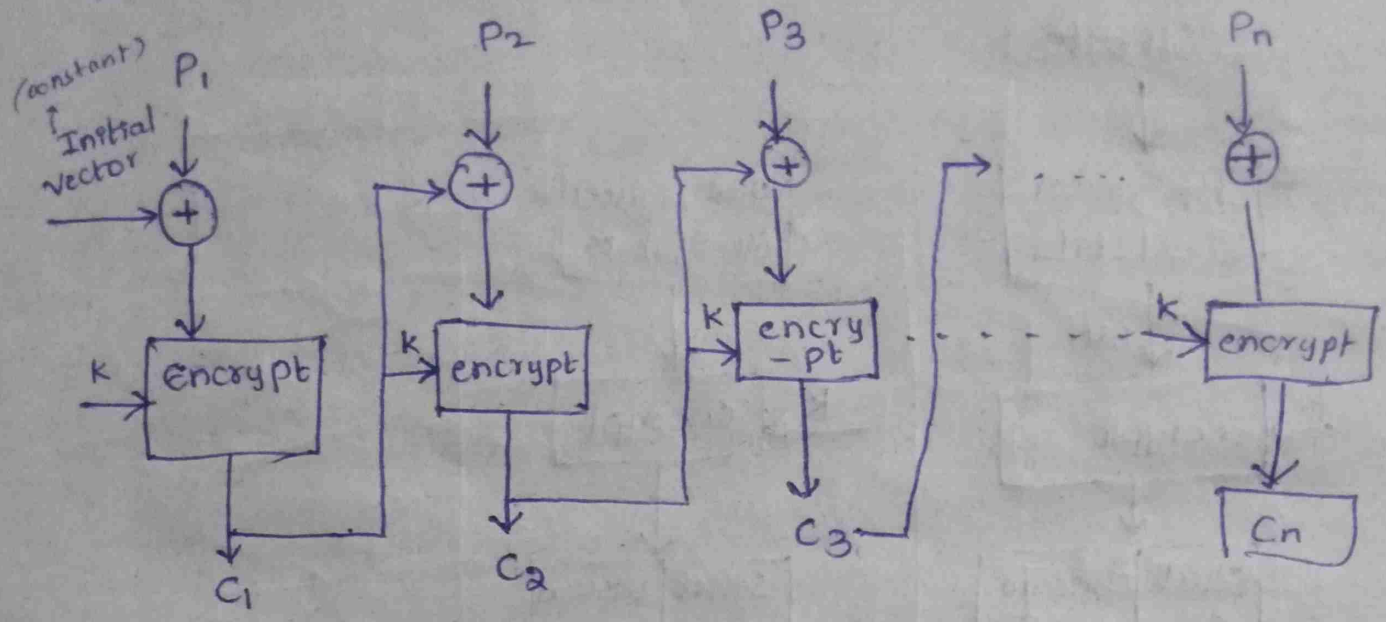
→ CFB (cipher feedback mode)

→ Counter mode.

* Electronic Code Book (ECB)

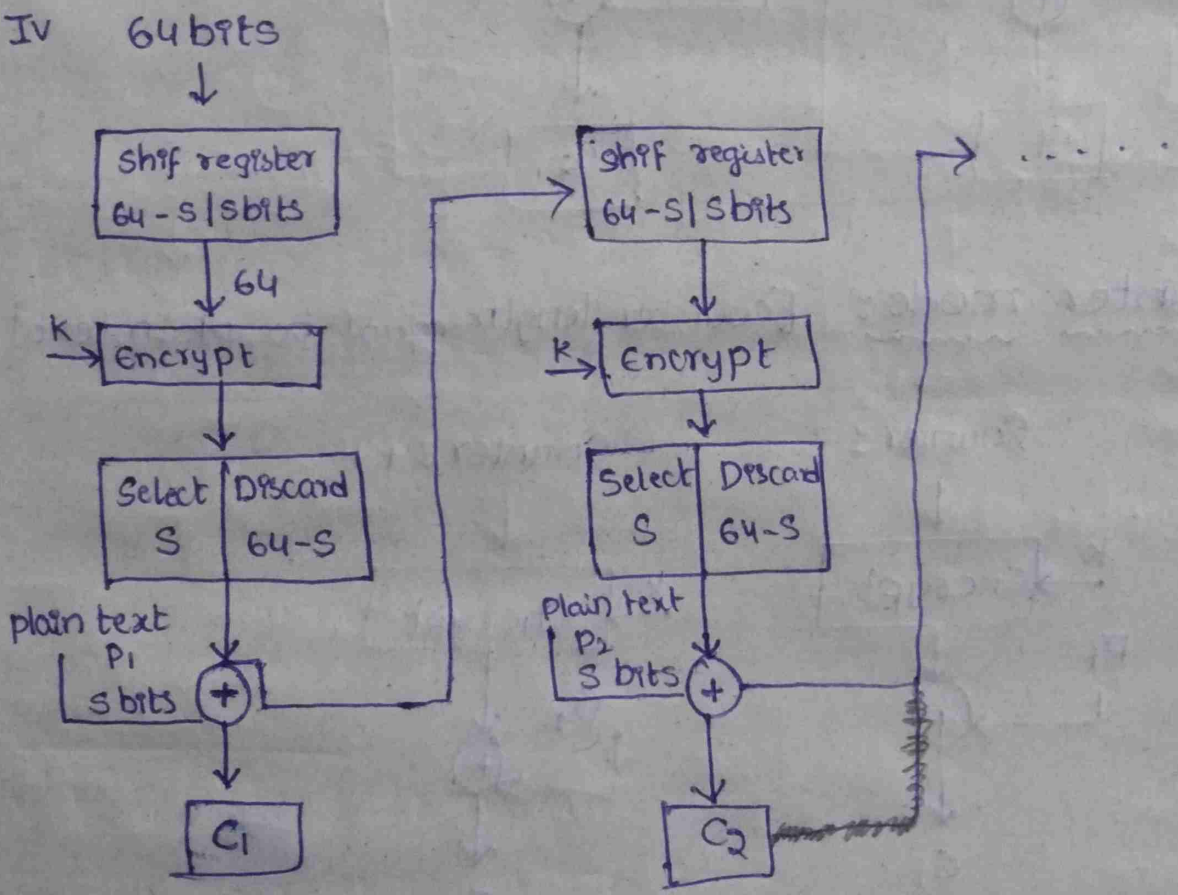


* Cipher Block chain (CBC):

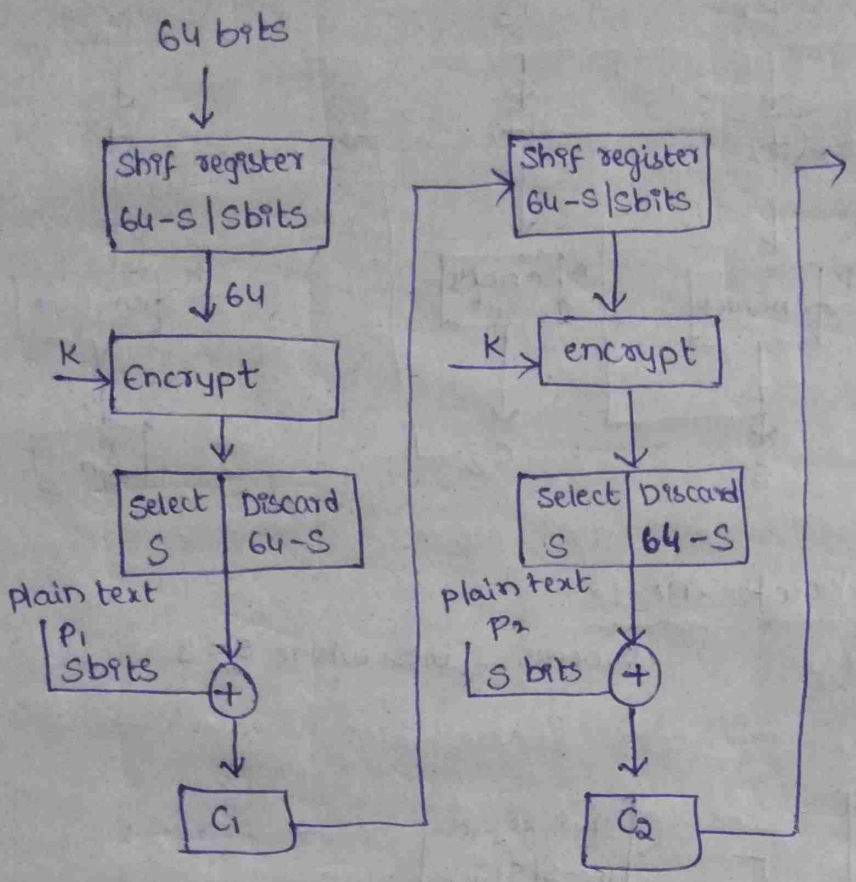


* Output feedback mode:

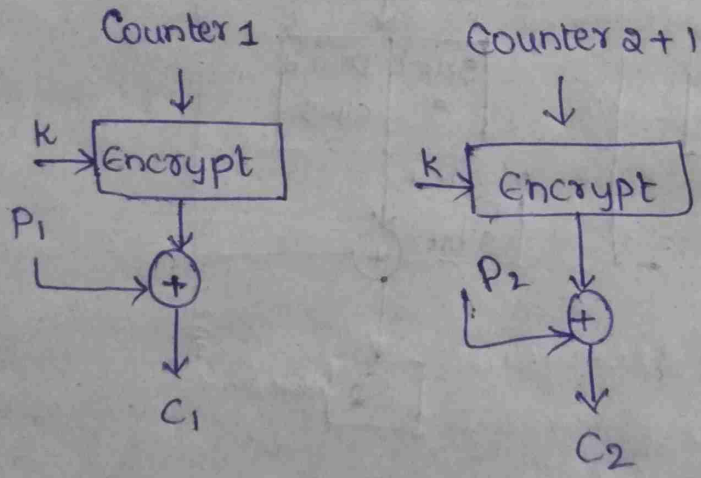
process S bits where S = 8



* Cipher feedback mode (CFB):



* Counter mode: [counter length equal to plain text]



STREAM Cipher

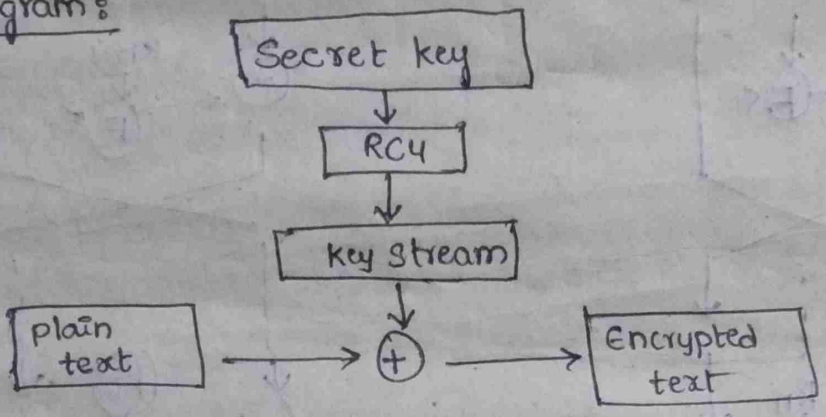
RC4 Algorithm:-

→ RC4 means Rivest Cipher 4 invented by Ron Rivest in 1987 for RSA Security. It is a

Stream ciphers. Stream ciphers operate on a stream of data byte by byte.

→ RC4 stream cipher is one of the most widely used stream ciphers because of its simplicity and speed because of its simplicity and speed of operation. It is a variable key-size stream cipher with byte-oriented operations. It uses either 64 bit or 128 bit key sizes.

Block diagram:



Ex:- plain text to cipher (Encryption)

```
  1 1 0 0 1 1 0 0   plain text
  0 1 1 0 1 1 0 0   key stream
-----------------
  1 0 1 0 0 0 0 0   cipher text
-----------------
```

Cipher text to plain text (Decryption)

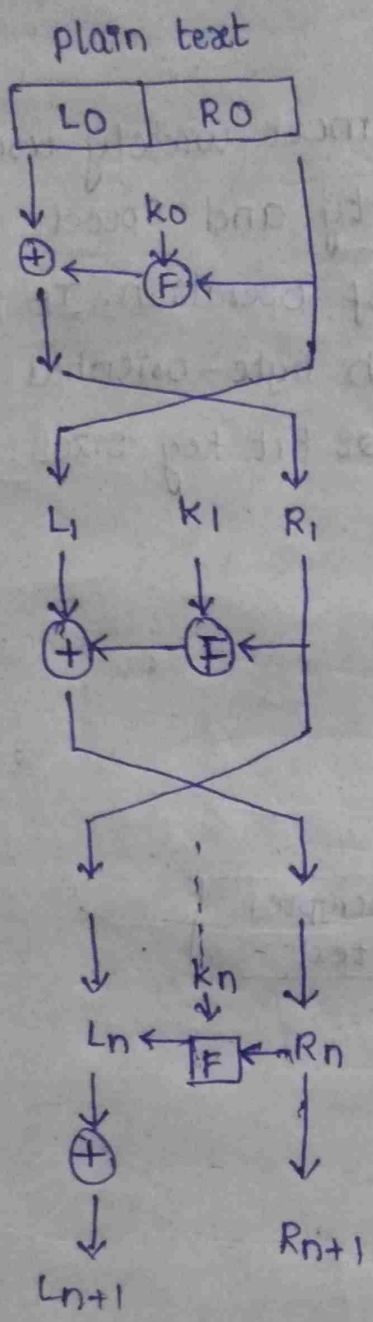
```
  1 0 1 0 0 0 0 0   cipher text
  0 1 1 0 1 1 0 0   key stream
-----------------
  1 1 0 0 1 1 0 0   plain text
-----------------
```

* Feistal Structure:

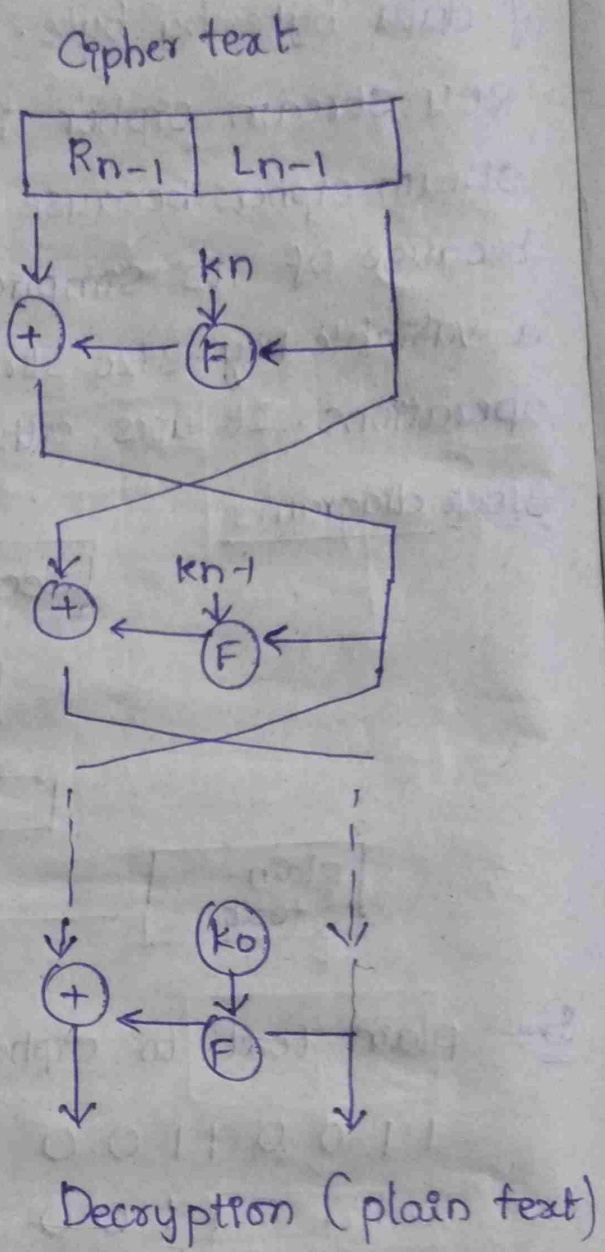
→ It is followed by block cipher

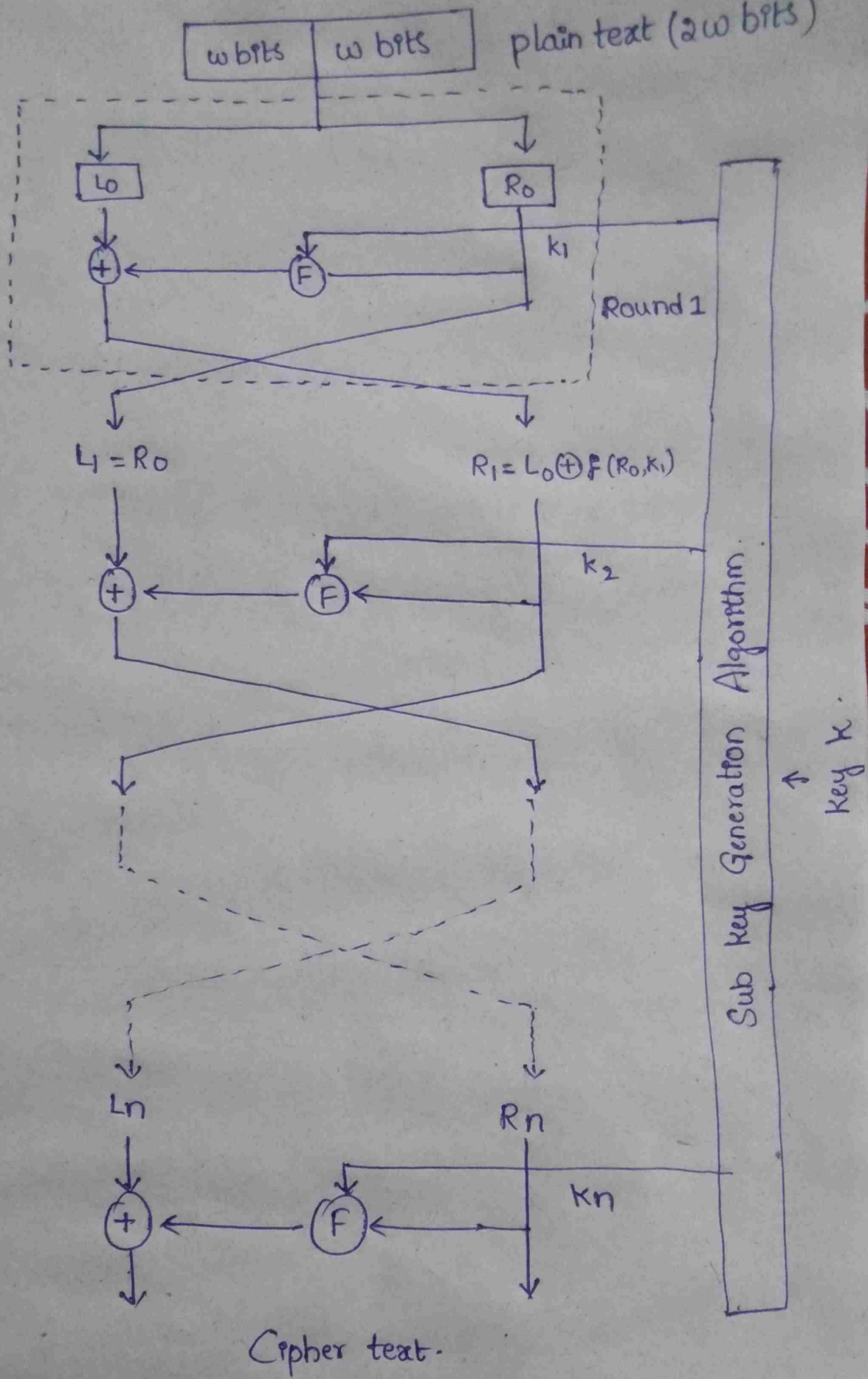
→ Block cipher implemented by Feistal Structure to improve the security.

Encryption:-



Decryption :-

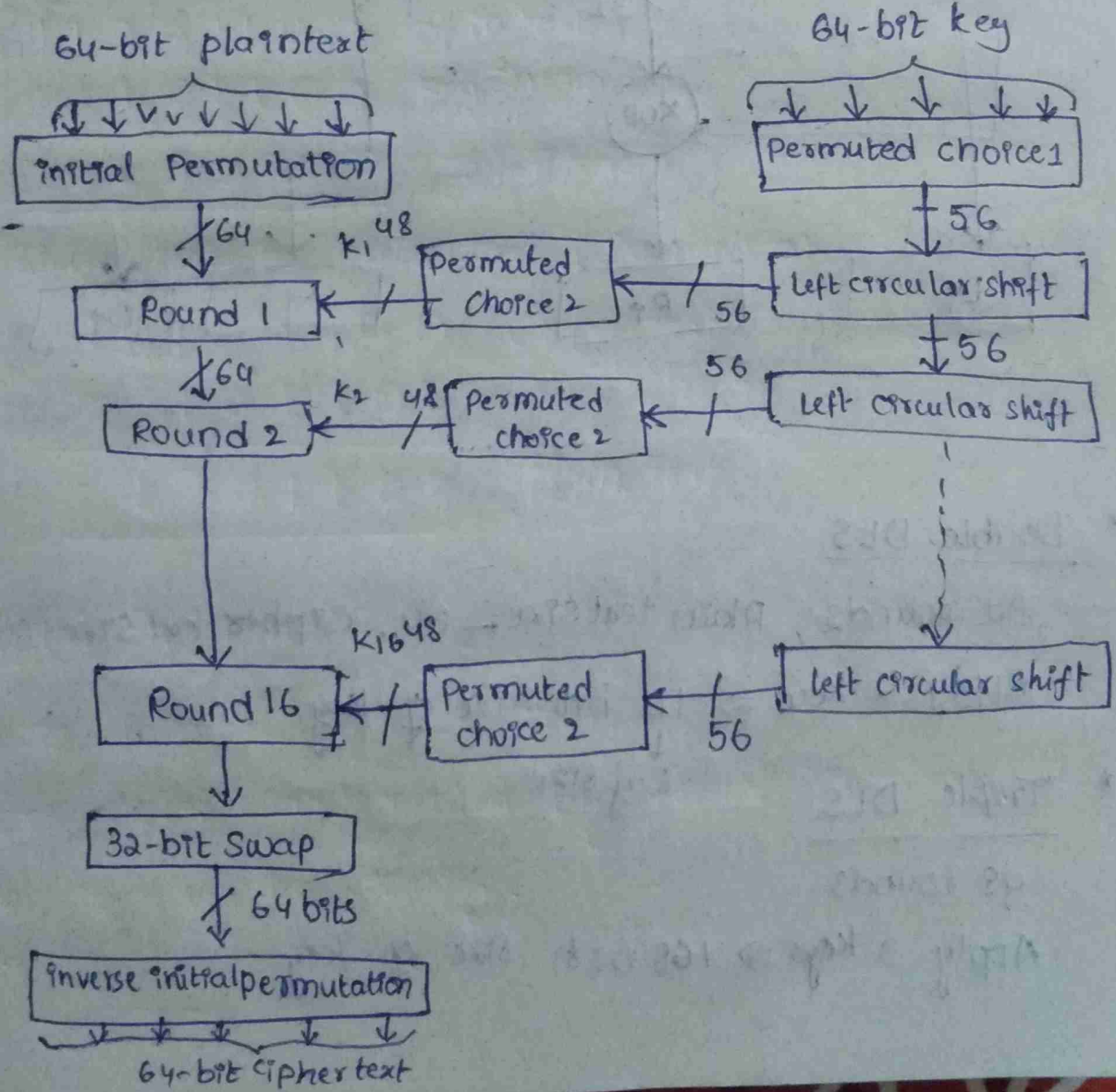



w bits
w bits
plain text (2w bits)
L_0
R_0
k_1
F
Round 1
$L_1 = R_0$
$R_1 = L_0 \oplus f(R_0, K_1)$
k_2
Sub key Generation Algorithm
Key K
L_n
R_n
k_n
Cipher text.

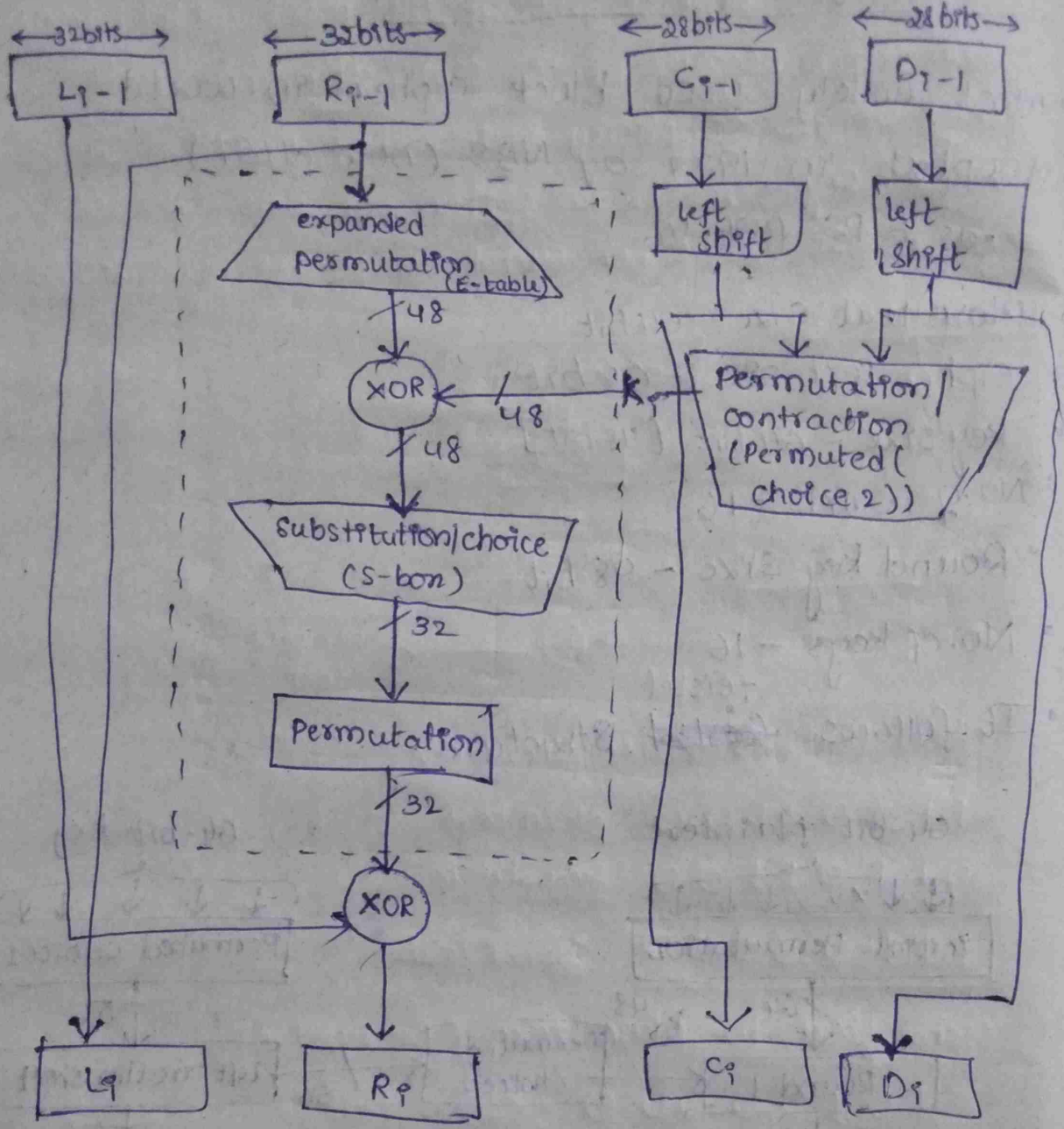
Conventional Encryption Algorithms

** Data Encryption Standard (DES)

- most widely used block cipher in world
- adopted in 1977 by NBS (now NIST)
  - as FIPS PUB 46
- Plain text size - 64 bit
- cipher text size - 64 bit
- key size - 64 bit [48 bit]
- No. of rounds - 16
- Round key size - 48 bit
- No. of keys - 16
- It follows ferstel Structure.



Detail Overview About Round



* Double DES

32 rounds, plain text size - 64, Cipher text size - 64

Apply 2 keys ⇒ 112 bit size of key.

↓

key size.

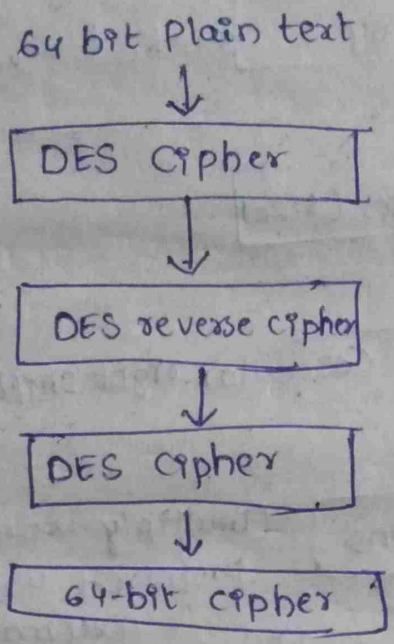
* Triple DES

48 rounds

Apply 3 keys ⇒ 168 bit size of key

plain text size - 64 bit
cipher text size - 64bit feistel structure.

Block diagram of double, Triple DES.

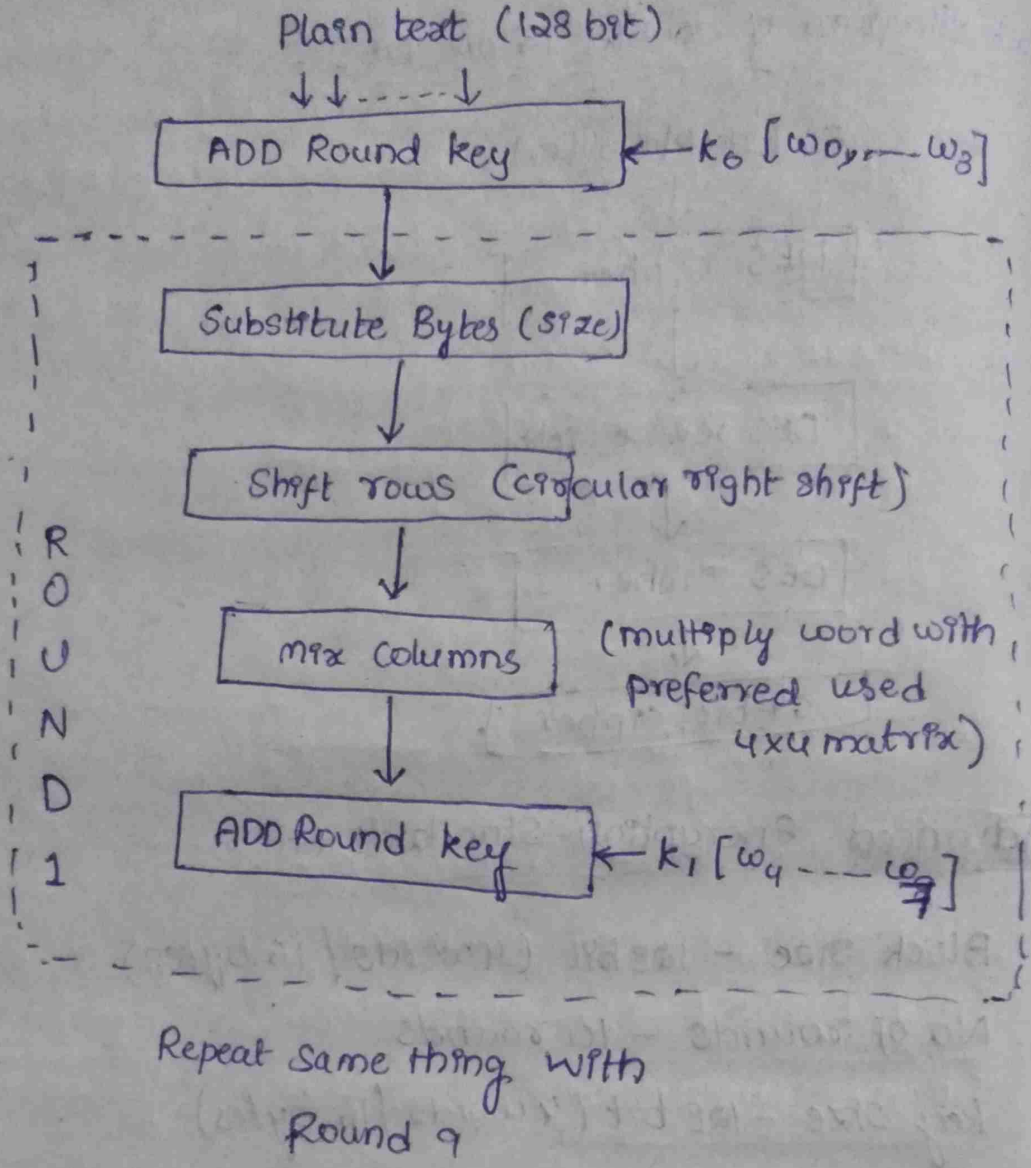


* Advanced Encryption Standards (AES)

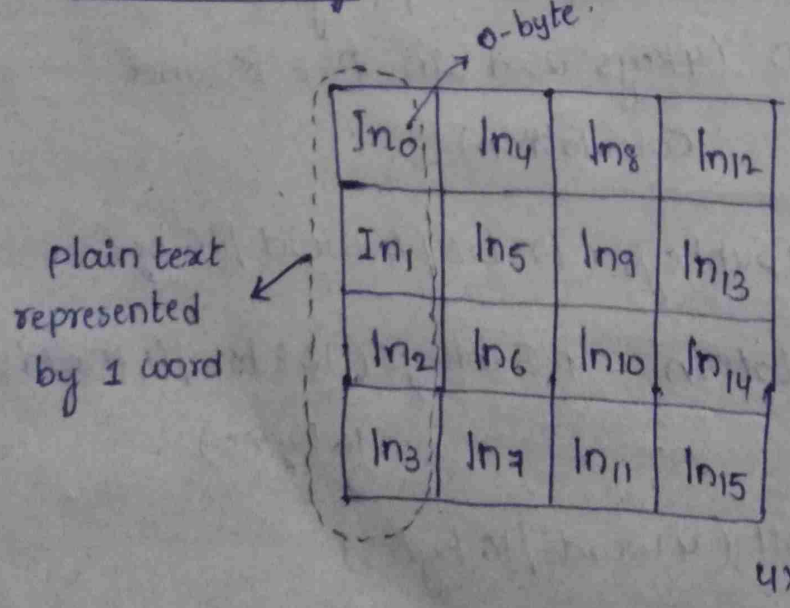
1. Block size - 128 bit (4 words / 16 bytes)
2. No of rounds - 10 rounds
3. key size - 128 bit (4 words / 16 bytes)
4. No. of Sub keys - 44 Subkeys
5. Each Sub key size - 32 bit / 1 word / 4 bytes
6. No. of keys - 10 (4 keys used in PRE Round Calculation)
7. Each round - 4 Subkeys (128 bit / 4 word / 16 bytes)
8. pre round Calculation - 4 Subkeys (128 bit / 4 words / 16 bytes)
9. Cipher text - 128 bit (4 words / 16 bytes)

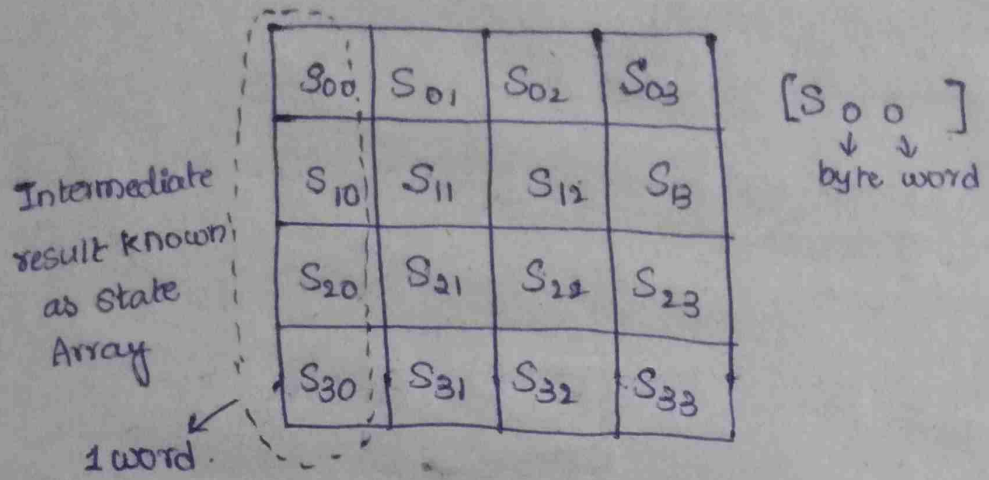
AES follows feistel Structure.

* Block diagram:

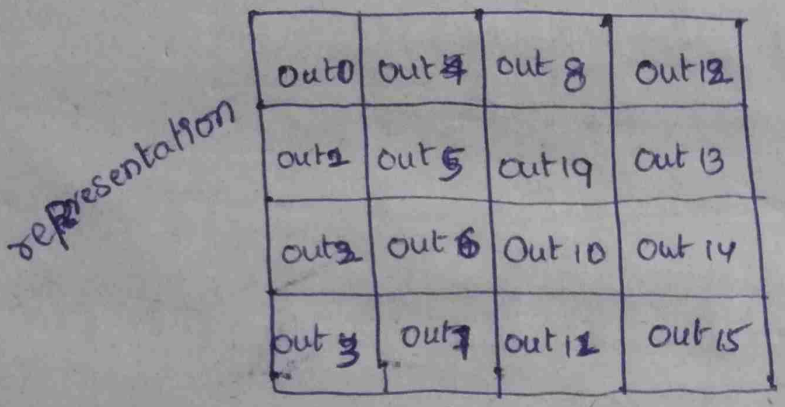


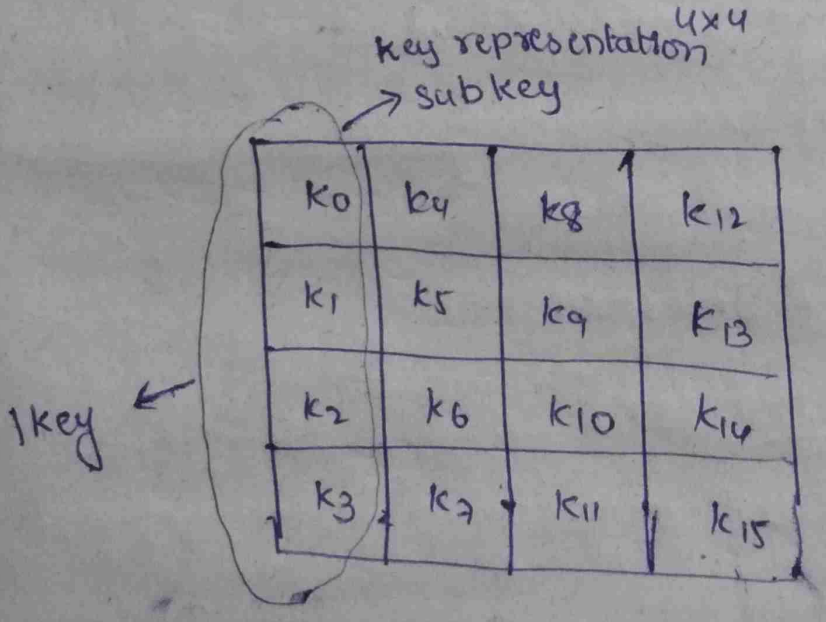
Input array




Intermediate result known as State Array
1 word
S_{00} S_{01} S_{02} S_{03}
S_{10} S_{11} S_{12} S_{13}
S_{20} S_{21} S_{22} S_{23}
S_{30} S_{31} S_{32} S_{33}
$[S_{00}]$
byte
word

Output :


representation
out0 out4 out8 out12
out1 out5 out9 out13
out2 out6 Out10 out14
out3 out7 out11 out15


key representation 4×4
subkey
1key
k0 k4 k8 k12
k1 k5 k9 k13
k2 k6 k10 k14
k3 k7 k11 k15