Unit-2

DES:

* DES is also known as data encryption standard.

* Same key is used for both encryption and deryption. So it is known as symmetric block cipher.

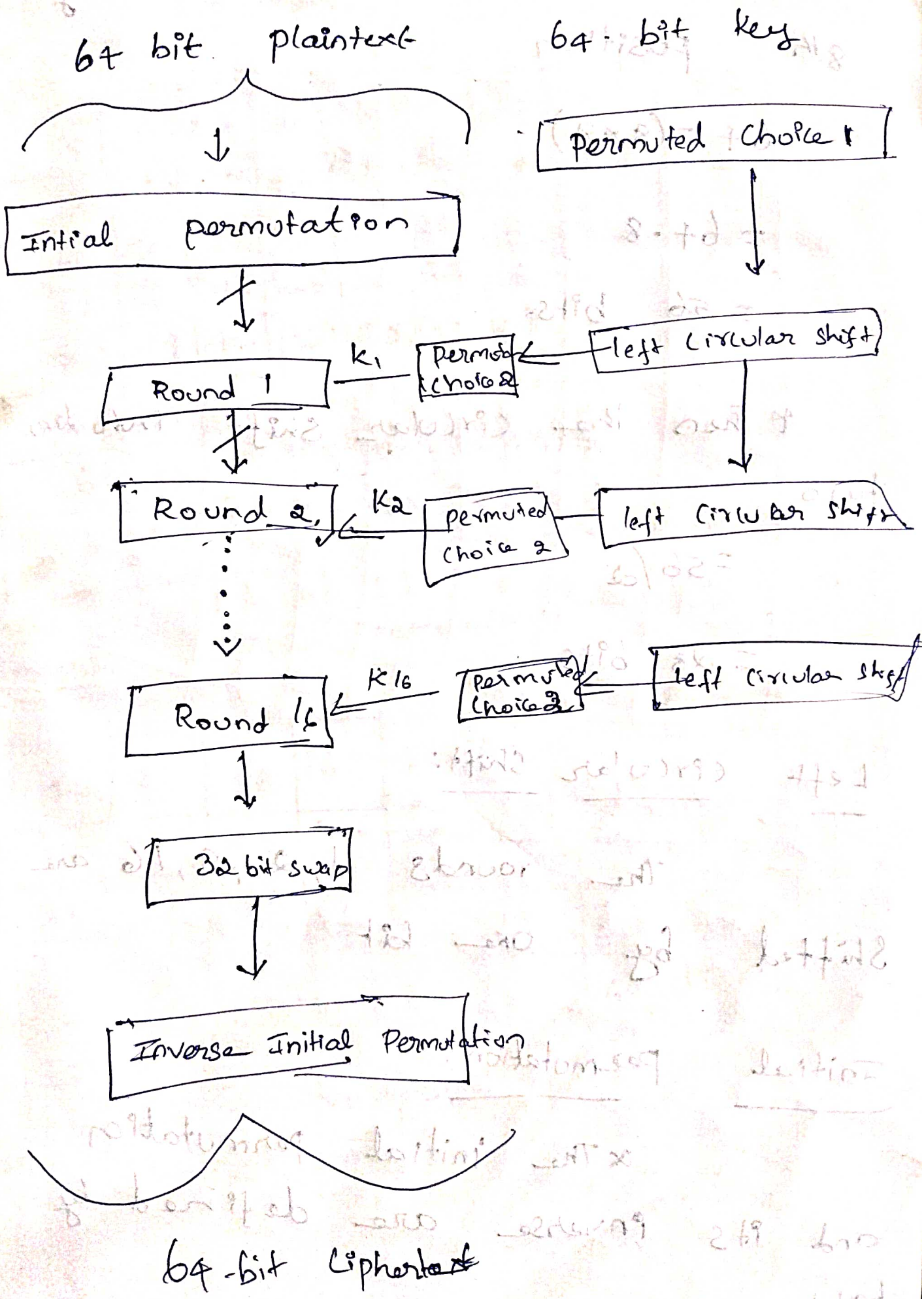
* It is adopted by National institute of Science & Technology in 1977

* It is completely replaced by Advanced data encryption Standard in 2001

* It is a powerfull algorithm algorithm

* The input size is 64 bits

Key is 64 bit


64 bit plaintext
64 bit key
Permuted Choice 1
Intial permutation
left circular shift
Permuted Choice 2
K_1
Round 1
left circular shift
permuted choice 2
K_2
Round 2
left circular shift
permuted choice 2
K_{16}
Round 16
32 bit swap
Inverse Initial Permutation
64-bit ciphertext

* Initially 64 bits, 8 parity bits are to be removed from every 8th position

$64 = (8 \times 8)$

$= 64 - 8$

$= 56$ bits

* Then the circular shift into two

$= 56/2$

$= 28$ bits

<u>Left circular shift:</u>

The rounds 1, 2, 9, 16 are shifted by one bit

<u>Initial permutation:</u>

* The initial permutation and its inverse are defined by tables.

* The input table consists of 64 bits numbered from 1 to 64.

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

Inverse Initial 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

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

Single Round for DES :

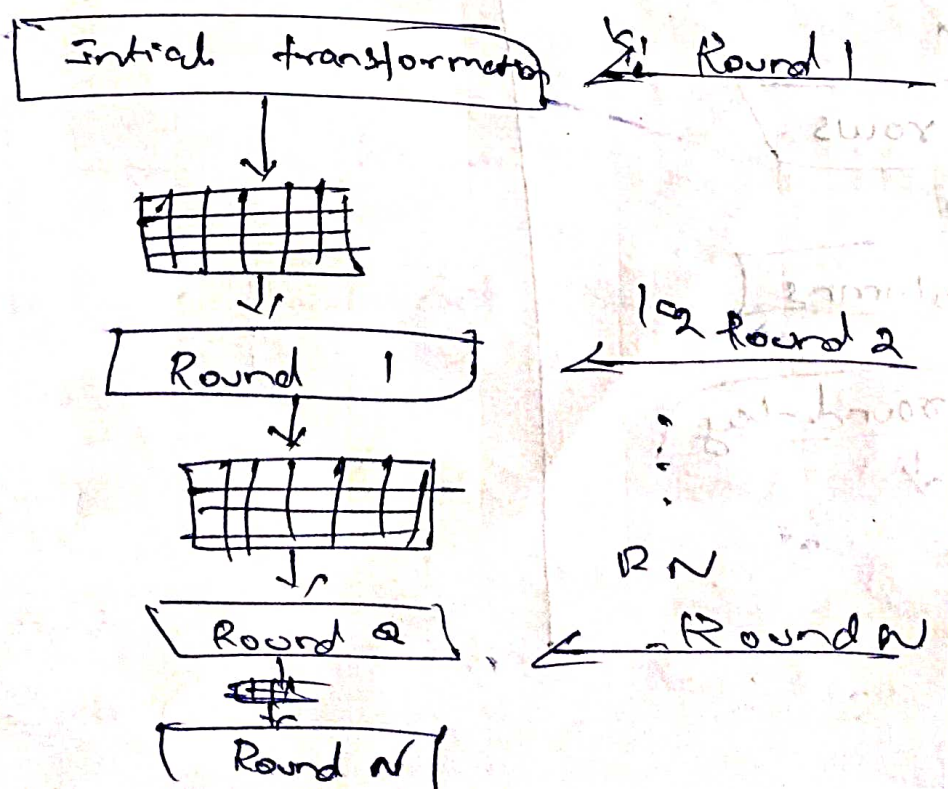
* Round key is 48 bits
* Input is 48 bit
* Result is 48 bit

2) AES

* Advanced encryption Standard
* Developed by NIST in 2001
* More popular symmetric encryption algorithm is AES
* It is found atleast six time faster than DES
* DES is replaced by AES
* It is widely used

AES Structure:

128 bits plaintext



* AES is an Iterative faster than Feistal Cipher

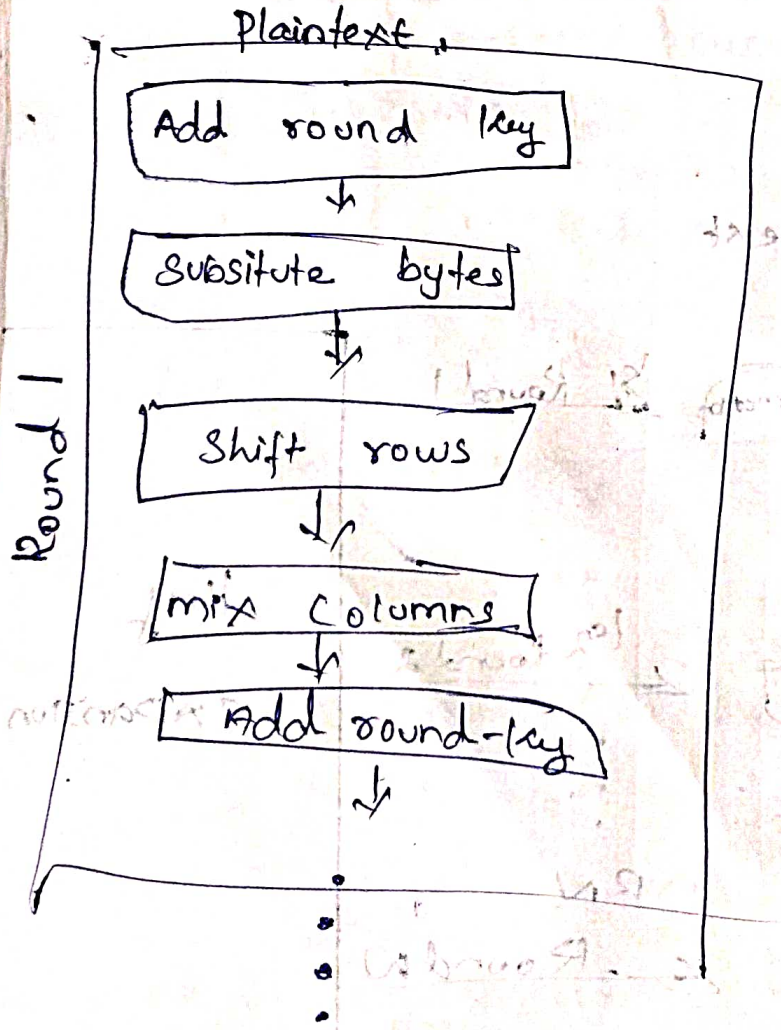
* It is based on subsitution-permutation network

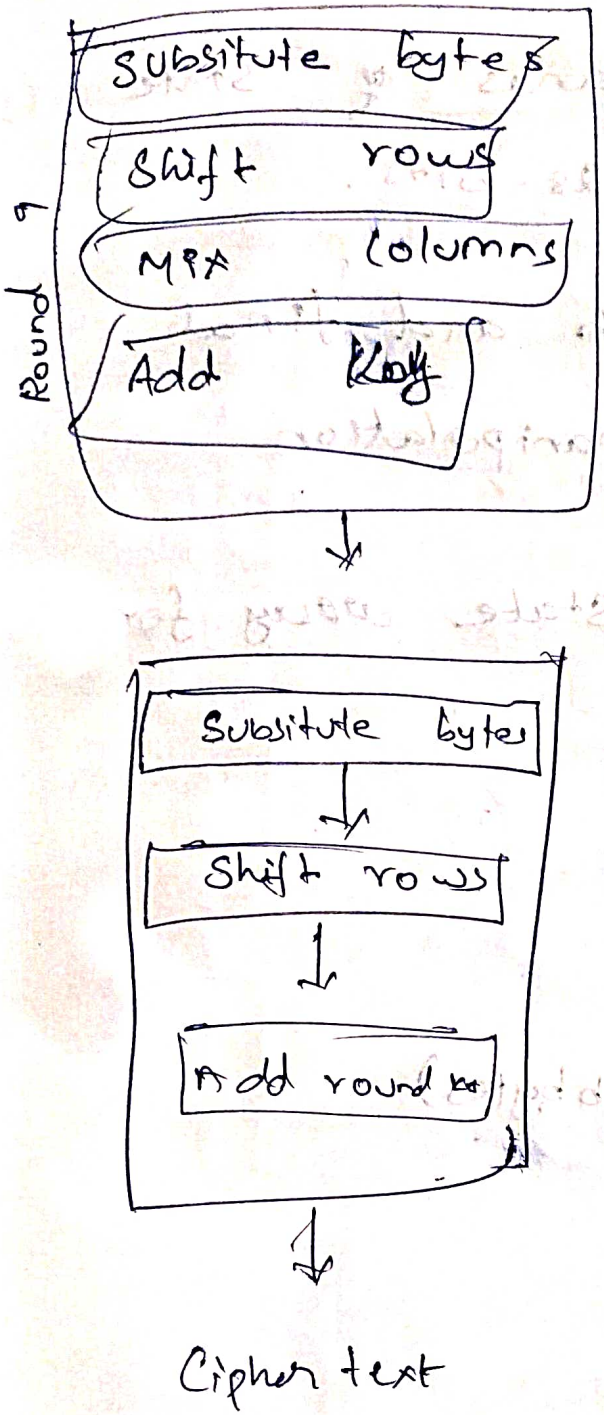
* It uses 10 rounds for 128 bits key

12 rounds for 192

14 rounds for 256-bit

AES Encryption and Decryption:





Steps in Encryption:

* Derive the set of round keys from cipher key
* Initialize plain text
* Add the intial round key to plain text.

* Perform nine rounds of state manipulation for 128-bits.

* Perform the tenth and final round of state manipulation

* Copy the final state array for encrypt the data

Operations of AES.

* Byte Sub Sitiution (Sub bytes)
* Shift Rows
* Mix Columns
* Add Round Key

Byte subsitiution.

* The 16 input bytes are substituted by looking fixed table.
* The result is in matrix of four rows and four columns

3) Euclid's algorithm:

* An Euclid's alogrithm is a method for efficiently finding the greatest common divisor

* The GCD of two integers x and y is the largest number divides both of x and y

* It is also used for finding HCD.

Understanding GCD:

	12	33
Divisors	1, 2, 3, 6, 4, 12	1, 3, 11, 33
Common Divisors	1, 3	
GCD	3	

$\therefore$ GCD (12, 33) = 3

Euclid's Algorithm for GCD:

find the GCD (12, 33)

Q	A	B	R
2	33	12	9
1	12	9	3
3	9	3	0
X	3	0	X

$$\begin{array}{r|l} & 2 \\ \hline 12 & 33 \\ & 24 \\ \hline & 9 \end{array}$$

$$\begin{array}{r|l} & 1 \\ \hline 9 & 12 \\ & 9 \\ \hline & 3 \end{array}$$

$$\begin{array}{r|l} & 3 \\ \hline 3 & 9 \\ & 9 \\ \hline & 0 \end{array}$$

GCD (12, 33) = 3

GCD:

* It is used to find GCD of non-prime numbers

4) RC4.

* It is a type of Psudo random number generator

* It is uses Symmetric Key for encryption

* It was invented by Ron Rives

RC Stands for Ron's Code.

* RC4 is a Stream Cipher

* It is used to generate a Random Number using a Key

* RC4 is Classified into two types

1) KSA (Key Scheduling Alg)

2) Psuedo-Random generation Alg (PRGA).

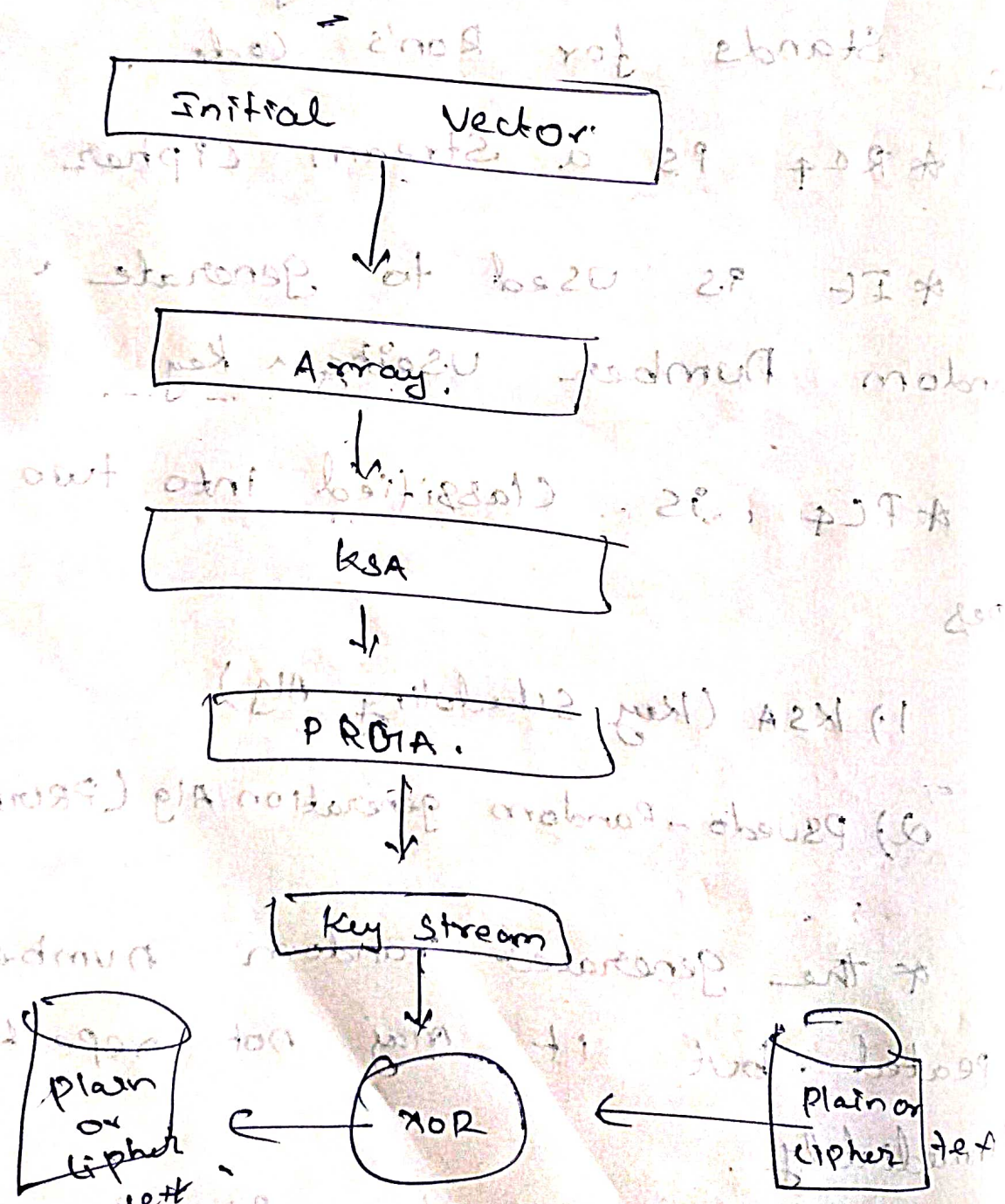
* the generated random number repeated. but it may not repeat immediately.

* Key must be long, It guard against brute force attack

* RC4 is used in WiFi

* Variable key length from 1 256 bytes.

Block diagram:



// generating number.

for

i = 0 to 255

do S[i] = i

T[i] = K[i mod K-len];

---

j = 0 // swapping random number

for

i = 0 to 255

do

{

j = (j + S[i] + T[i]) mod 256;

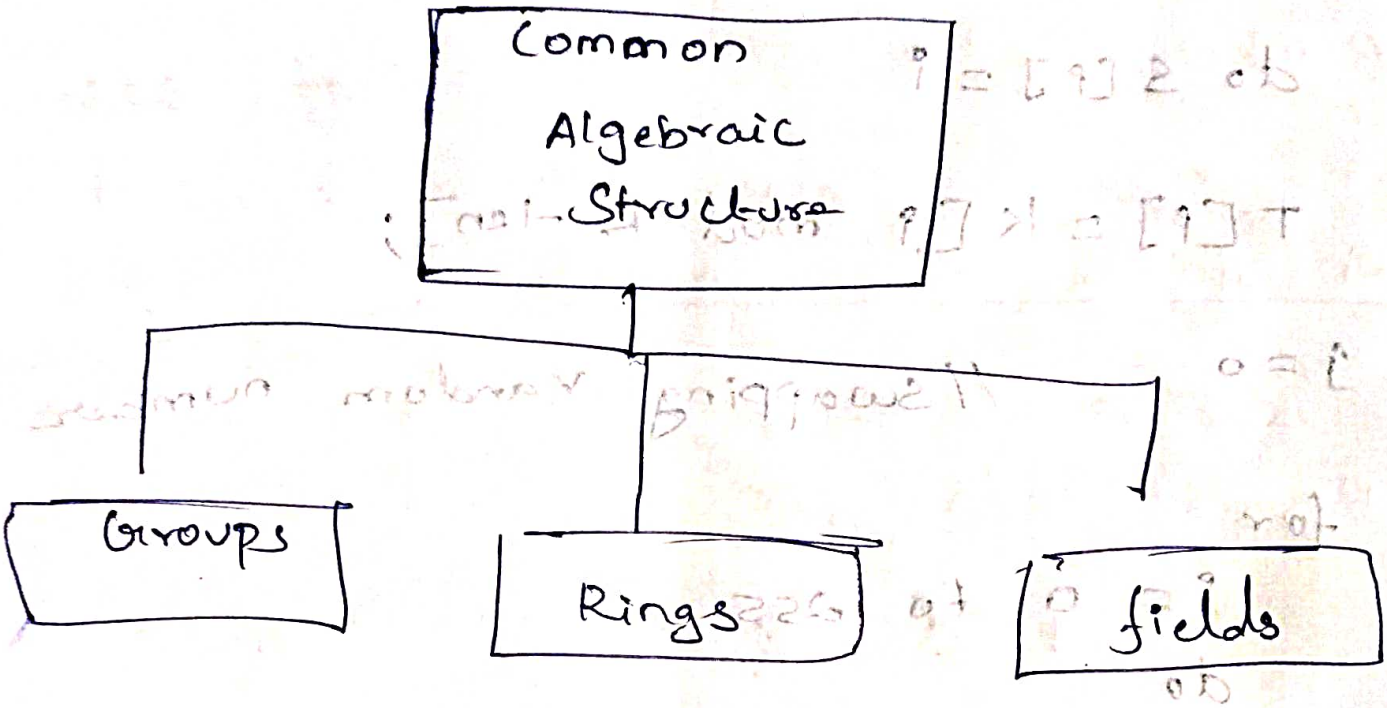
Swap (S[i], S[j]);

}

& MSg can be encrypted using

X-or();

5). Algebraic Structure.



Groups :

Closure property : a and b belongs to G

Commutative ~~Associate~~ property : $a * b = b * a$.

Inverse element = $a * a = e$

Associative property = $(a * b) * c = a * (b * c)$

Ring:

R, +, ×.

+ - addition

× - Multiplication

Fields.

F, +, ×

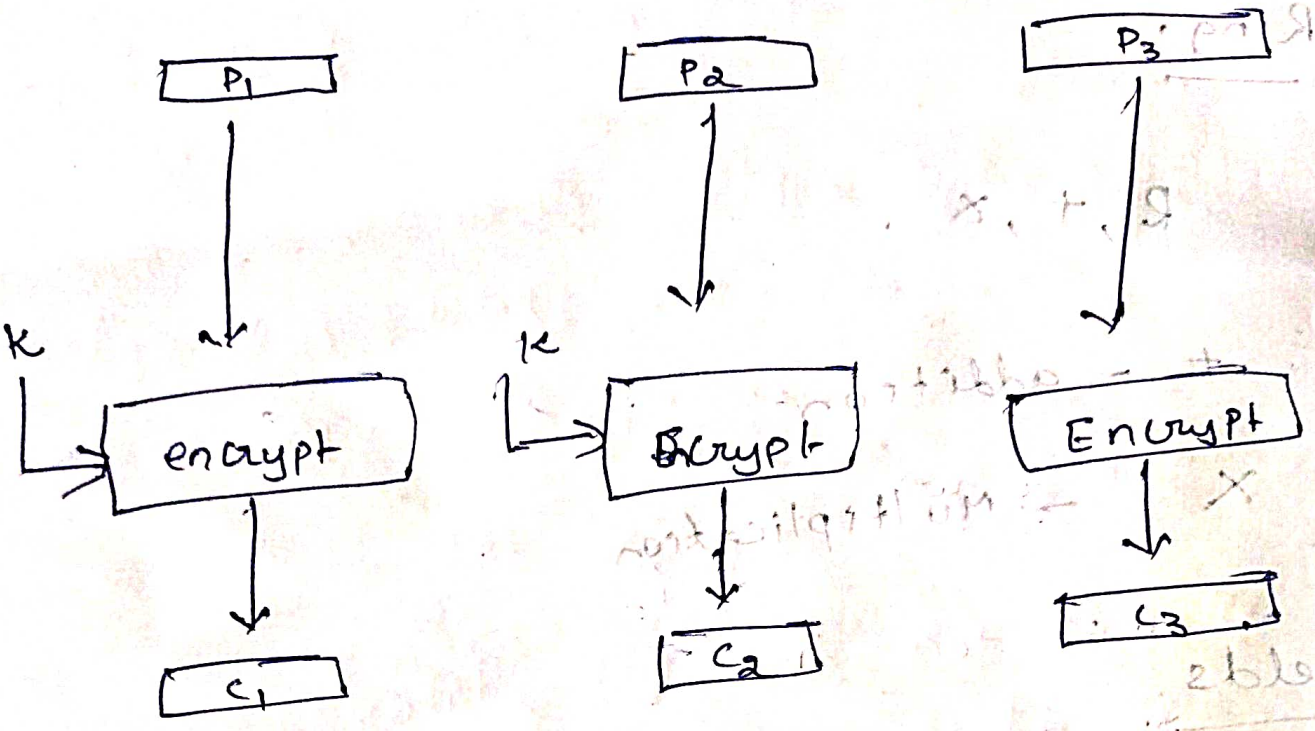
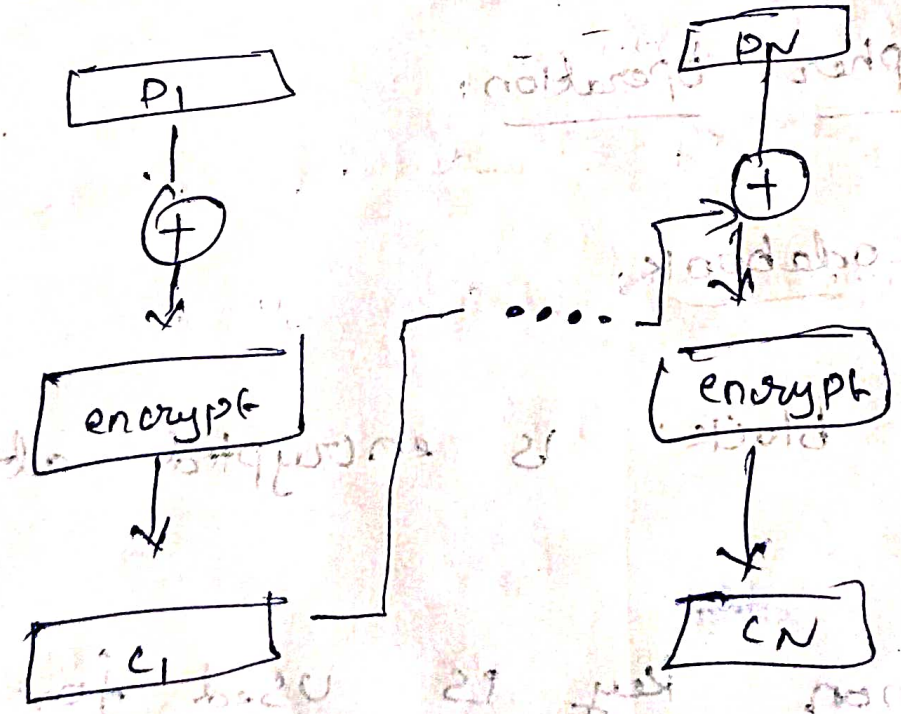
6) Block Cipher Operation:

Electronic codebook.

* One block is encrypted at a time.

* Common key is used for encryption and decryption.

* It is one of technique used in block cipher operation.



2) Cipher Block Chaining Mode: