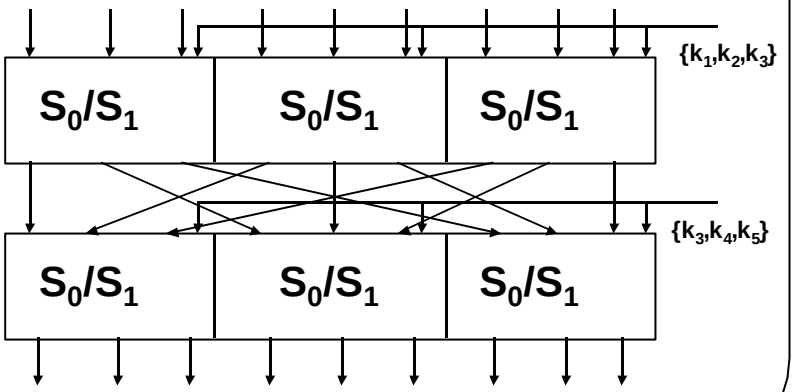
S-P(Substitution-Permutation) Network



Block Cipher

- **Characteristics**
  - **Based on Shannon's Theorem(1949)**
    - ✓ **Repetitive use of Confusion (Substitution) and Diffusion (Permutation)**
    - ✓ **Iteration : Weak -> Strong**
  - **Same P => Same C**
  - **{|P| = |C|} 3 64 bit, |P| 1 |K| 3 56 bit**
  - **Memoryless configuration**
  - **Operate as stream cipher depending on mode**
  - **Shortcut cryptanalysis (DC, LC etc) in 90's**

*** DC :Differential Cryptanalysis, LC : Linear Cryptanalysis**

Design Criteria of DES

- Provide a high level of security
- Completely specify and easy to understand
- Security must depend on key, not algorithm
- Available to all users
- Adaptable for use in diverse applications
- Economically implementable in electronic device
- Efficient to use
- Able to be validated
- Exportable

* Federal Register, May 15, 1973

DES(Data Encryption Standard)

- Based on Lucifer (1972)
- Developed by IBM and intervened by NSA
- Adopted Federal Standard by NIST, revised every 5 years (~' 98),
- 64bit Block cipher, 56bit key
- 16 Round, Nonlinearity : S-box
- Cryptanalysis like DC LC, etc after 1992

* DC:Differential Cryptanalysis, LC : Linear Cryptanalysis

DES Designers

- **IBM Team at Kingston and Yorktown Heights**

  Roy Adler, Don Coppersmith, Horst Feistel, Edna Grossman, Alan Konheim, Carl Meyer, Bill Notz, Lynn Smith, Walter Tuchman, Bryant Tuckermann

DES Documents

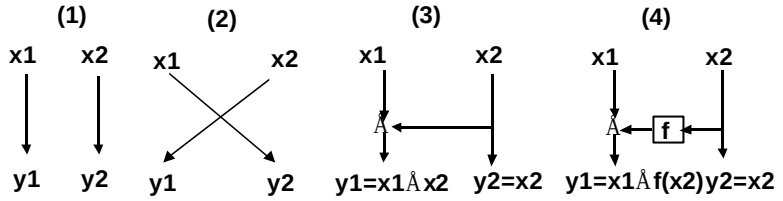
- **FIPS PUB 46-(2), Data Encryption Standard", 1977(83,88)**
- **FIPS PUB 81, "DES modes of operation",1980**
- **FIPS PUB 74, "Guidelines for implementing and using the NBS Data Encryption Standard", 1981**
- **FIPS PUB 112, "Password Usage", May 1985**
- **FIPS PUB 113, "Computer Data Authentication", 1985**

*** FIPS : Federal Information Processing Standard**

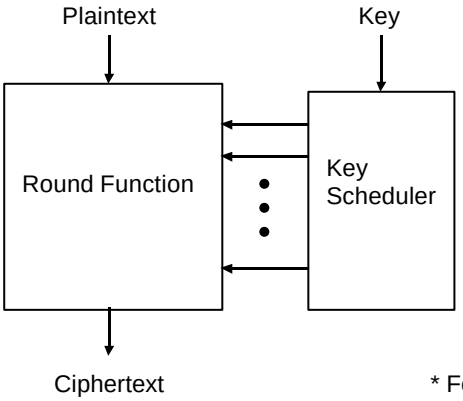
*** http://www.nist.gov**

Involution structure

- Repeats its operation 2 time and returns to the original value, e.g., f(f(x)) = x.
- Type of $f^{-1}(x) = f(x)$

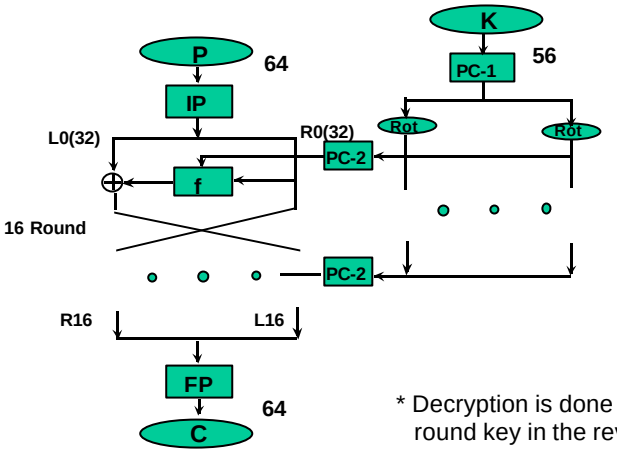


2 Building blocks of DES



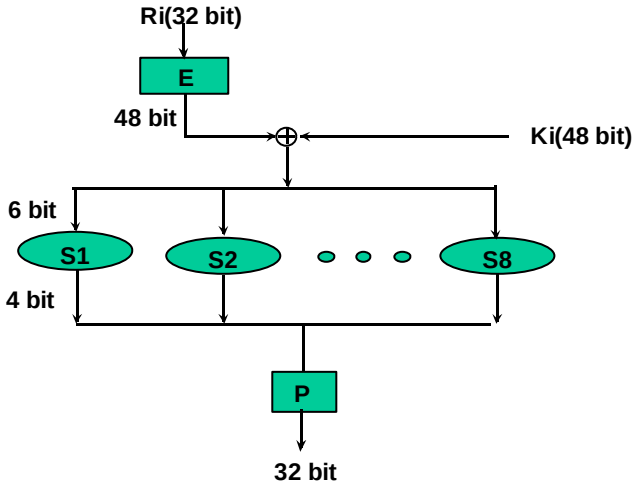
* Feistel Network

Structure of DES



* Decryption is done by executing round key in the reverse order

f-function of DES



Initial Permutation(IP)

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

Final Permutation($FP=IP^{-1}$)

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

P Permutation

- Permutes the order of 32 bits

16	7	20	2	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

E Expansion

- Expands 32 -> 48 bits by duplicating 16 bits twice

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

Permutated Choice-1(PC-1)

- 64 -> 56 bits

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Permutated Chioce-2 (PC-2)

- 56 -> 48 bits

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Rotation Schedule

Rnd 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Rot 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1

- **Total rotation = 28**
- **After final rotations, the final round keys return to the input of the 1st round keys.**

DES S-boxes

- **8 x S-box (6 -> 4 bits)**
- **each row : permutation of 0-15**
- **4 rows : choose by MSB & LSB of input**
- **some known design criteria**
  - **not linear (affine)**
  - **1:2 error prog.**
  - **S(x) and S(x Å 001100) differs at least 2bits**
  - **S(x) ¹ S(x Å 11ef00)**
  - **Resistance against DC etc.**

DES S-boxes(I)

- **Input values mapping order**

0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62
33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63

DES S-boxes(II)

- **S1-box**

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

- **S2-box**

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

DES S-boxes(III)

- **S3-box**

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

- **S4-box**

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

DES S-boxes(IV)

- **S5-box**

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	6	8
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

- **S6-box**

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

DES S-boxes(V)

- **S7-box**

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

- **S8-box**

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Criticism of DES

- **Short key size : 112 -> 56 bits by NSA**
- **Classified design criteria**
- **Hidden trapdoor**
- **Revision of standard every 5 yrs after 1977 by NIST**

Cryptographic properties

- (P,C) dependency with fixed Key : after 5 round
- (K,C) dependency with fixed pt : after 5 round
- Avalanche effect
- Cyclic Test : Random function
- Algebraic structure : Not a group

  i.e., $E(K_1, E(K_2,P)) \stackrel{1}{} E(K_3,P)$

Known Weakness of DES

- Complementary Prop.
  - ✓If C= E(K,P), _C = E(_K, _P)
- Weak Key : 4 keys
  - ✓E(K, E(K,P))=P
- Semiweak Keys : 12 keys (6 pairs)
  - ✓$E(K_1, E(K_2,P))=P$
- Key Exhaustive Search : 2^{55}

H/W implementation of DES

Maker	Chip	yr	Clock	Speed	Avail'ty
AMD	Am9518	'81	3MHz	1.3MB/s	N
AMD	AmZ8068	'82	4MHz	1.7MB/s	N
WD	WD2001/2002	'84	3MHz	0.23MB/s	N
AT&T	T7000A	'85	?	1.9MB/s	N
Cryptech	Cry12C102	'89	20MHz	2.8MB/s	Y
Newbridge	CA95C68/18/09	'93	33MHz	14.67MB/s	Y
VLSI	VM007	'93	32MHz	23.7MB/s	Y
VLSI	VM009	'93	33MHz	14.0MB/s	Y
VLSI	6868	'95	32MHz	64.0MB/s	Y
DEC		'95	250MHz	1Gbit/s	?

S/W implementation of DES

Processor	Clock(MHz)	Speed(block/sec)
8088	4.7	370
68000	7.6	900
80286	6	1,100
80386	25	5,000
80486	66	43,000
Sun ELC		26,000
Sparc 10/52		84,000
DECAlpha4000/610		154,000
HP9000/887	125	196,000

DES Key Search Machine

- **Diffie & Hellman (' 77)**
  - **10^6 keys/sec VLSI**
  - **Cost = $20,000,000**
- **Wiener (' 93)**
  - **5 x 10^7 keys/sec**
  - **1 Frame :10$/VLSI x 5,760 =$100,000**
  - **10 Frames : $1,000,000 (3.5hr in average)**

Cost of Key Exhaustive Search Machine

Budget	Tool	Breaking time(cost)		Req't key size ('96-'18)
		40bit	56bit	
small		1 wk	impossible	45~60
$400	FPGA-1 chip	5hr($.08)	38yr($5,000)	50~65
$30,000,000	Cray T3D-1024 nodes	10min	15month	-
$10,000	FPGA-25 chips	12min($.08)	18min($5,000)	55~70
$30,000	FPGA-750 chips	24sec($.08)	19day($5,000)	60~75
	ASIC-15,000 chips	18sec($.001)	3hr($38)	
$10,000,000	FPGA-25,000 chips	.7sec($.08)	13hr($5,000)	70~85
	ASIC-500,000 chips	.005sec($.001)	6Min($38)	
$30,000,000	ASIC-1,500,000 chips	.002sec($.001)	12sec($38)	75~90

(1) FPGA(Field Programmable Gate Array) : AT&T ORCA Chip($200), 3,000 counts/sec for 56-bit key
(2) ASIC(Application Specific IC) : $10, 20 Million /sec search
(3) Reduce the value of money in half every 18 months till 2018
http://guru.cosc.georgetown.edu/~denning/crypto/Trends.html

DES Challenge(I)

- RSA Data Security Inc' s protest against US' s export control(' 97)
  - $10,000(' 97) award
  - Key search machine by Internet Loveland' s Rocker Verser
  - 60.1 Billion/1 day Key search, Succeed in 18 quadrillion operations and 96 day
    - ✓ 25% of Total 72 quadrillion (1q=10^{15} =0.1 kyung)
    - ✓ 90MHz, 16MB Memrory Pentium(700 Million/sec)
  - http://www.rsa.com/des/

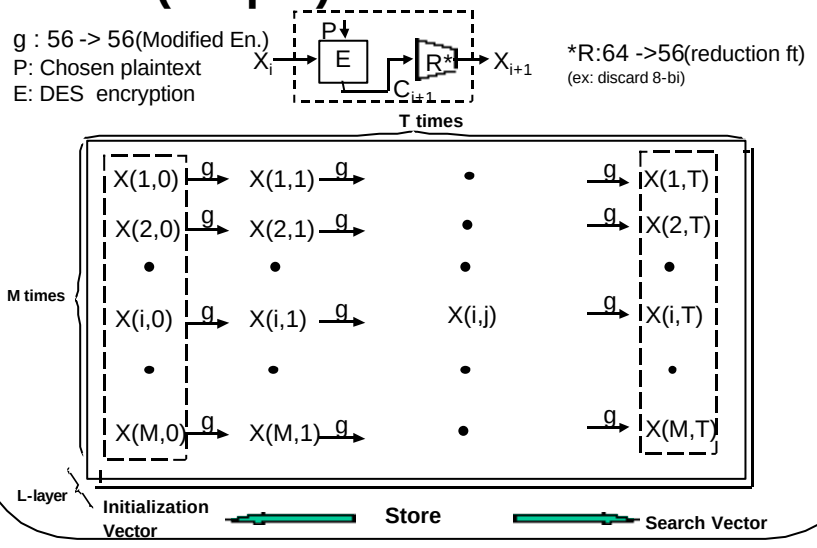
DES Challenge(II, III)

- Distributed.Net + EFF
  - 100,000 PC on Network
  - 56hr
- EFF
  - http://www.eff.org/DEScracker
  - Specific tools
  - 22hr 15min
  - 250,000$

Time-Memory Trade Off(I)

- Given E and (P,C), find K (CPA)
- Consist of 2 steps
  - Step to make pre-computation : Space complexity
  - Step to search key : Time complexity
- (Step 1)
  - (1) Select initial M plaintexts by random
  - (2) Encrypt them and yield ciphertext
  - (3) Using reduction function, reduce 64-bit to 56-bit
  - (4) Using reduced 56-bit as a key
  - (5) Repeat (2) to (4) T times
  - (6) Repeat (1) to (5) L times

(Step 1) Search Table

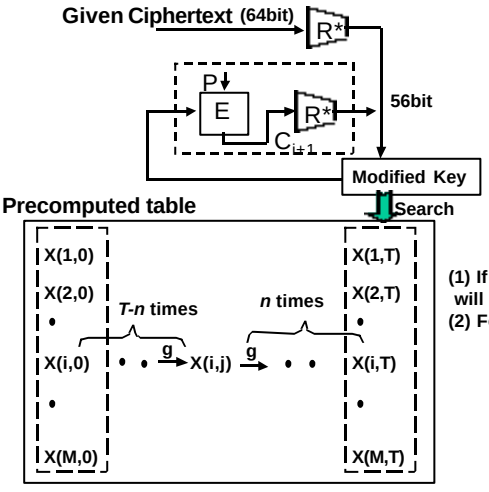


Time-Memory Trade Off(II)

(Step 2)

- **(1) Reduce a ciphertext into a modified key using reduction ft.**
- **(2) Find a matched value in search table in Step 1**
- **(3) If not found, repeat to generate new modified key by inputting a modified key as a key**
- **(4) If found, save loop counter and check the from the initialization vector to find an unknown key**
- **(5) Repeat (1) to (4) T times**

(Step 2) Key search



(1) If loop counter becomes *n*, modifiedkey will be unknown key with high probability.
(2) For verification, check from IV.

TMTO Machine

Goal of TMTO machine of DES :
success rate : 80%, Pre-computation table : 1 month,
key search : 1 hr

Type of TMTO machine (estimation)
- 786 VLSI (2 DES Chips operating 33 MHz)
- 512 Gb HDD
- space of 16 W/S

"The Feasibility Study of a Machine for Time-Memory Tradeoff Cryptanalysis", Proc. of SCIS' 98, 6.2.C., Jan. 29-31, Hamanako, Japan, 1998, Masahiro Iida, Katsumi Takahashi, Hiroyuki Miyata,Tsutomu Matsumoto,

Strengthening DES(I)

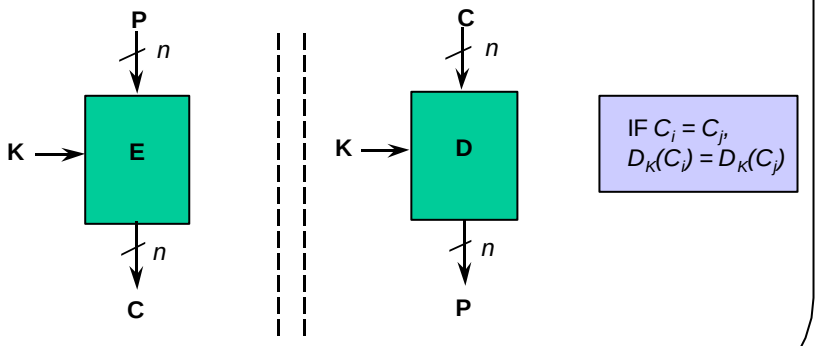
- **Key size expansion**
  - **Double Encryption**
    - ✓ e_k:$E_2(K_2,E_1(K_1,P))$, d_k:$D_1(K_1,D_2(K_2,C))$
    - ✓ **Meet-in-the-middle attack**
    - ✓ **No effectiveness**
  - **Triple Encryption**
    - ✓ e_k:$E(K_1,D(K_2,E(K_1,P)))$, d_k:$D(K_1,E(K_2,D(K_1,C)))$
    - ✓ e_k:$E(K_1,D(K_2,E(K_3,P)))$, d_k:$D(K_3,E(K_2,D(K_1,C)))$
    - ✓ **112 or 168 bits**

Strengthening DES(II)

- **Internal structure change**
  - **S-box Change : s^5DES**
  - **Swapping Change**
    - ✓ **Dynamic (pt-dependent) swapping**
    - ✓ **Static (key-dependent) swapping**
  - **Generalized DES, etc**

Mode of operation(I)

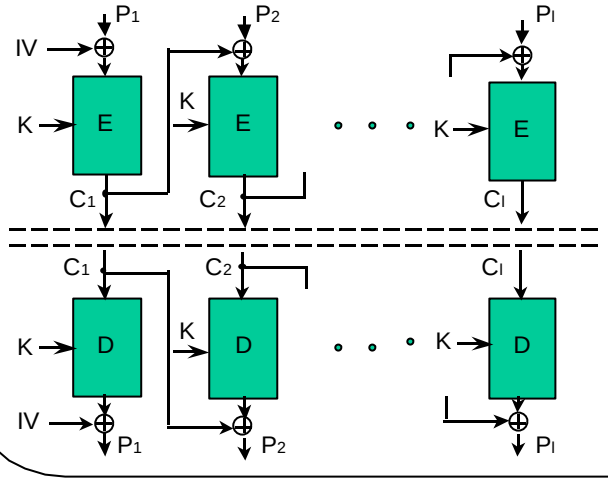
- **ECB (Electronic CodeBook) mode**



i) Encryption ii) Decryption

Mode of operation(II)

❑ CBC (Cipher Block Chaining)



IV : Initialization Vector

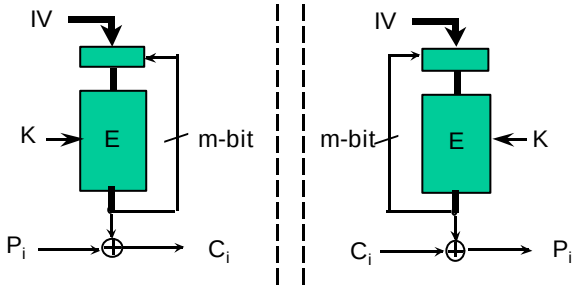
$C_i = E_K(P_i \oplus C_{i-1})$

$P_i = D_K(C_i) \oplus C_{i-1}$

- 2 blk Error Prog.
- self-sync
- If $|P_l| \neq |P|$, Padding req'd

Mode of operation(III)

❑ m-bit OFB (Output FeedBack)



I) Encryption

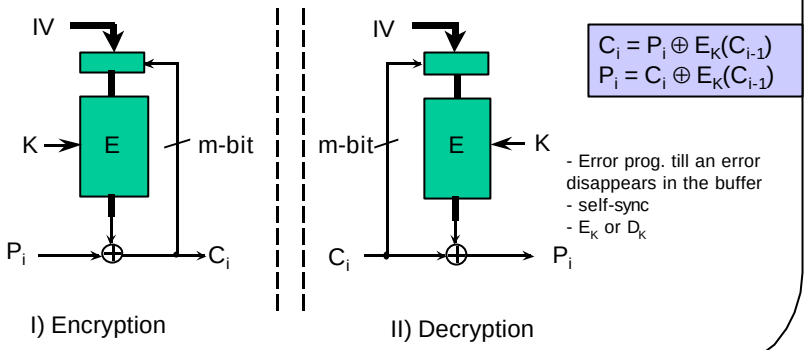
II) Decryption

$C_i = P_i \oplus O(E_K)$
$P_i = C_i \oplus O(E_K)$

- No Error Prog.
- Req'd external sync
- Stream cipher
- E_K or D_K

Mode of operation(IV)

- **m-bit CFB (Cipher FeedBack)**



$C_i = P_i \oplus E_K(C_{i-1})$
$P_i = C_i \oplus E_K(C_{i-1})$

- Error prog. till an error disappears in the buffer
- self-sync
- E_K or D_K

Mode of operation(V)

- **Use of mode**
  - **ECB : key mang' t, useless for file encryption**
  - **CBC : File encryption, useful for MAC**
  - **m-bit CFB : self-sync, impossible to use channel with low BER**
  - **m-bit OFB : external-sync**
    - ✓ **m-bit : 1, 8 or n**
  - **Etc : New IV per new block**
  - **Performance Degradation/ Cost Tradeoff**