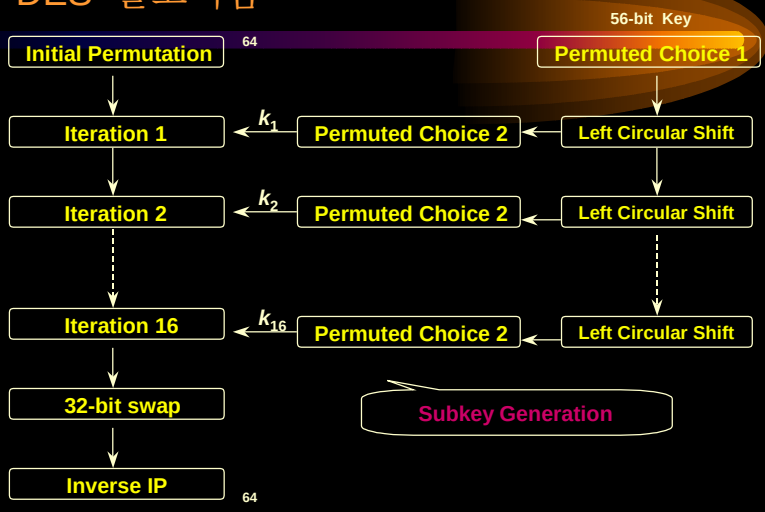
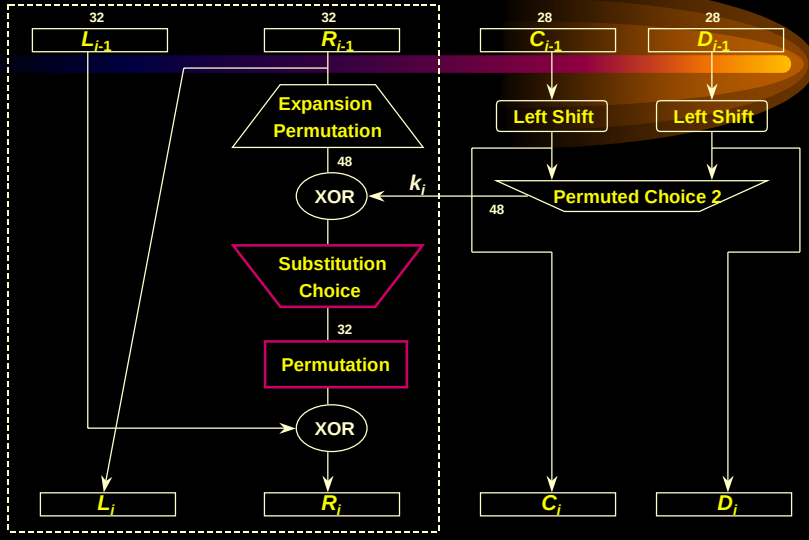
❑ Data Encryption Standard

- ❑ **배경**
  - 1960년 말 ~ 1971년, IBM Project "LUCIFER", by Horst Feistel
  - 1973년 NBS (National Bureau of Standards, NIST 전신)
  - 1977년 미국정부 암호 표준으로 DES 채택
- ❑ **특징**
  - Diffusion, Confusion
  - Product Cipher, Substitution Cipher and Permutation
  - **Symmetric 암호시스템**, $c = E_k(m)$
- ❑ **비판**
  - Key Size
  - Design 원리의 비공개
  - 1999년 까지 미국 정부 표준 유효 (NSA, National Security Agency)

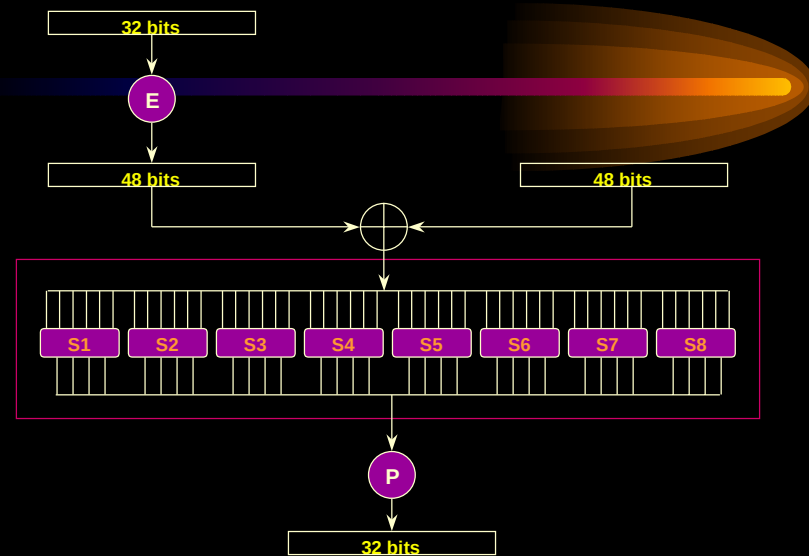
암호이론과 보안 대칭형 암호

❑ DES 알고리즘





암호이론과 보안 대칭형 암호



❑ Permutation Tables

IP (Initial Permutation)

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

P-BOX

16	7	20	21
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

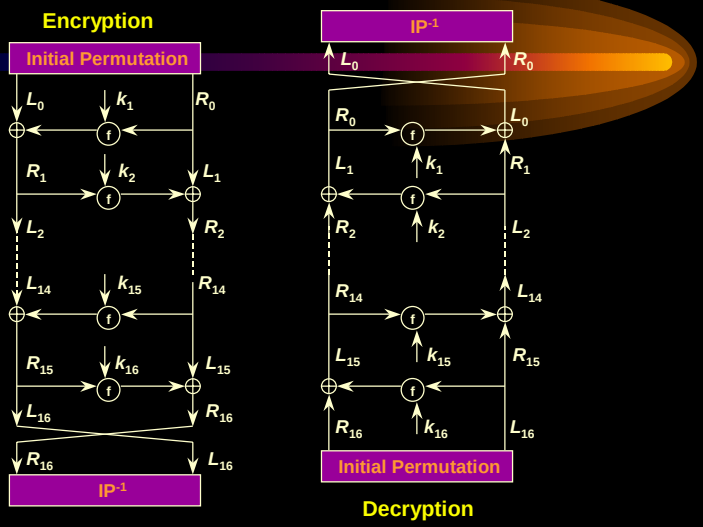
Expansion Permutation

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

❑ S - BOX

Choice Substitution (S-Box)

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
Row	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
s2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
Row	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
:		:		:		:		:		:		:		:		:	
s8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
Row	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11



❑ Avalanche Effect (쇄도효과)

Change in Plaintext		Change in Key	
Round	Change	Round	Change
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	29	15	34
16	34	16	35

Two Plaintexts
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
10000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
with the key
0000001 1001011 0100100 1100010
0011100 0011000 0011100 0110010

Plaintext
01101000 10000101 0010111 01111010
00010011 01110110 1101011 10100100
with the Two key
1110010 1111011 1101111 0011000
0011101 0000100 0110001 1101110
0110010 1111011 1101111 0011000
0011101 0000100 0110001 1101110

❑ Security of DES

❑ Exhaustive Key Search

- Known-Plaintext Attack, $m \rightarrow c = E_k(m)$
- 2^{56} Keys
- 5 micro-seconds for testing a key
  - $2^{56} \sim 10^{15}$ tests, $5 \times 10^{-3} \times 10^{15}$ seconds $\sim 10^6$ years
- Moore's Law
  - Computing power doubled every 18 months

Cost	56-bit	64-bit	112-bit	128-bit
$100K	35hours	1year	10^{14} years	10^{19} years
$1 M	3.5hours	37days	10^{13} years	10^{18} years
$10M	21min	4days	10^{12} years	10^{17} years
$1G	13sec	1hour	10^{10} years	10^{15} years

암호이론과 보안 대칭형 암호

❑ Security of DES

❑ Weak Keys ■ Semiweak Keys

0000000	0000000
0000000	FFFFFFF
FFFFFFF	0000000
FFFFFFF	FFFFFFF

01FE	01FE	01FE	01FE	and	FE01	FE01	FE01	FE01
1FE0	1FE0	0EF1	0EF1	and	E01F	E01F	F10E	F10E
01E0	01E0	01F1	01F1	and	E001	E001	F101	F101
011F	011F	010E	010E	and	1F01	1F01	0E01	0E01

❑ Complement Keys

- $E_k(m) = c$, $E_{k'}(m') = c'$
- Key Search reduced to 2^{55}

❑ Why 16 rounds ?

- 4 rounds (1982), 6 rounds (1985)
- Differential Cryptanalysis (1990) : Adi Shamir and Eli Biham

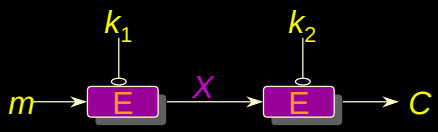
❑ Commercial DES Chip

Manufacturer	Chip	Year	Clock	Data Rate
AMD	Am9518	1981	3MHz	1.3MByte/sec
CE-Infosys	Supercrypt	1994	30MHz	20.0Mbyte/sec
VLSI Technology	6868	1995	32MHz	64.0MByte/sec

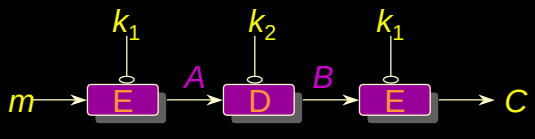
❑ Software Implementation

Processor	Speed(in MHz)	DES Blocks/sec
8088	4.7	370
68040	40.0	23,000
80486	66.0	43,000
Sparc 10		84,000
HP 9000	125.0	196,000

❑ Multiple DES Encryption



• $c = E_{K2}[E_{K1}(m)]]$



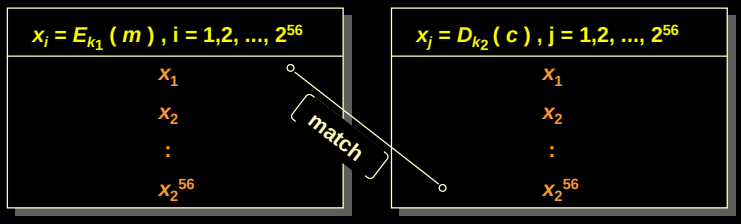
- $c = E_{K1}[D_{K2}[E_{K1}(m)]]]$
- Key Management Standard for ISO 8732 and PEM

❑ Meet-In-the-Middle-Attack

- ❑ $c = E_{k2} [E_{k1} (m)]] = ? E_{k3} (m)$

  $(2^{64}) ! > 10^{347380000000000000000}$

  $2^{56} < 10^{17}$
- ❑ $x = E_{k1} (m) = D_{k2} (c)$
- ❑ Given a pair of (m, c),



❑ Operation Modes for DES

- ❑ **ECB** (Electronic CodeBook)
- ❑ **CBC** (Cipher Block Chaining)
- ❑ **CFB** (Cipher Feedback)

❑ ECB Mode

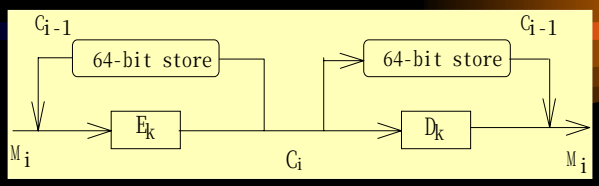
- ❑ $E_k(m) = E_k(m_1)\ E_k(m_2)\ E_k(m_3)$, ... , where $m = m_1\ m_2\ m_3$ .....
- ❑ 단점

  - 동일 암호문은 동일한 평문
  - Database 응용에 부적당

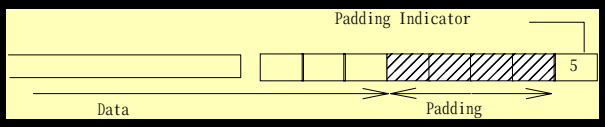
Name	Salary
평문	암호문

Give	Park	$100	Give	Lee	$50

❑ CBC (Cipher Block Chaining)

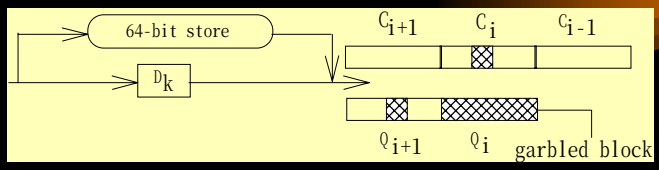


- ❑ Encryption : $c_i = E_k(m_i \oplus c_{i-1})$, $i = 1,2,3,...$
- ❑ Decryption : $m_i = D_k(c_i) \oplus c_{i-1}$, $i = 1,2,3,...$
- ❑ $c_i = f(m_1, ... , m_i)$
- ❑ First Block m_1 , $c_1 = E_k(m_1 \oplus IV)$, where IV is Initialization Vector
- ❑ Last Block



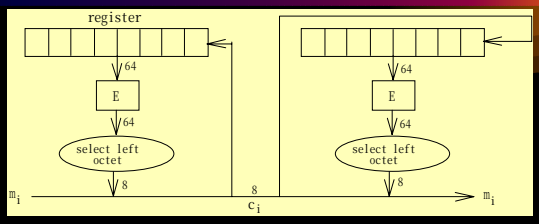
암호이론과 보안 대칭형 암호의 운영방식

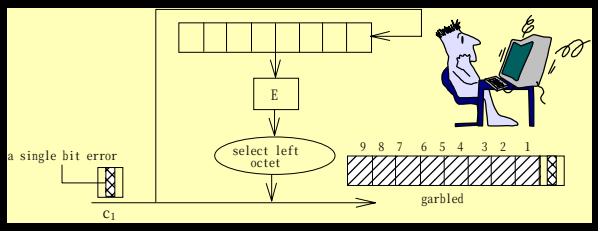
❑ CBC (Cipher Block Chaining)



- ❑ stage i : $D_k(c_i) \oplus c_{i+1} = Q_i$
- ❑ stage (i+1) : $D_k(c_{i+1}) \oplus c_i = (m_{i+1} \oplus c_i) \oplus c_i = Q_{i+1}$
- ❑ after stage (i+1), CBC is **self-recovering**.
- ❑ **Error-Control Codes** are used to prevent "**Error Propagation**".

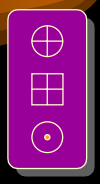
❑ CFB (Cipher FeedBack)





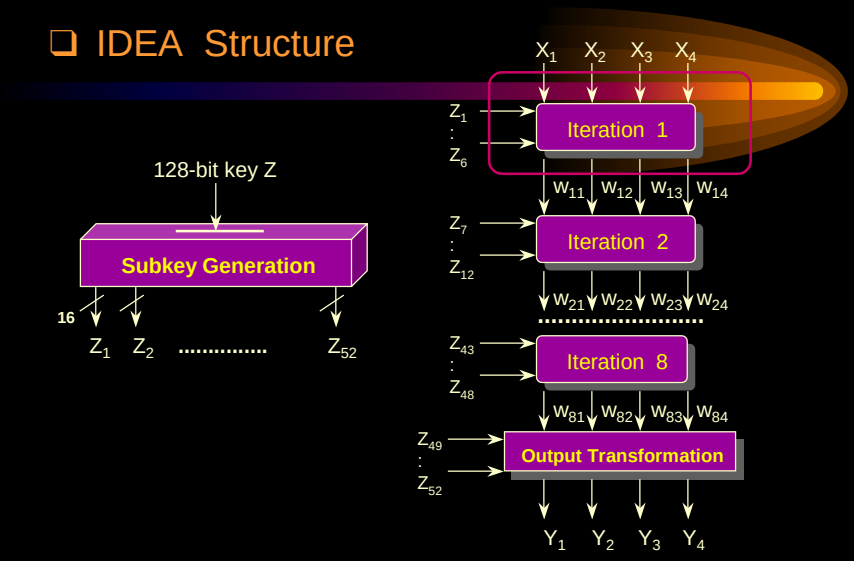
❑ International Data Encryption Algorithm

■ Design Principle



- Block Length, 64-bit
- Key Length, 128-bit
- Confusion
  - XOR, Addition mod 2^{16}, multiplication mod $2^{16} + 1$
- Diffusion
  - two 16-bit sub-block, two 16-bit subkey, two 16-bit output
- Software Implementation
  - 16-bit sub-block for easy programming
- Hardware Implementation
  - similarity between encryption and decryption
  - modular structure for easy VLSI implementation

❑ IDEA Structure



암호이론과 보안 IDEA

- Single Iteration of IDEA