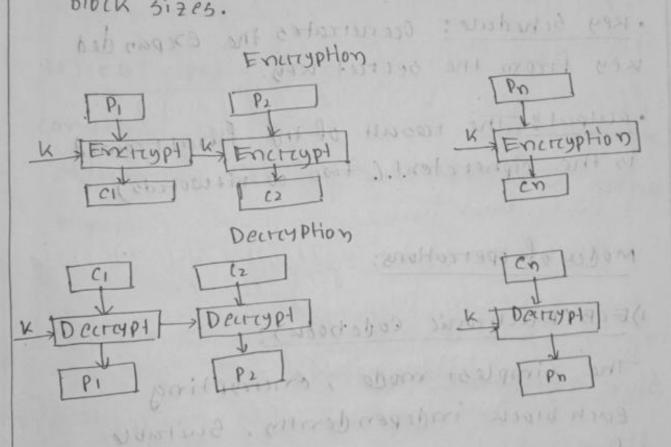
Port its simplicity and flexibility in key and block sizes.

Ministry Wireday Skifts Theor Operation



PCB Block Diagramo

- · Input! The plaintent is divided into two worlds (w bits each)
 - Combined with a portion of the Expanded

- exor and Retations) are applied iteratively in multiple trounds.
 - " key schedule: ocenercates the expanded key from the secret key.
 - is the cipheratent (two w-bitwords)

Co11415159

Modes of opercations:

1) ECB (Eleitronic Codebook):

each block independently, Suitable
Pote short, random data but can a
treveal patterns in non-trandom

(i) CBC (ciphera Block chaining).

Each block is xored with the pravious cloherctent block before encryption.

Providing better security than ECB

111) OFB Coutput Feedback):

the key stream, marking it suitable fore noisy channel.

W) (FB (ciphere feedback):

converts the block ciphere into a stream
ciphere by Feedingback previous ciphereten
blocks.

N) Counter (CTR):

Uses a counton to generate the key stream allowing for parcalled energytion and decreption.

A: (((Cholos) RS) 7 CASTO & CASTO 7) = 1 EVINA.

101 f = 2x(n);

6 - xun f miner 1;

6 - xun f in (+1);

7 - xun f in (+1);

7 - xun f in (+1);

8 - xun f in (+1);

9 - xun f in (+1);

10 - xun f in (

Dava implementation of RC5%

when the previous ciprorings billion import Java nio. Byte Buffett; import Java util Artrays; James Coise

Public class Res 1 (Stradbar Siriais) 8 75 (6)

Pruvate Anal int w= 32;

private Anai totape 12/19/19 soft atmosphere

Provate final int b = 163

provate final inters;

provate final intpu = 0xb7e15163, QW=0x9e37798 SCATIL STATERNAL (

Public RIS (bytto [] Key) }

Inti = (key. length +3)/1/2 3107 grissills

dinte 3 213 new intect; colleges soll

forc lint 1=0; 12 key. length; i++)

L (1/4] 1 = (CKEY Eiz & OXFF) 4 (8 * (10/04)));4

int t = 2*(p+1);

5= NEW INTEKJ;

5[0] = PW;

Porclin+ (=1; (2+; 1+))

SEIJ = STI-17+4W; 4

```
int A=0) (B=0) (=0) 5+951009 11114 1114 1114 11
Int v=13 ×1 (Math = max(c)+1) stated - magado = A
FORE ( IN+ 5=0; 524; 547)
A = SEIZ = Integer. Morateleft ((SEIZ+A+B),3);
B = L[j] = Integer : trotateleft((L[i] +A+B), (A+B));
 i = (i+) > 1/26 to to a possent of or more brown to a side of
 J = (3+1) 0/01; " a page 1 kast to mask in a kast in Jahrd
                      PCE VIE - NEW PCE(VCT);
public, Inter encrept (Interpt) 1 1111
int A = P+EOI+ 5 EOI; calcing 1) thoing too materd
PIRITATION ( ELECT ELECTION )
 Forz Cint 1=1 3 it= pint+ 1 to - lead model = Ital
 A= Integer rotate Left (ANBIB) + 5[2+1];
B = Integer. Hotateleft (BNA, A) + 5[2*1+1];
 tretures news intfo d A183; & = haramond Fitter
public Intia decrept Chitiactal
in+A= C+[0];
                              Surrey output; Lin
 in+B= (+[1])
 Port (1=n; 1>=131=01946 8£12164 3 + 491011919
                              Decre 1 2 421 97 1139
```

B = Integer. Protate Right (B-902*i1) A) ^A; A Integer. trotate Right (A-502*i1) B; G

A = -= 501;

B = -= 501;

teturen new Int [] d. A. B. S. G.

Public Static void main (String [] arcgs) {

byte [] Key = "Mysectre+Key 12345" getBytes();

RCS PCS = New PCS(Key);

bystem out printf ("Plaintent: 9008x 0/08x10",

Plaintent [0], Plaintent[1]);

System out prantf (" Encrypted: 0/008x 01,08x")

Clovertent of illoher tent [1];

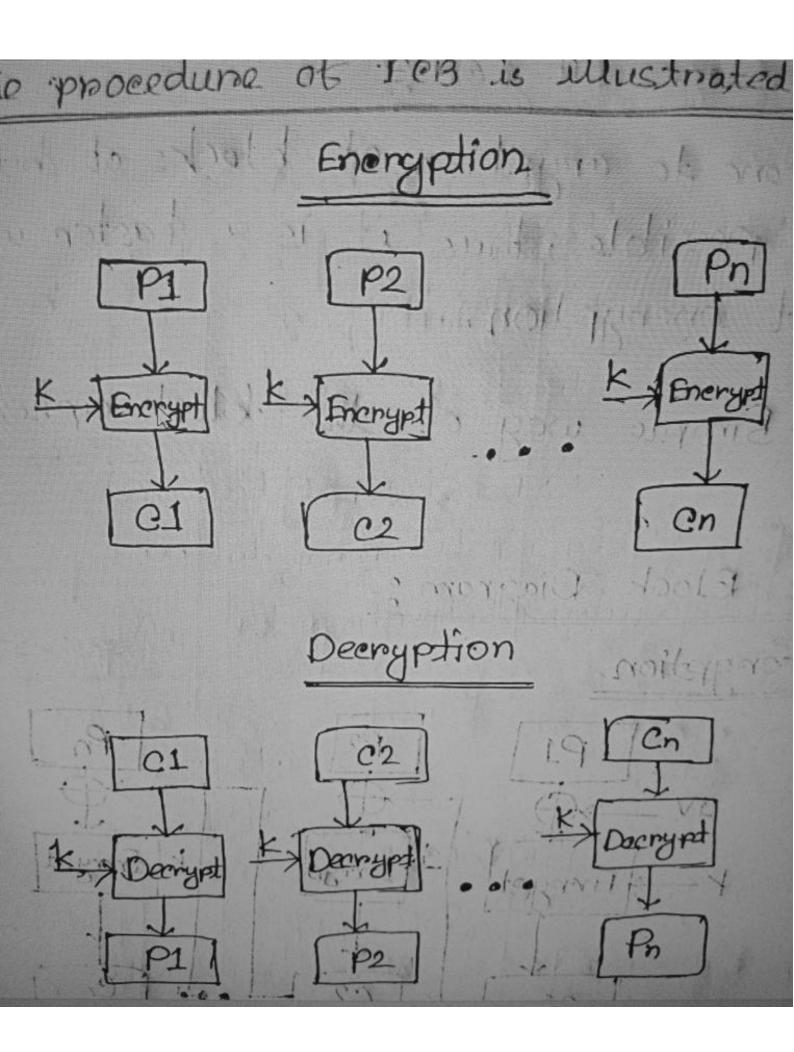
int[] decrypted = riis decrypt ((Ipherstent);

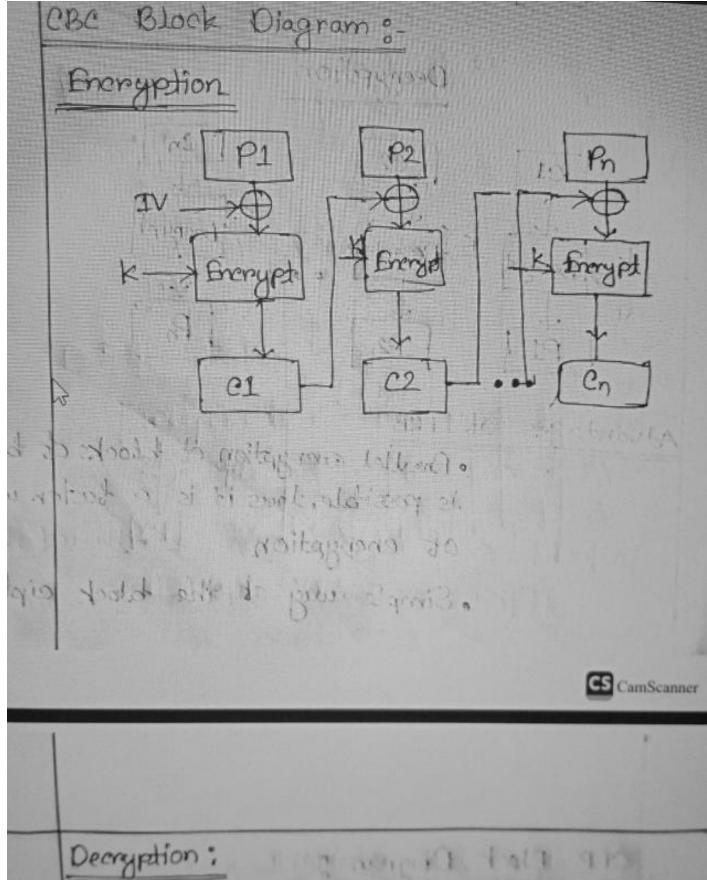
575tem out printf ("Decrypted: %0.08 x 1008 x

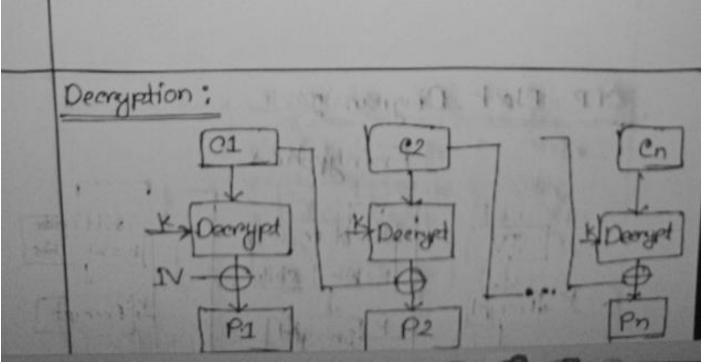
([]] = 9 +0

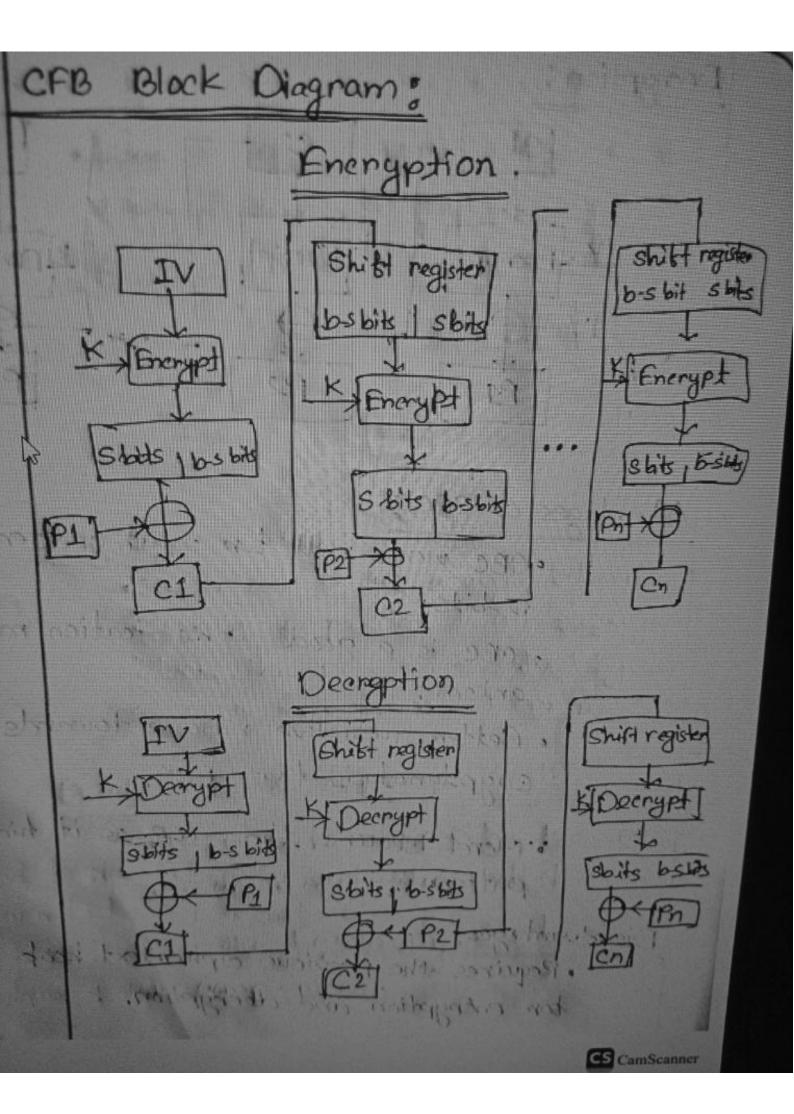
Bumple output:]

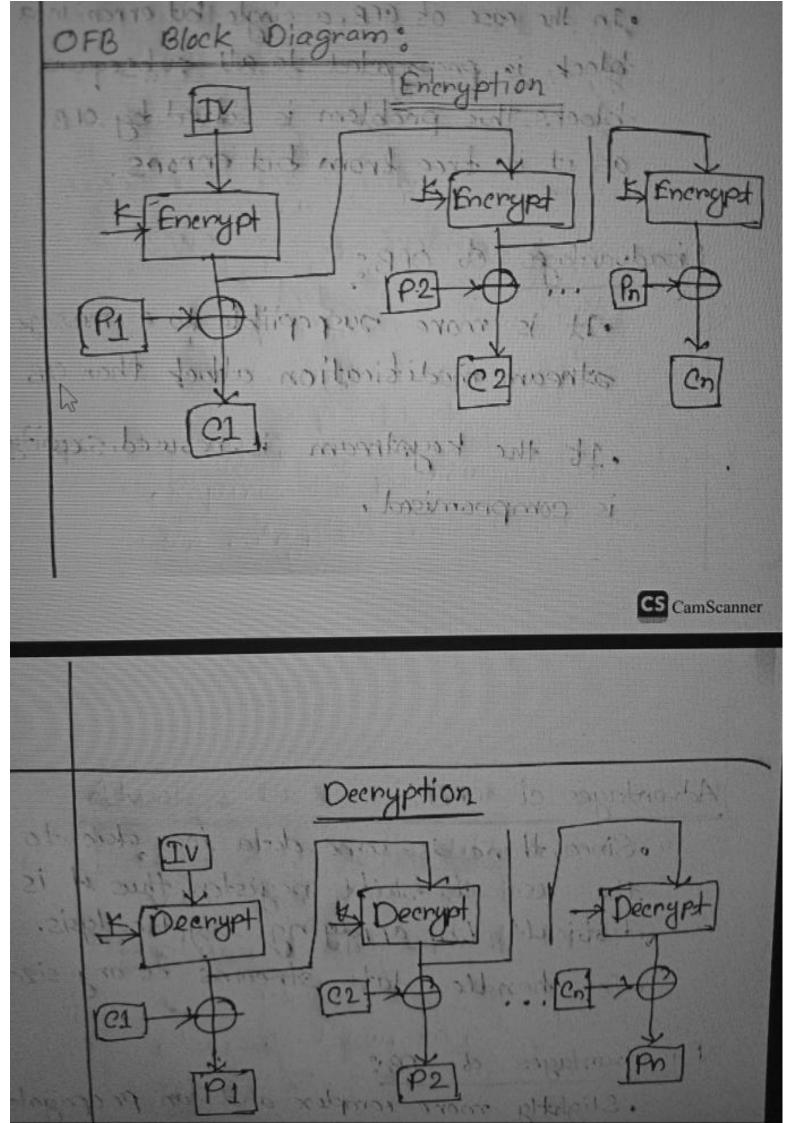
plaintent: 12345678 9AB(DEFO Encrypted: E2(3456 5E91A7B9 Decrypted: 12345678 9AB(DEFO

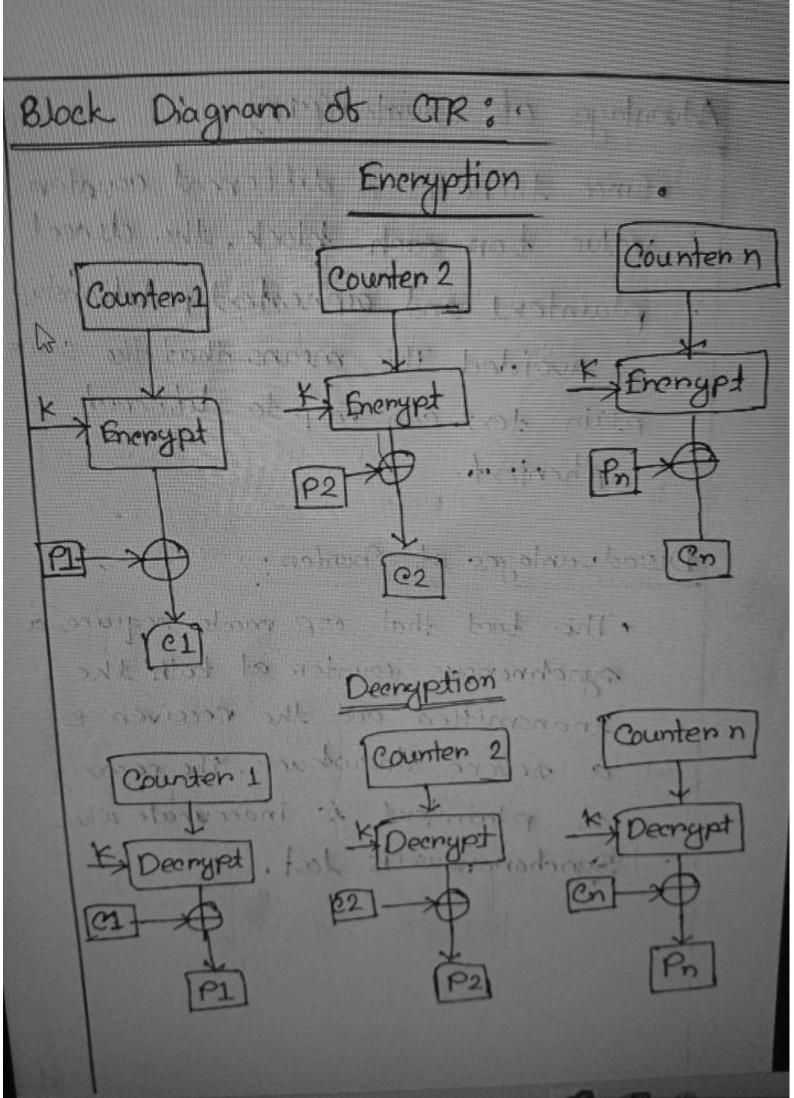






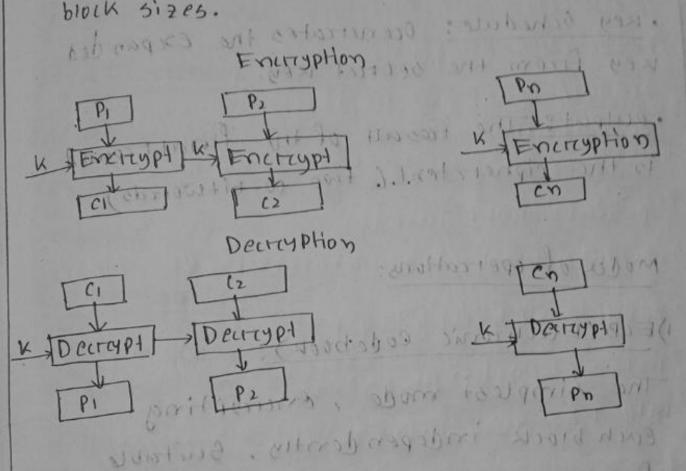






RC50 is a symmetric block ciphen known Port it's simplicity and Alexability in key and block sizes.

a mission of the color state of men competer



PCB Block Diagramo

- · Publication of manual too parties. The Plaintent is divided into two Worlds (w bits each) was rivings) ago (i)
 - · Initial Key Addition to The input worlds Combined with a parthon of the expande Key much (His mose stated burgers

- · Mining Icitaculari-shifts These operations

 (XOR and Retations) are applied iteratively

 in multiple trounds.
 - key schedule: ocenercates the expanded way from the secret key.
 - · output: The trosult of the final round is the cipheratent (two w-bitwords)

modes of opercations:

1) ECB (Eleitronic Codebook):

each block independently, Suitable

Porc short, random data but can a

reveal patterns in non-trandom.

(i) CBC (ciphere Block chaining) ...) chows

clonerations block before encryption.

Providing better security than ECB

111) OFB Coutput Feedback):

Uses the pravious cipheretext block to generate the key stream, making it suitable for noisy channel. (2400-1014-11-10-00-06- 10-10900)

W) (FB (cipheir Feedback):

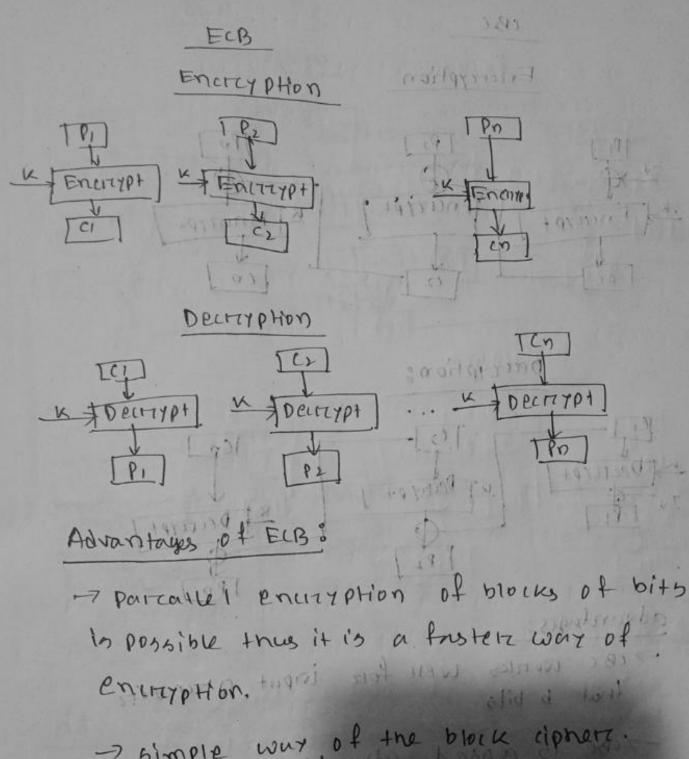
on test land almoving convertes the block ciphere into a stream cipher by Feedingback previous ciphereter califor family atavisia PICHALL TIMES TO PERSONELLES GULLONS STAND

N) Counter (CTR):

PRINCE RES (PAIRE I PER) \$ allowing for parcallel energytion and SENT FOR MIN decreption.

\$ (+5) 6, attacks - 63 x x (0=1 +01) 2003 1. (((4,101) # S) 21 (14×0 % F136273) -1 FDXIST

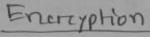
CHATE =) fort

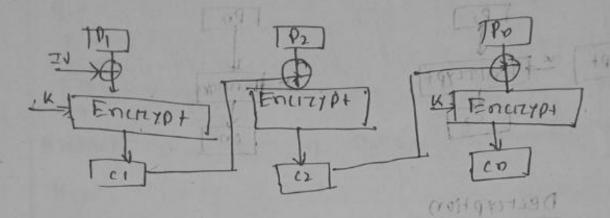


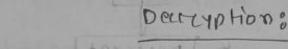
Disadvantages of ECB's

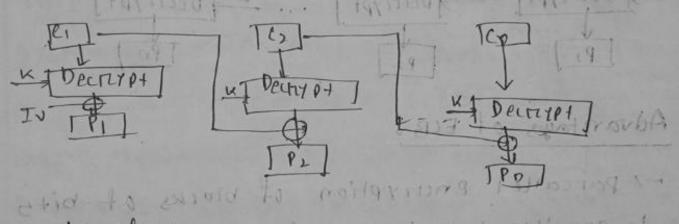
- 1 prone to actorphon of blocks of bits
is possible

-7 simple loung of the block appell









advantages: stant a citi aunt sudiacos of

trut b bits.

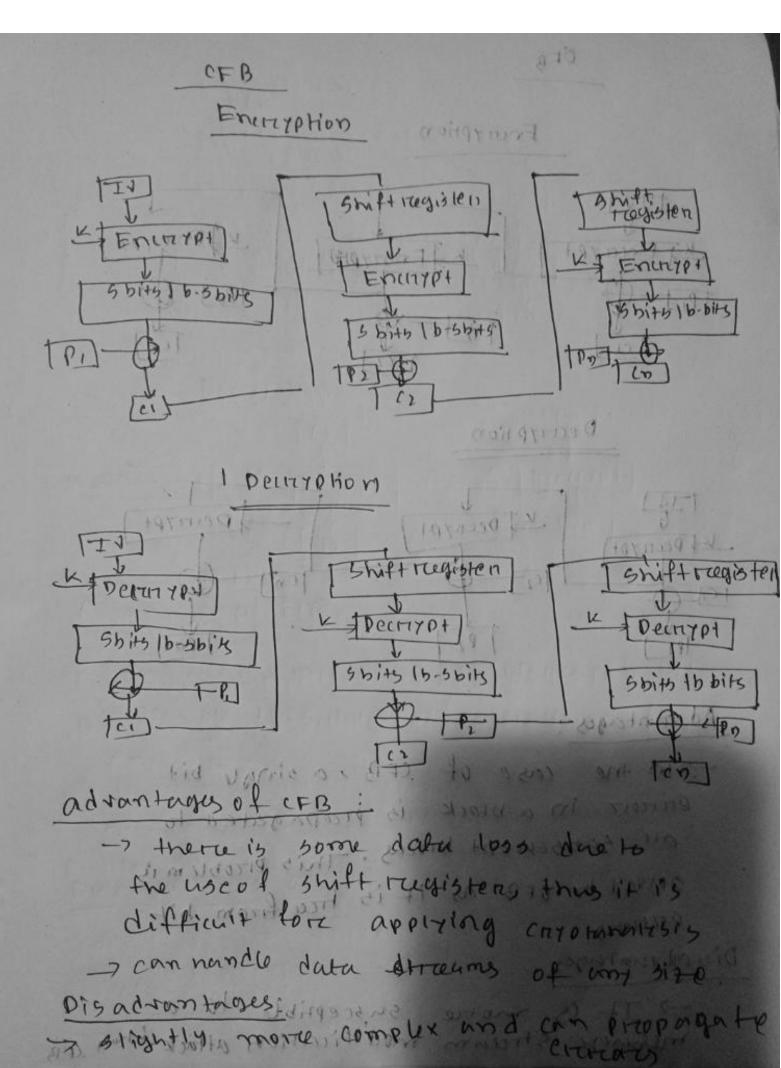
TOBE 15 agood athen Heation mechanism

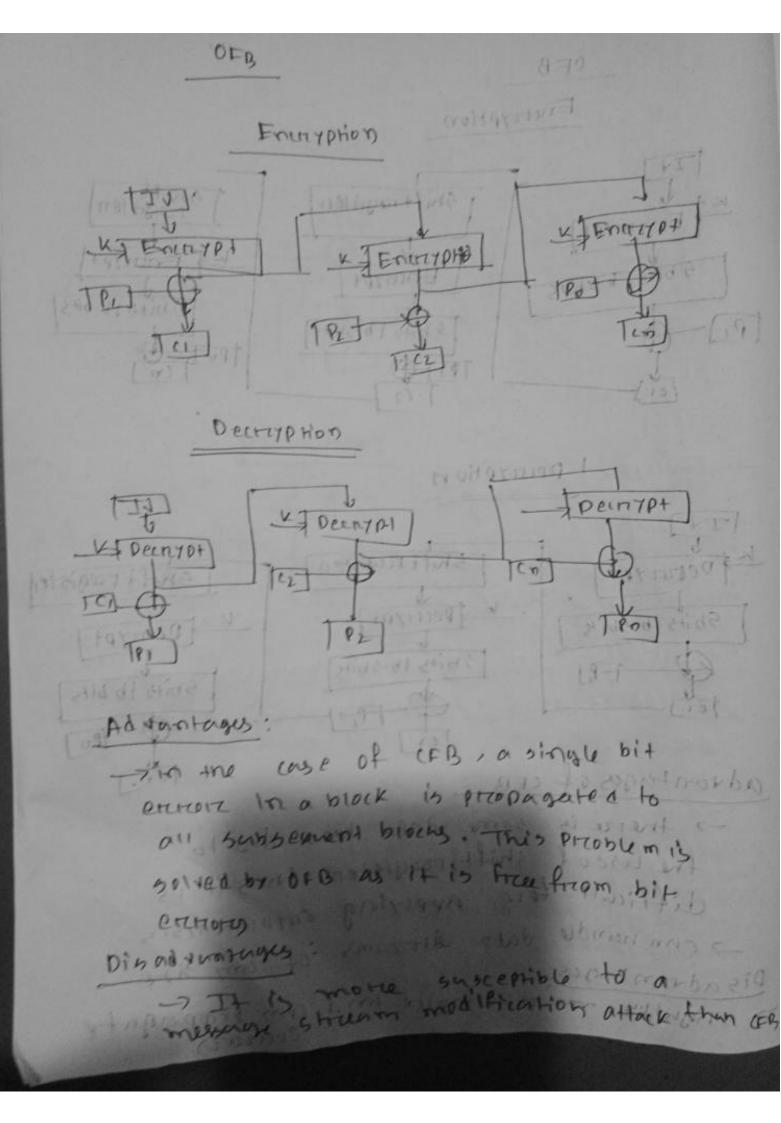
enenzatalysis than Ecs

15 PEOP 18 18 18

Dis ad vantages:

- Repuires the ottevious deherstent book for encorption and decryption.





Dava implementation of RC5:

of world testerations entering with early importet Java nio. Byte Buffer; imported Java Cutil Artercays; Imman's coison

Public class Res à 2 (Nondhand 31 21913) 8 73 (8)

Pravate Anal int w= 32;

private Anai totapi pilola sul atristica

Provate final intb= 16:31 bad and

pravate final inters;

10/10/18 Private final intpu = 0xb7e15163, QW=0x9e377989 3 (97) 1 519 ((CTP) 8

Public RC5 (bytel] Key) }

int[] (key length +3)/4;

Minte I 1 = new intecz; coliger sob

forc lint 1=0; 12 key. length; i++)

L (1/4] 1 = (CKEY Eiz & OXFF) 4 (8 * (10/04))) j4

Int t = 2*(p+1);

5 = new Intet];

5[0] = PW;

Porc (in+ 1=1'> (2+31+1) a

STIJ = STI-17+4W; 4

```
int A=0) B=0, 1=0, 5=0; ma + 1 = 1 = 1 = 1
Int v= 3 x Math max(cit);
FORELIN+ 5=0; 52435H) $
 A = SEIJ = Integen. HOHATELEFT ((SEIJ+A+B),3);
 B = L[]] = Integer : trotateleft((L[i] +A+B), (A+B));
 i = (it) x 2/6/2 or a borrens) commer property single
  1 = (3+1) 0/0() " 3 per ( 12 per 12 per ( 146) (1+6) = C
                       5(600)557d max = 510, 57d
 public, inter encrypt (interpt) formall color
 int A = Ptfolt 5 Cold of Cold of the State of the
  1n+ B = P+E17+0+17; 107 +0 10019
  Forz Cint 1=13/14= p; 14+230 - had margin 13+01
   A= Integer rotate Lift (ANBIB) + 5[2+1];
  B = Integer. trotateleft (BNA, A) + 5[2xi+17;4
   tretures new intfl & A183; & batters of the
  Public lote decrept Clote 3(4)?
   in+A= C+E01;
                                 1 STORY SON SUPERIOR
    Porc(1=n; 1>=1312-3200 25121651 31 antonista
   in+B= (+[1])
```

B = Integer. Protate Right (B-902*iti], A) ^A;

(118 5 × 79 : 0=9 (12)) 210

A = - = 5 [0];

+ cetures new lot [] d. A.B.B. is

Public Static void main (String [] arcgs) {

byte [] Key = "Mysectre+Key 12345". getBytes();

PCS ncs = new PCS(Key);

bystem out printf ("Plaintent: 9008x 0/008x/0",

Plaintent[0], Plaintent[1]);

System out pruntf (" Encrypted: 1008x 01,08x
Cloneration to 2) cloneratent (1)

int[] decrapted = rais decrapt ((lone ratent);

575 tem out printf ("Decrapted: 9008 x 9008x)

decrapted [0], decrapted [1]; 41

Sumple output.]

Plaintent: 12345678 9ABCDEFO

Enury pred: E2(3456 5E7) A789

Decreypted : 12345678 PABOFFO