Cryptography & Network Security.

I) Plain text (P) → Original message

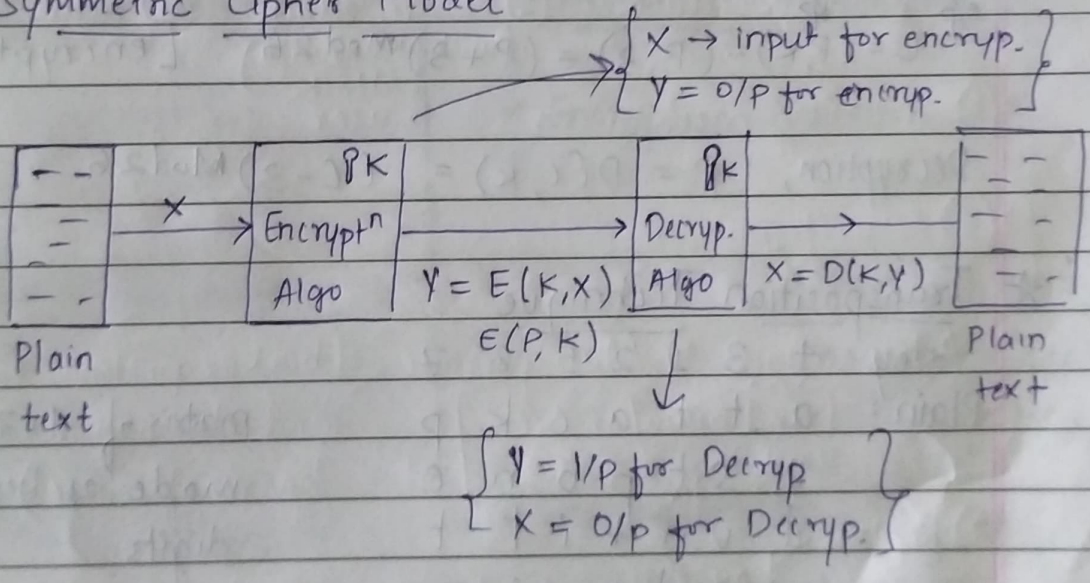
II) Encryption Algorithm (E) → Applied on P.

III) Secret key (K) → technique by which we can convert encrypted message to original form.

IV) Cipher text (C) → After applying encryption on P it is converted into cipher text.

V) Decrypted Algorithm (D) → Reverse process of encryption with the help of key.

★ Symmetric Cipher Model



★ Characteristics of Cryptographic system

① Types of operation } Software
② No. of keys used
③ The way in which the plain text is processed (transmission medium) → hardware

Cryptanalysis

Study of Cryptography

Brute force Attack (cryptanalysis for hackers).

imp Types of Encryption Algo.

1) Substitution Algo 2) Transposition Algo.

★ Substitution Technique

Plain: meet me after the toga party

(Caesar) Cipher: PHHW PH DIWHU WKH WRJD SDUWB

o/p $C = (P, K) = (P, 3) = (P + 3) \bmod 26$ [encryption.

Decryption, $P = D(C, K) = (C - 3) \bmod 26$

★ Transposition Technique.

Key	4	3	1	2	5	6	7
Plain:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	d	a	y	s	z.

matrix of 4x7 is made as key is of 7 digits.

Cipher: ttnd apta tsuo aodw coiy knls petz
(rail fence)

Decrypt^n → arrange according to key, the cipher text in group of 4 words (letters) as matrix, no of times key is used.

Characteristics of Cryptography

It is characterised in 3 independent dimension

① Type of operation used for transforming plain text to cipher

② No of keys used [Symmetric key → both sender & receiver have same key]

[Asymmetric key → both uses different key]

③ The way in which the plain text is processed through transmission media

(Cyptanalysis) Types of attack

Type of attack	Known to Cryptoanalyst
① Cipher text only	* Encryption Algorithm * Cipher text
② Plain text only	— ll — (above 2 points) * One or more plain text, cipher text formed with secret key.
③ Chosen Plain text	* plain text chosen by the cryptanalyst together with its corresponding cipher text, generated with the secret key.
④ Chosen Cipher text	* above 2 points & chosen cipher text.
⑤ Chosen text	* every points aboves.

Network Security's Objectives

1) Confidentiality (for all) ① Data Confidentiality ② Data Privacy (b/w 2 parties)

2) Integrity ① Data integrity (error free) ② System integrity (hardware check)

3) Availibility

4) Authenticity (Verification)

5) Accountability (Responsibility, maintanance)

---

* OSI Security Architecture

① Security attack (silent attack) (direct attack)
- (I) Passive attack (without any info of attack to user)
- (II) Active attack.

② Security mechanism

③ Security services

Active attack 1) Masquerade (hacker pretends to be source and destination can't identify change of source)
(and actual source is not able to perform transfer)

2) Replay → All (the actual source, hacker & destination) communicate & flow the data

3) Modification of Message → Source to hacker to destination single flow & hacker change the actual message.

4) Denial of service → not providing access to user.

Security Services

1) Authentication
   i) Peer Entity Authentication
   ii) Data origin Authentication.

2) Access control → [limited & authorized access to resource]

3) Data Confidentiality
   i) Connection confidentiality → (Physical connection b/w source & destination)
   ii) Connection less confidentiality → (wifi connection b/w 2 party)
   iii) Selective field confidentiality → select the best/optimum path & sending data through it
   iv) Traffic flow confidentiality
      ↳ (While multitasking keeping data confidential)

Data Integrity (adding extra bit for transfer of data)

① Connection Integrity with Recovery → (if data loss occur, it recovery in Physical connection)
② Connection less Integrity without Recovery → (data loss occur, and recovery not done)
③ Selective field Connection Integrity.
④ Connection less Integrity
⑤ Selective field connection less Integrity. (Virtual path data integrity)

Non Repudiation (to not deny; allow it)

1) Non Repudiation origin → (it should allow data transfer)

2) Non Repudiation destination. (it should always receive data (allowed form))

★ Security Mechanism

Specific security Mechanism → security only on specific layer (application or presentation)

Pervasive → applied on all the layer

- Encipherment → encryption
- Digital Signature → for validation purpose ; confirmation
- Access control → limited access to resources
- Data Integrity
- Authentication Exchange → exchange of info among verified users to prove authenticity of user
- Traffic padding → filling gaps blw data flow to distort the traffic analysis attack.
- Routing control → router path security processing
- Notarization → Trusted third party (using for data exchange)

Pervasive Security mechanism.

1. Trusted functionality → every components, layer must be trusted, authentic
2. Security label → verification tag, number, Id
3. Event detection. → security related event detection

④ Security Audit Trail. → record of every security mechanism used. (status)

⑤ Security Recovery. → if problem occurs in security then we have to recovery & operate on it again.

UNIT-2

Stream Cipher (single character encryption)
Block Cipher (grouped character encryption)
↳ in Block Cipher bits are selected then the given 2 mappings are done

★ Reversable Mapping (long distance, strong message)

n = 2 bits no of combinations → 2^n

Plain text	→ Cipher text.
0 0	01
0 1	10
1 0	11
1 1	00

{ Encryption process }

{ cipher text selection is based on the user

★ Irreversable Mapping (for short distance, weak message)

n = 2 bit for given example combinations = $2^n - 1$ (variable acc. to user.)

Plain text	Cipher text.
00	01
01	10
10	00
11	00

} 2 can be same but it is not that secure way.

During decryption

Cipher text	⟶	Plain text
01		00
10		01
11		10
00		11

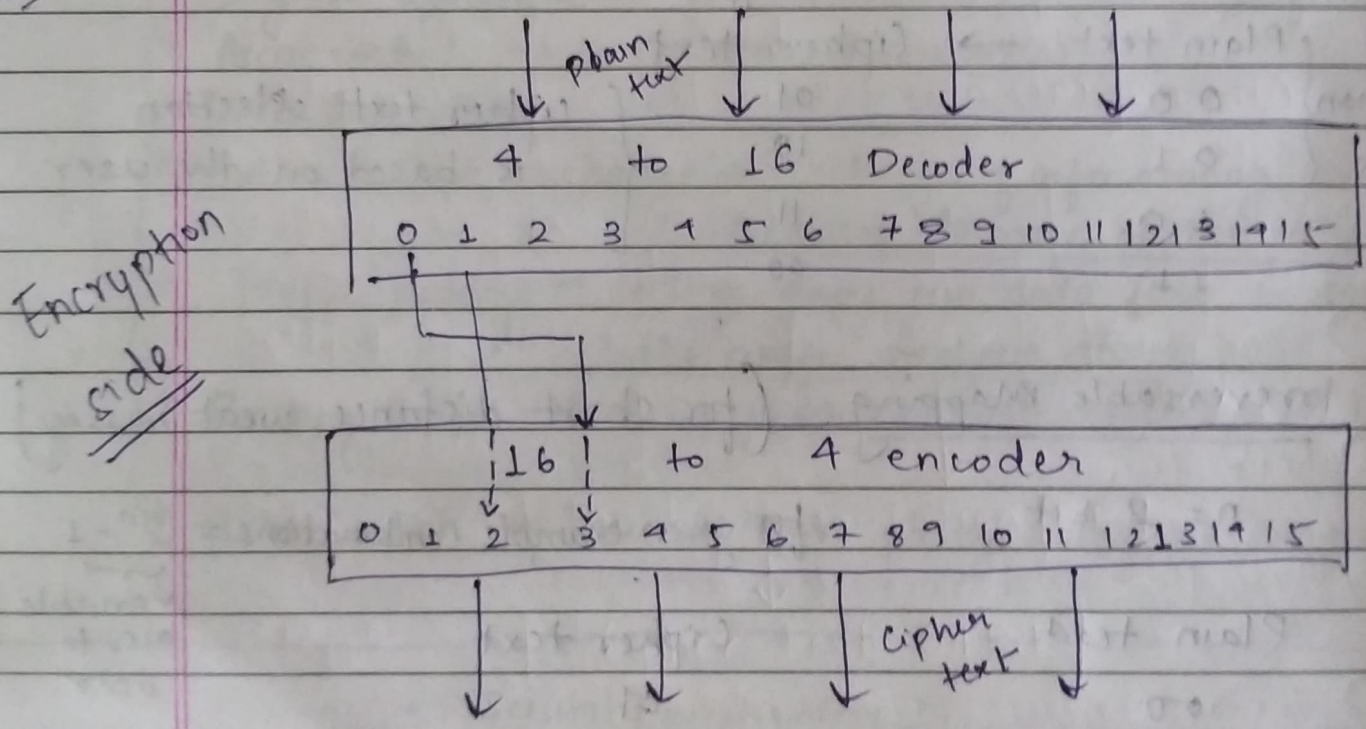
Values taken from same table of encryption sort of key.

Required Key length = $n \times 2^n$

for a single input ~~64~~ $n \times 2^n$ keys option.

for $n = 64$ key = $64 \times 2^{64} = 2^{70}$ or 10^{21}

imp Hardware Structure (Ideal Block Cipher)

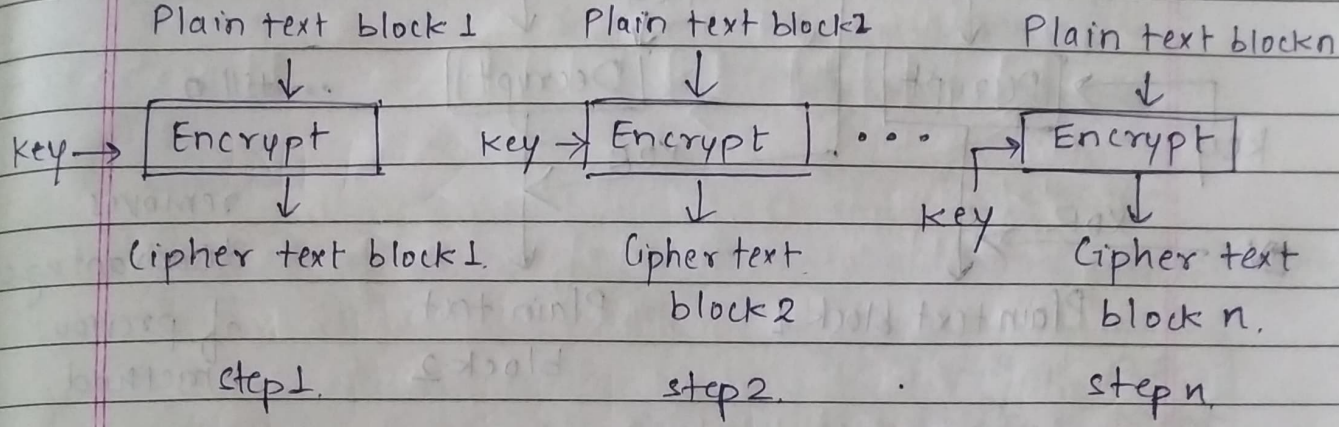


	plain		cipher
here	0000	→	0011
	0001	→	0010

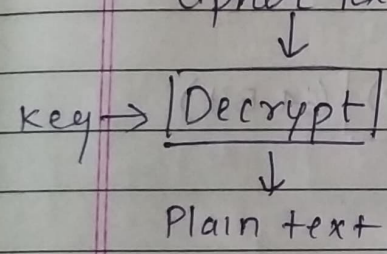
2 tables, 2 diagram for complete ideal Block Cipher

Algorithm Modes → (Block Cipher)

1) Electronic Code book (ECB) Mode :-



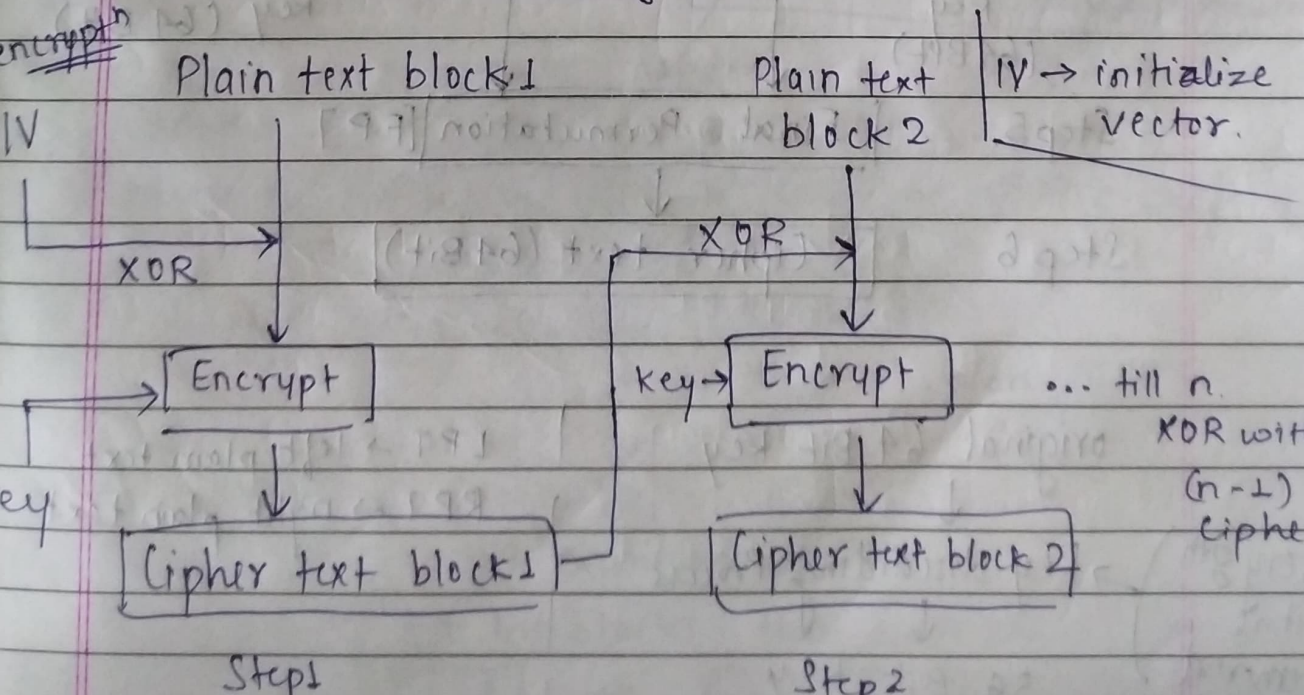
Decryption part.



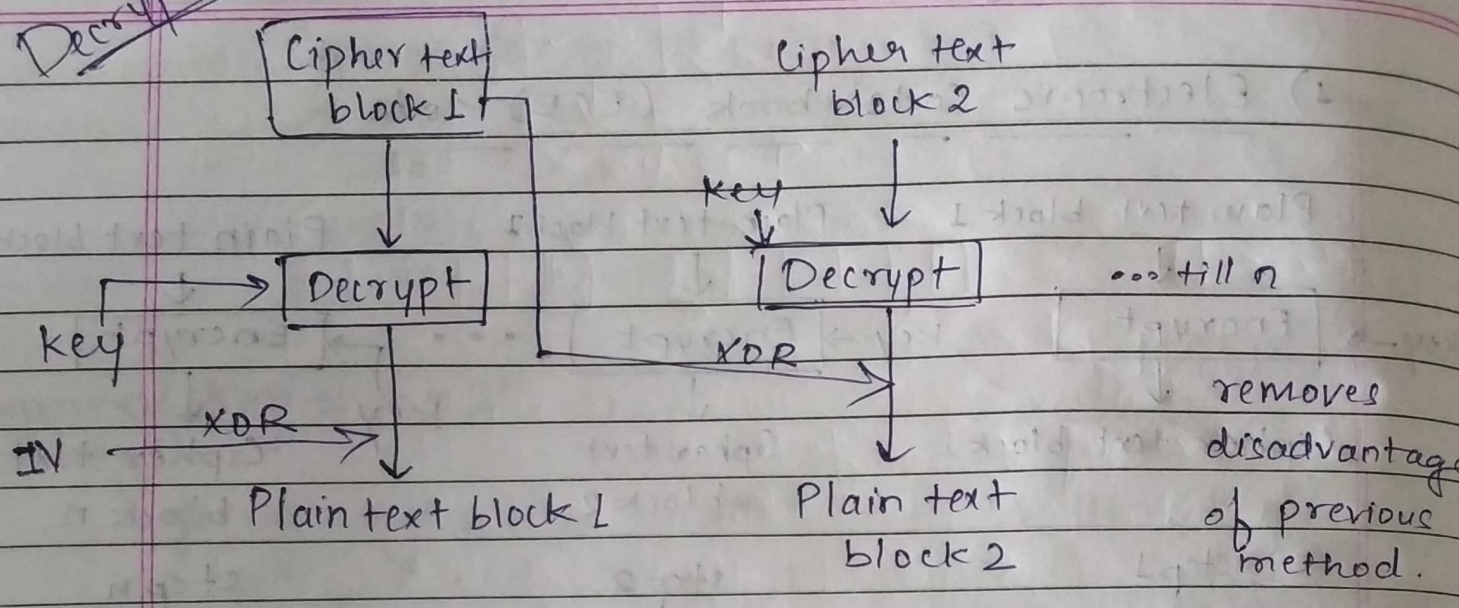
... till n.

Disadvantage
→ for same plain text same cipher text is generated.

2) Cipher block chaining Mode (CBC)



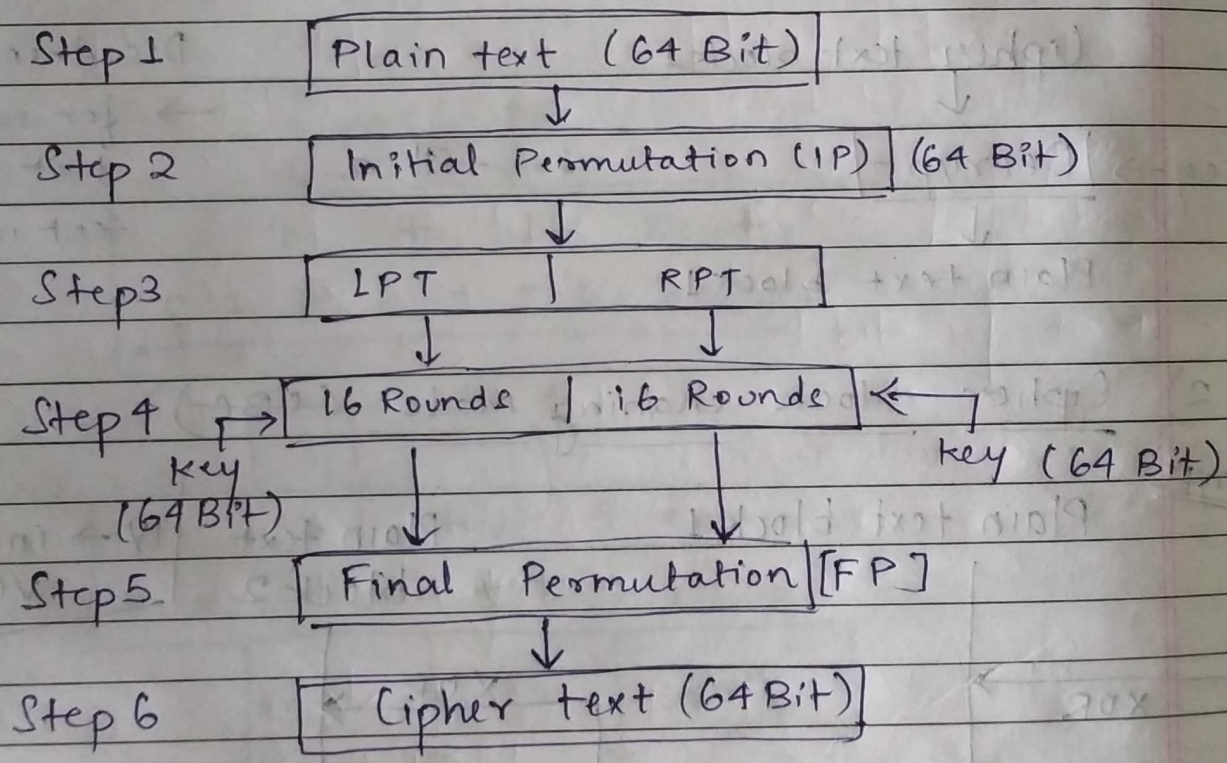
Decryption



removes disadvantage of previous method.

imp

* DES (Data Encryption Standard)



original 64 Bit key

(every 8th bit is removed) → Key discarding Process

56 Bit key.

LPT → left plain text

RPT → right plain text

64 Bit plain text

1 2 3 45. . . .
. 64

↓ IP

58-50 . . .
7

transposition process
(random order change of bit via permutation)

~~transportation process~~

Rounds

key transformation

↓

Expension Permutation

↓

S-box Substitution

↓

P-box Permutation

↓

XOR and swap

Key transformation

by key discarding process (56 Bit)

56 → | 28 Left key | 28 Right key |

Left circular shift of bit in the 28 Bit left key & right key.

↓

48 Bit key
[random discarding of 8 Bit]
compressed permutation

(Step 4) Round 1-2-9-16 (1-Bit shift)

~~Remaining~~ Remaining Rounds perform 2 Bit shift.

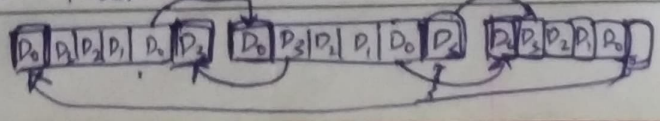
Expension Permutation

We work on RPT

LPT (32 Bit)	RPT (32 Bit)

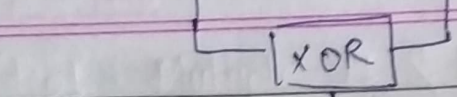
↓ expanded into 48 Bit

32 ÷ 8 = 4 bit blocks then each has 2 extra bit

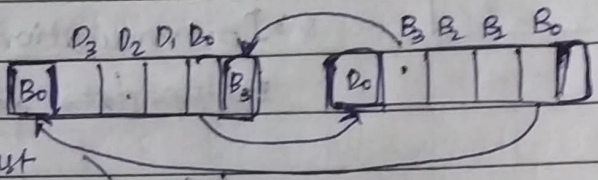
as [ ] → 

& RPT 48 Bit

key 48 Bit



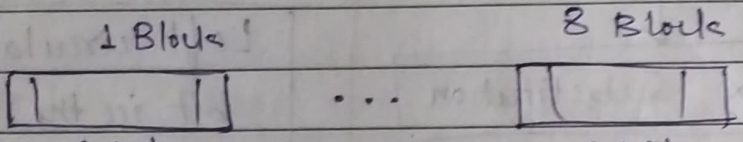
48 Bit O/P

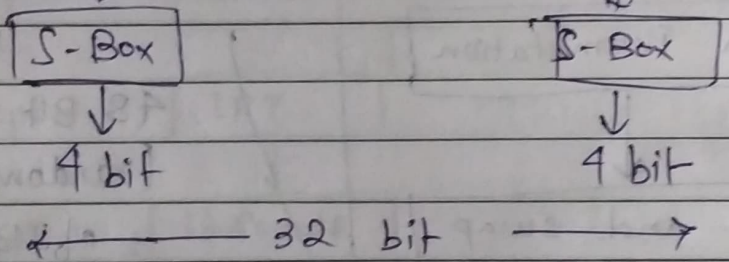


last bit of last block

switch of D_0 & D_3 for extra addition of bits

S-box Substitution





P-box Permutation

32 bit RPT

Permutation

32 Bit RPT

XOR and SWAP

LPT & RPT (both 32 bit)

XOR

After XOR swap LPT & RPT.

Final Permutation → Cipher text.

* IDEA (International Data Encryption Algo)

↓

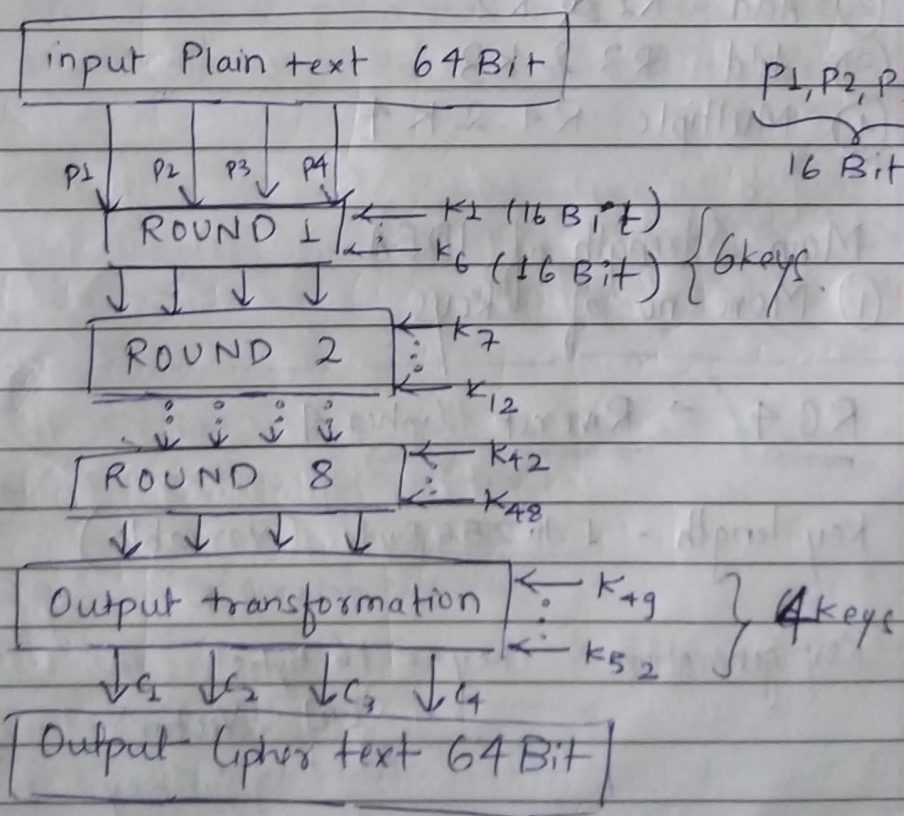
Plain text size = 64 Bits block

key size = 128 Bit

DES is more popular as it is patented as less complexity than IDEA.

no of Rounds = 08

Broad level stages of IDEA



Steps in Round

Step1 : Multiple P1 & K1
Step2 : Add P2 & K2
Step3 : Add P3 & K3
Step4 : Multiple P4 & K4
Step5 : XOR the result of step1 & 3
Step6 : XOR the result of step2 & 4
Step7 : Multiple the result of step5 with K_5.
Step8 : Add the result of step6 & step7
Step9 : Multiple the result of step8 with K_6
Step10 : Add the result of step7 & step9
Step11 : XOR the result of step1 & step9
Step12 : XOR the result of step3 & step9
Step13 : XOR the result of step2 & step10
Step14 : XOR the result of step4 & step10

Output transformation

1. R1 & K1 Multiple
2. Add R2 & K2
3. Add R3 & K3
4. Multiple R4 & K4.

Main Strength of IDEA
1. More no of keys

RC4 → Riverst Cipher 4

Key length - 1 to 256 Bytes (variable)

Key generation : key = 16 Bytes
= S[0] } (Vector)
S[1] }
:
S[15] } Subkey

Steps

i) initialization - key is converted into subkey
ie S[0], S[1] ... S[15] if key = 16 bytes

ii) stream generation → by using Encryption Algo
(XOR b/w plaintext & subkey)

inf

RC5 (2)

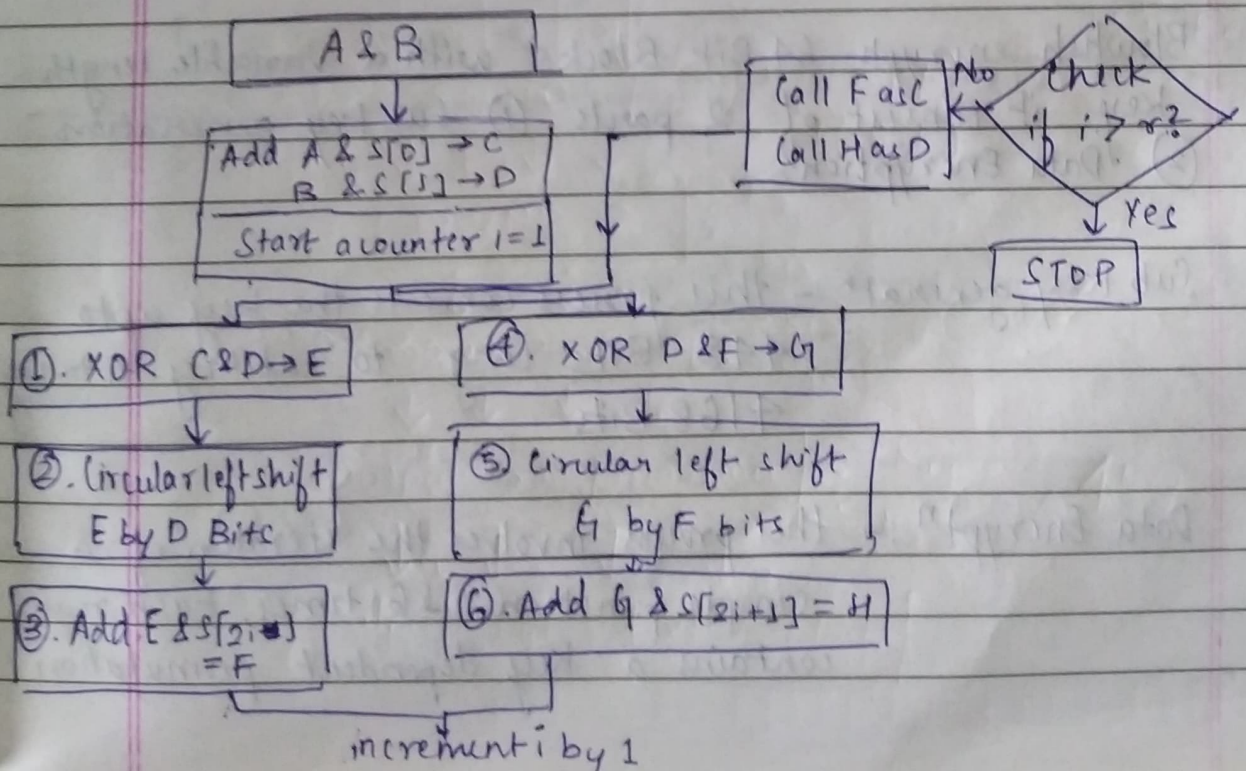
Basic Principle of RC5

(1) The plain text block size can be of 32 Bit, 64 Bit, 128 Bit [since 2-word block size is used]

(2) The key length can be of 0 to ~~256 B~~ 2040 Bit [0 to 255 Byte]

(3) No of Rounds = 0 - 255

(1) Divide the original plain text into 2 equal part A & B
(2) Add A & S[0] to produce C & B & S[1] to produce D



imp Blowfish Algorithm

Introduce by Bruce Schenier

Characteristics:-

① Fast → Blowfish encryption rate on 32 Bit Microprocessor is 26 ~~Blocks~~ Clock cycles per Byte.

② Compact → Blowfish can execute in less than 5KB memory

③ Simple → Blowfish uses only primitive operations such as addition, XOR, and table look up making its design and implementation very simple.

④ Secure → Blowfish has a variable key length upto a max. of 448 Bits longs making it both flexible & secure.

Operation

Blowfish encrypts 64 Bit Blocks with a variable length key it consist of 2 parts ① Sub key generation ② Data Encryption.

Sub key generatⁿ :- this process converts the key upto 448 Bits long to sub key totaling 4168 Bits

Data Encryptⁿ :- this process involves the iteration of a simple function 16 times. Each round contains a key dependent permutation

and key & data dependent substitution.

Sub key generation

1) 32 Bit to 448 Bit
   two word.

K_1 = 32 Bit (two word)
K_2
⋮
K_{14}

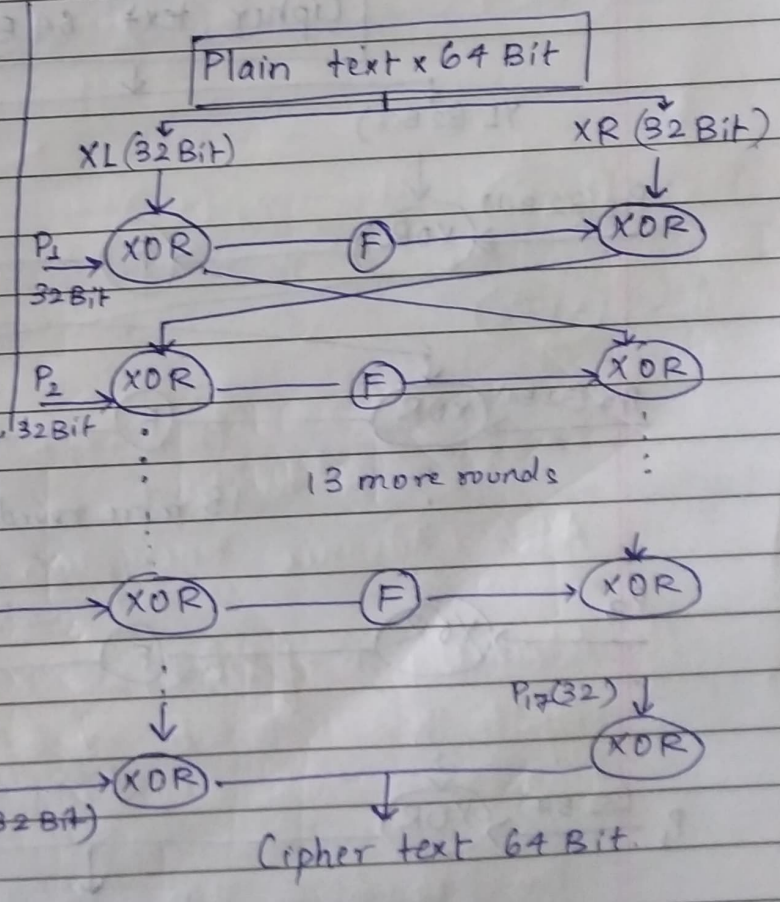
$n \leq 14$

ii) P-array (18 × 32 Bit subkey).
$P_1, P_2, P_3 \ldots P_{18}$

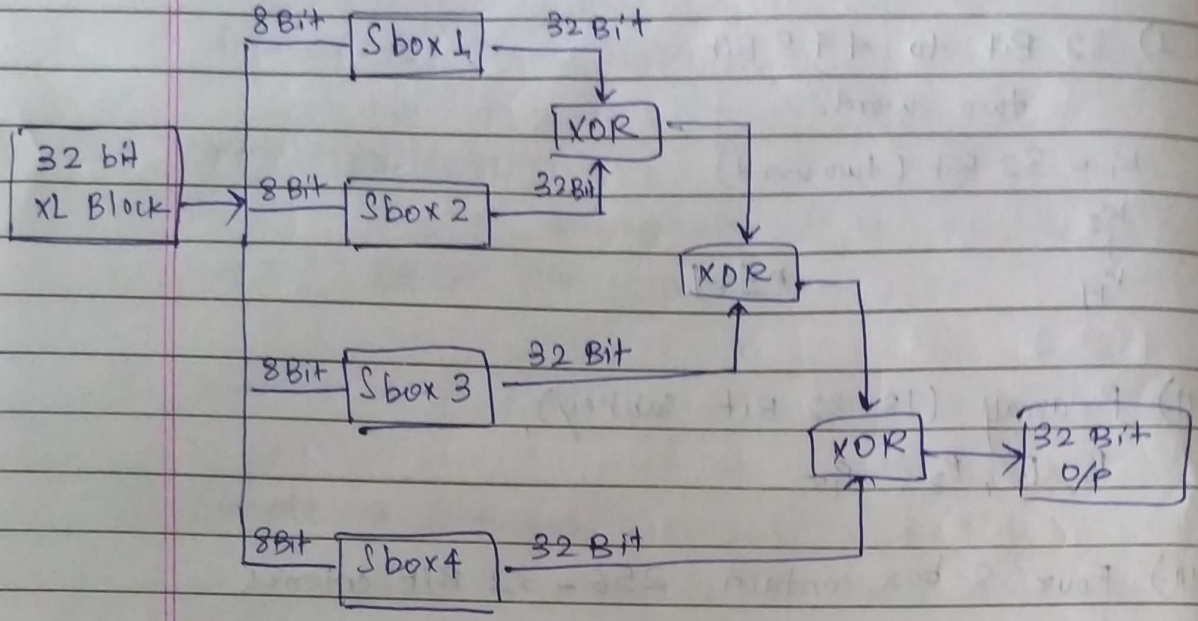
iii) Four S-box contain 256 - 32 Bit enteries
$S_1, 0, S_1, 1, \ldots S_1, 255$
$S_2, 0, S_2, 1 \ldots S_2, 255$

upto P_{14}

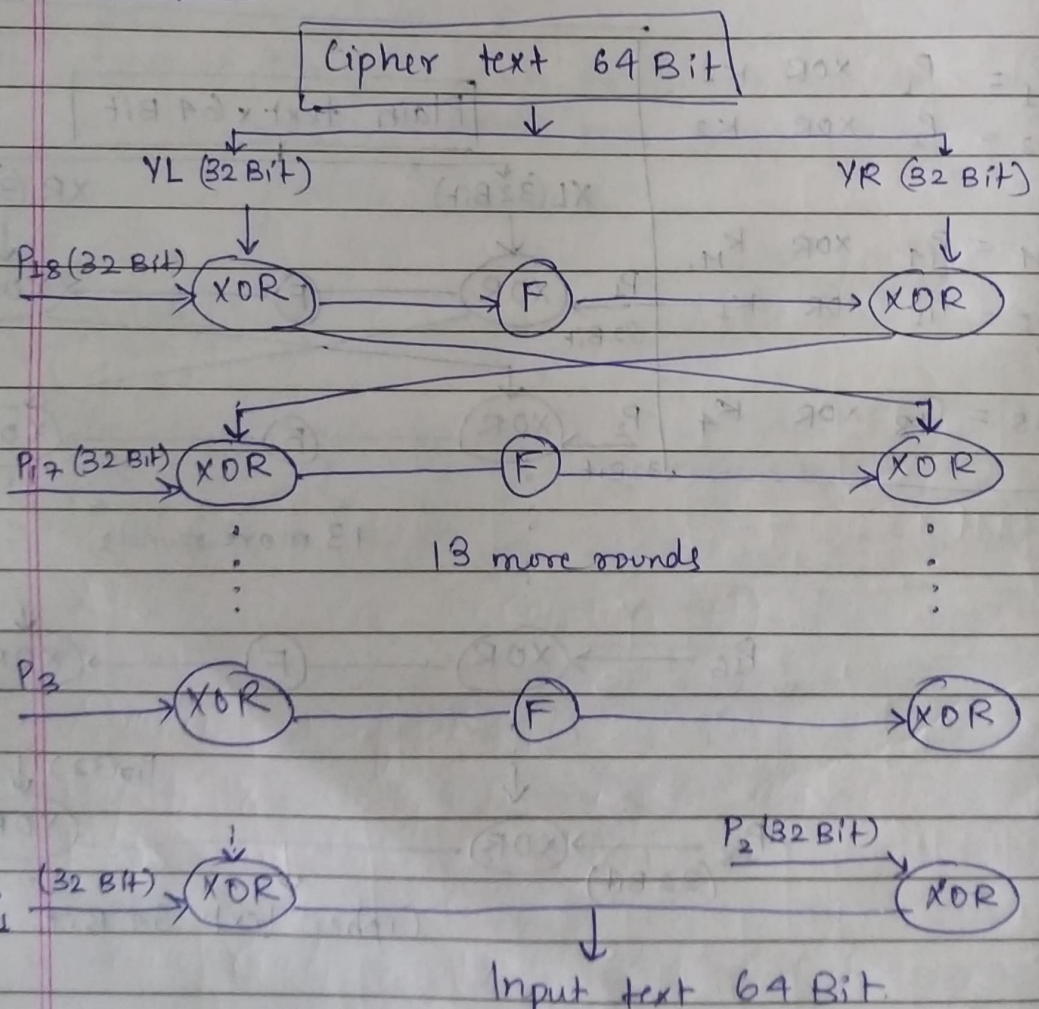
$P_1 = P_1$ XOR K1
$P_2 = P_2$ XOR K2
⋮
$P_{14} = P_{14}$ XOR K_{14}.
$P_{15} = P_{15}$ XOR K_1
⋮
$P_{18} = P_{18}$ XOR K_4



inside F



Decryption



"Rijendel" is another name of AES method

Operation or Description of Algo.

① Do the following one-time initialization process.
a) Expand the 16 byte key to get the actual key block to be used
b) Do one time initialization of the 16 byte plain text block (called state)
c) XOR the state with the key block.

② For each round, do the following.
a) apply s-box to each of the plain text block.
b) Rotate row k of the plain text block (i.e state) by k byte
c) Perform mix column operation.
d) XOR the state with the key block.

Procedure

①

→ first make all 4x4 matrix $\begin{bmatrix} : & : & : & : \\ : & : & : & : \\ : & : & : & : \end{bmatrix}_{4\times4} = 16$ bit

16 bit x 11 = 176 bit → Actual key block.

→ Also make 8, 4x4 matrix of plain text we will get.
16 x 8 (state) = 128 bit.

→ XOR new state x actual key.

② Apply S-block.

$$\begin{bmatrix} 2 & 3 & 4 & 5 \\ 9 & 8 & 7 & 6 \\ 10 & 11 & 9 & 8 \\ 10 & 11 & 13 & 15 \end{bmatrix}$$ ← state

k = no of round.

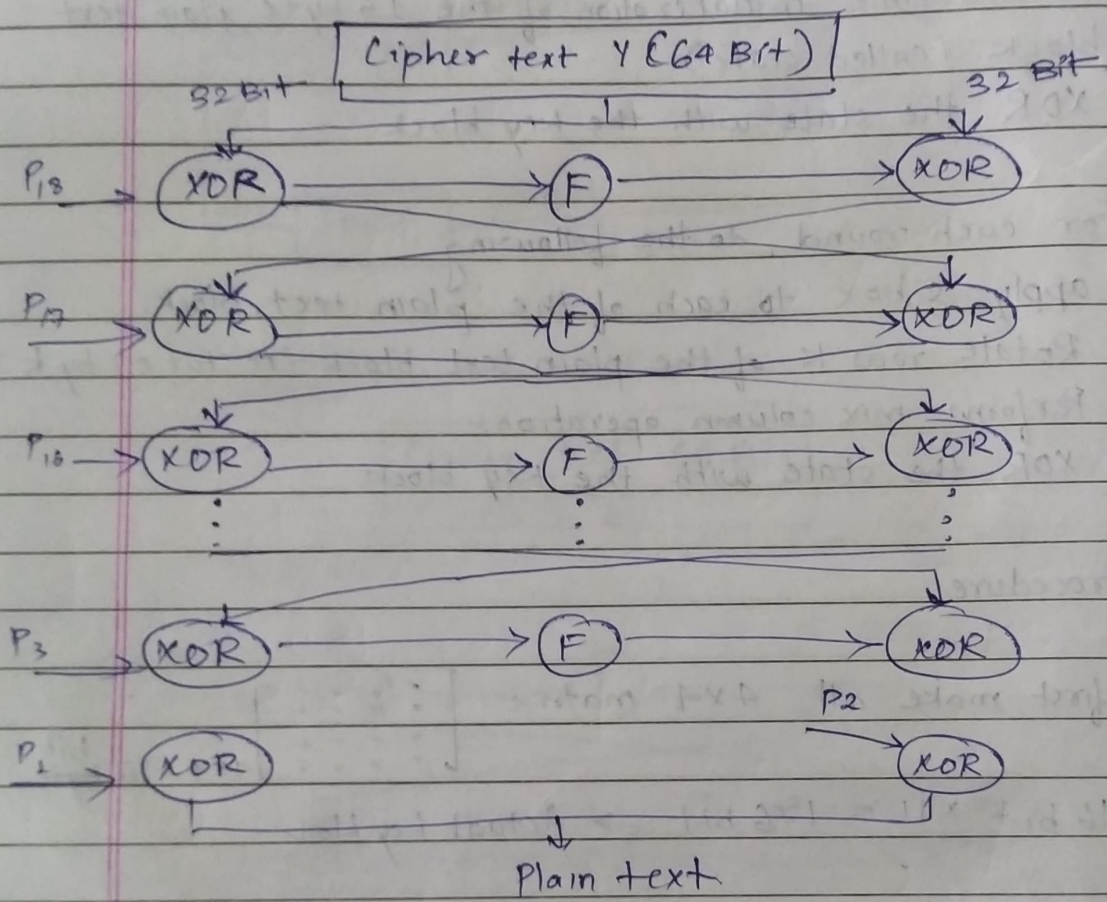
Rotation → rotate K row by K byte. we get for 1st round.

$$\begin{bmatrix} 5 & 4 & 1 & 2 \\ 9 & 8 & 7 & 6 \\ 10 & 11 & 9 & 8 \\ 10 & 11 & 14 & 15 \end{bmatrix}$$

→ Random changing of column

→ XOR state with key

Decryption procedure



AES (Advance Encryption std)

Advance part of DES

Key length = 128 Bit or 256 Bits

Plain text block = 128 Bit.

no of rounds = 10 (for 128 Bit key)
= 14 (for 256 Bit key)

imp

RSA Algo.

Description → ① Choose 2 large Prime no P & Q

② Calculate $N = P \times Q$.

③ Select the public key E such that its not a factor of $(P-1) \times (Q-1)$

④ Choose the private key D such that the following eqn is true. $\boxed{(D \times E) \bmod (P-1) \times (Q-1) = 1}$

⑤ For encryption calculate the cipher text as follows

$\boxed{CT = PT^{E} \bmod N.}$

⑥ Then send the CT to receiver (CT = cipher text)

⑦ For Decryption, Calculate,

$$\boxed{PT = CT^{D} \bmod N}$$

ample

Q $P = 7$, $Q = 17$.

$N = 119$

E ≠ factor of 96 => $E = 5$.

$(D \times 5) \bmod 96 = 1$.

$D = 77$

Let $PT = 10$.

$CT = 10^{5} \bmod 119 = 40$

$PT = 40^{77} \bmod 119 = 10$

83
120 | 100000
960
400
360
400