제 3 장 블록암호 와 DES

❑ 목 차

- ❖ 단순 **DES**
- ❖ 블록 암호 기법
- ❖ **DES**
- ❖ 블록 암호의 설계 원리
- ❖ 블록 암호의 운용 모드

DES의 역사

- 데이터 암호화 표준이 필요
- 미연방 정부에 의해 공개 암호 표준화 작업 진행
- 표준화 검토(1972), 적합한 암호 알고리즘 조사
- 1973년 5월: 암호방식 공모(1차)
  - 표준암호 알고리즘은 높은 수준의 안전성을 보장 할 수 있어야 한다
  - 표준암호 알고리즘은 사양의 정의가 완전하여 간단히 이해 할 수 있어야 한다
  - 표준암호 알고리즘이 제공하는 안전성은 알고리즘의 비밀성에 의존되어서는 안된다.
  - 표준암호 알고리즘은 사용자나 제작자가 모두 사용 가능해야 한다
  - 표준암호 알고리즘의 응용이 다양해야 한다
  - 표준암호 알고리즘은 전자장치로써 제품화가 간단하고, 또한 사용이 간단해야 한다.
  - 알고리즘 타당성 검증에 협력해야 한다
  - 표준암호 알고리즘은 수출할 수 있어야 한다

DES의 역사

- 1974년 8월: 2차 공모
  - IBM(Lucifer)이 요건을 갖춤
  - NBS가 요건을 NSA에 의뢰
- 1975년~1977년: 일반 comment, 계약 체결
- 1977년: NBS(NIST)가 DES를 표준 암호 알고리즘으로 채택 (FIPS PUB46)
- 5년마다 검토(1983, 1988, 1993)
- U.S.banks have been adopted DES
- NBS postponed guarantee term of DES from 1993 to 1998
- NSA proposed CCEP(Commercial COMSEC Endorsement Program; 상용 통신 안전 보증 계획)instead of DES
- U.S. bank expect to continue the use of DES

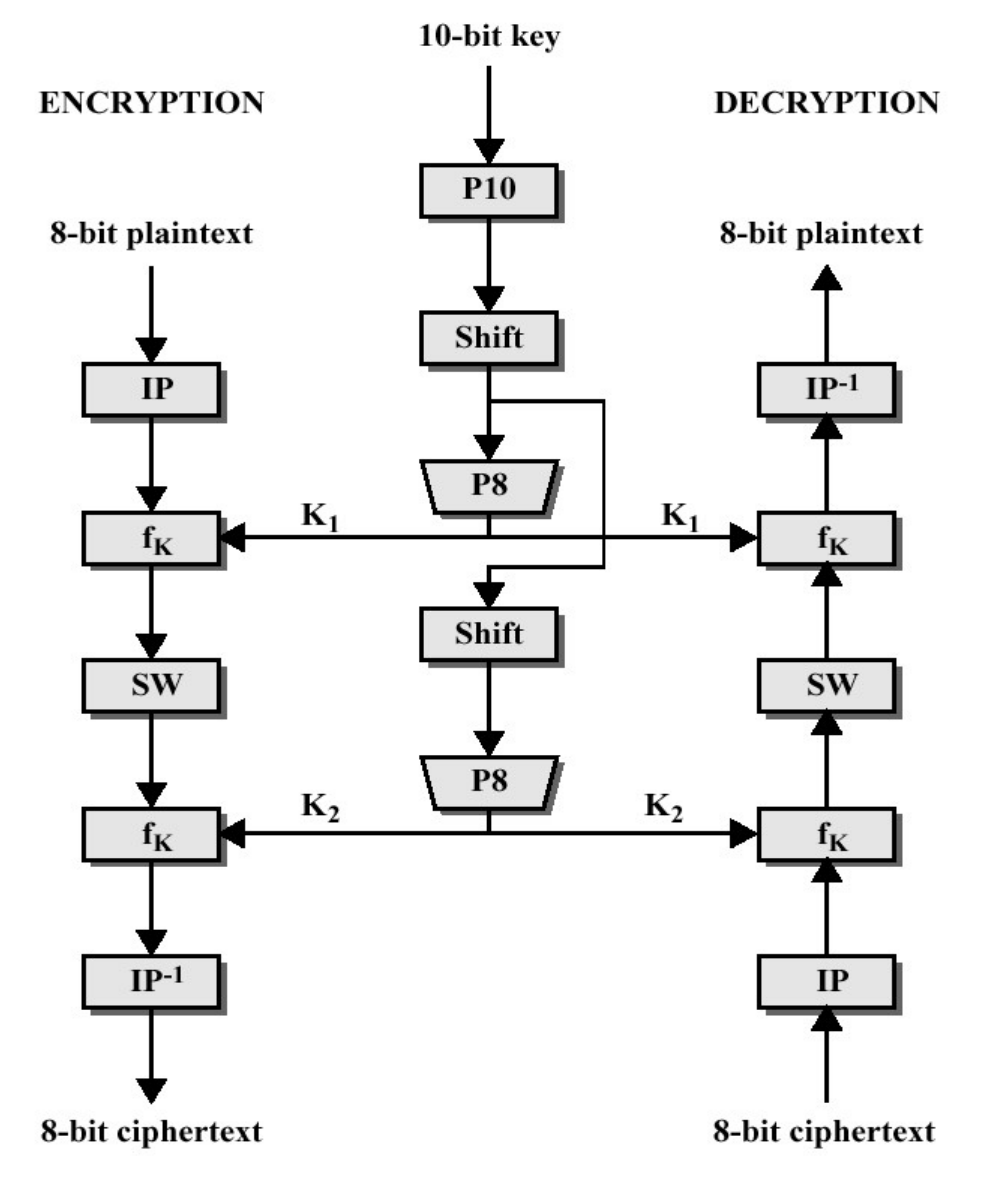
DES (Data Encryption Standard)

- 1977년 미 상무성의 국립 표준국(National Bureau of Standards)에서 연방 정보처리 표준 채택 46(FIPS PUB46)
  - NIST : National Institute of Standards and Technology
- 64비트 블럭 암호 알고리즘
- 56비트 키를 사용
  - 64비트 중 8비트는 parity check로 사용
- 기본 구조
  - round 수 : 16 round
  - 복호화는 암호화의 역순
- 최근에는 DES암호화를 세 개의 키로 세 번 반복함으로써 암호의 강도를 높인 Triple-DES를 사용
- 치환과 전치 혼합방법, 블럭 암호, 관용암호방식

❖ Brute force Attack

Key size	Number of Alternative Keys	One Encryption per micro sec	10^6 Encryption per micro sec
56bits	$2^{56} = 7.2 * 10^{16}$	1142years	10.01h
128bits	$2^{128} = 3.4 * 10^{38}$	10^{24}years	$5.4 * 10^{18}$ years

S-DES와 DES



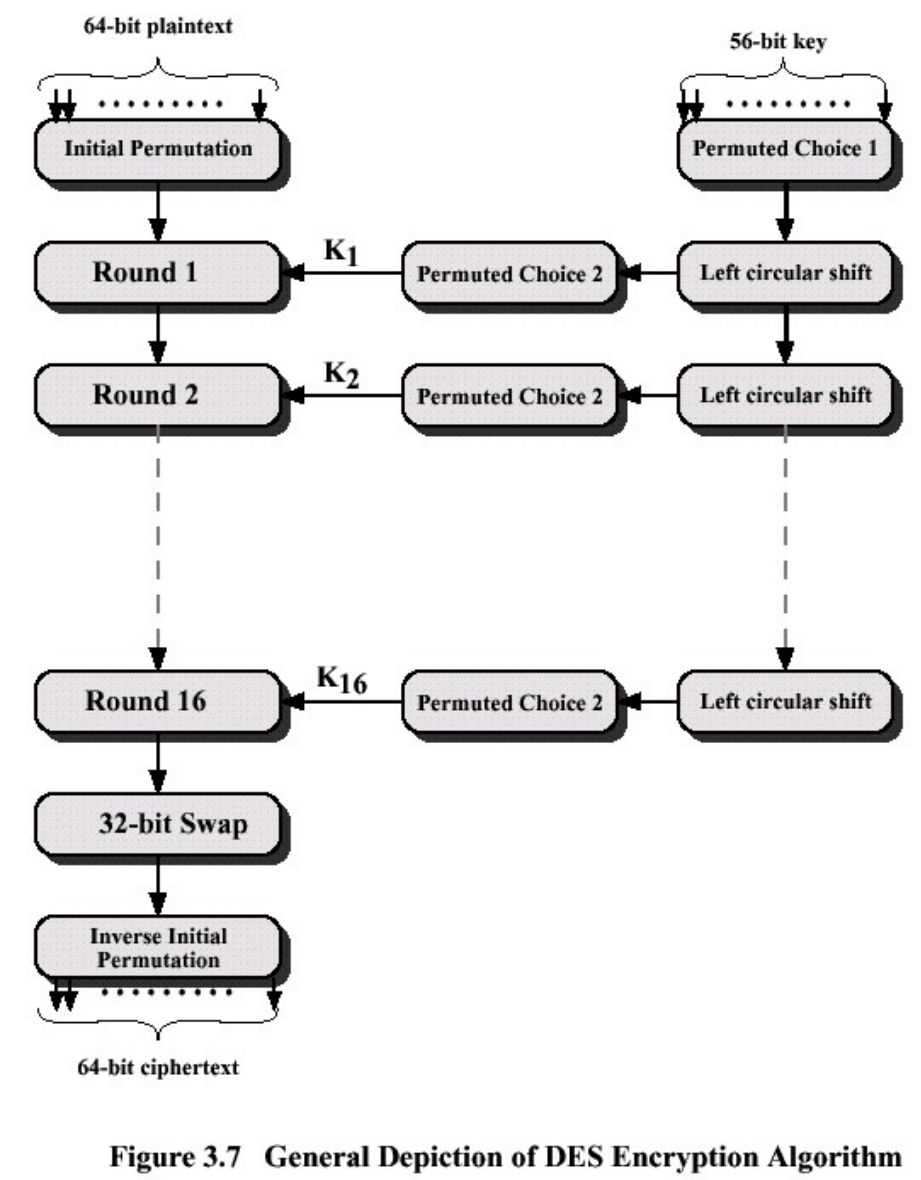


Figure 3.7 General Depiction of DES Encryption Algorithm

DES와의 관계

- 단순 DES는 8-비트 블록단위로 2단계 처리
  - $IP^{-1} \cdot f_{k_2} \cdot SW \cdot f_{k_1} \cdot IP$ (평문)
  - 10비트 키에서 2개의 8-비트 서브키 생성
  - F 함수는 4비트 연산
  - 4행 4열로 구성된 2개의 S 박스 사용
- DES는 64-비트 블록단위로 16단계 처리
  - $IP^{-1} \cdot f_{K_{16}} \cdot SW \cdot f_{K_{15}} \cdot SW \cdot \cdots\cdots \cdot SW \cdot f_{K_1} IP$
  - 키 56비트에서 16개의 48-비트 서브키 생성
  - F함수는 32비트 연산
  - 4행 16열로 구성된 8개의 S박스 사용

설계 특성

- ❖ 블록 크기(64비트)
  - ➢ 큰 블록은 보안 강화하지만 암/복호 속도는 저하
  - ➢ 암/복호 속도를 고려 64비트
- ❖ 키 크기(56비트)
  - ➢ 큰 키는 보안 강화 하지만 암/복호 속도는 저하
  - ➢ 암/복호 속도를 고려하여 56비트 (현재는 128비트)
- ❖ 반복 수
  - ➢ 다중 반복과정은 보안성 강화
  - ➢ 16회 반복이 일반적
- ❖ 서브키 생성 알고리즘
  - ➢ 서브키 생성 방법이 복잡할수록 강력
- ❖ 반복함수
  - ➢ 적용되는 반복함수가 복잡할수록 강력

DES 암호화

- DES의 알고리즘의 모델
  - 평문: 64bit
  - 키: 56bit + 8bit(패리티)
- 처리 단계
  - 초기순열 단계(IP)
  - 16라운드 반복
  - 좌우 교환단계
  - 역초기순열 단계(IP^{-1})

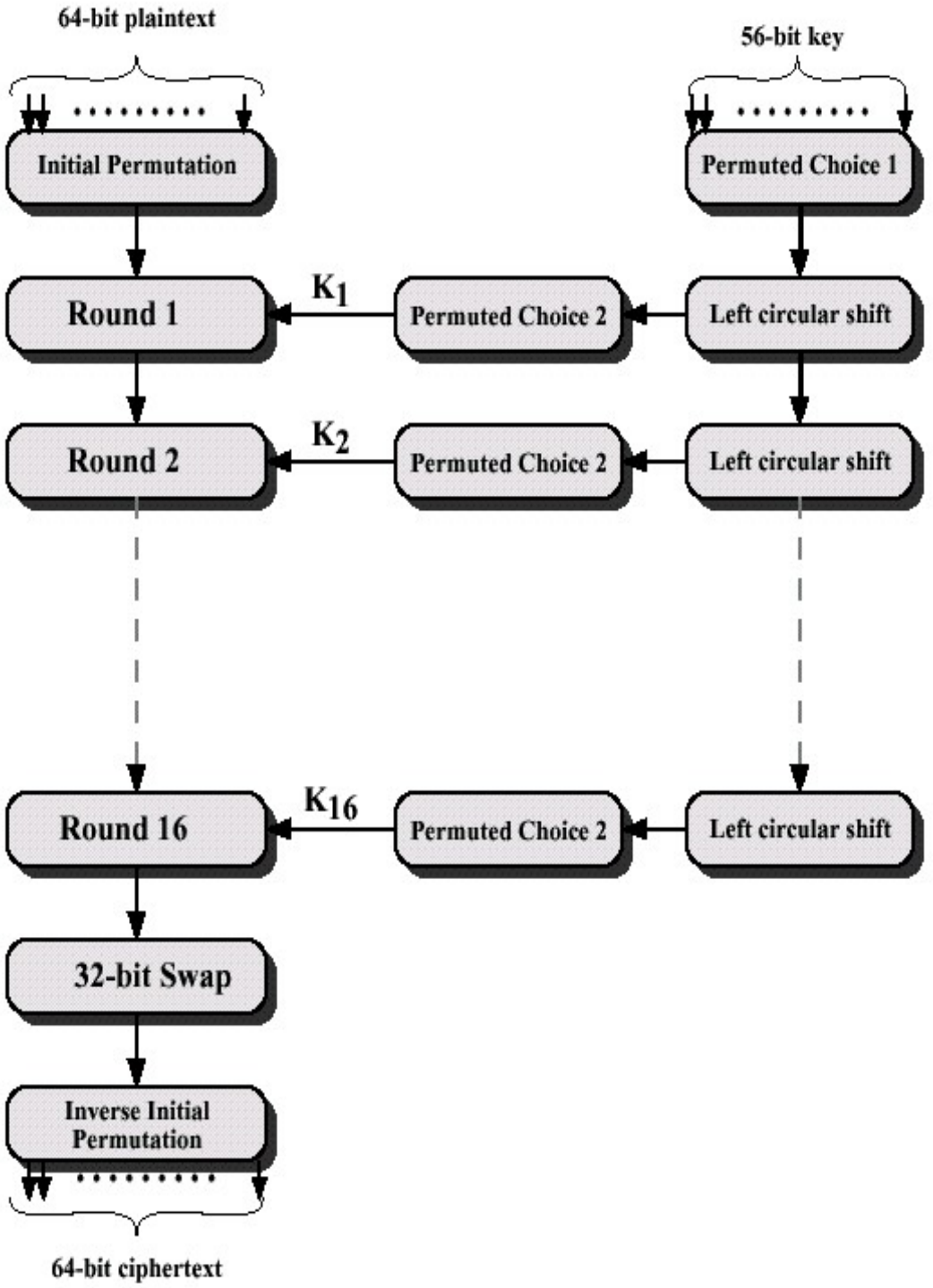
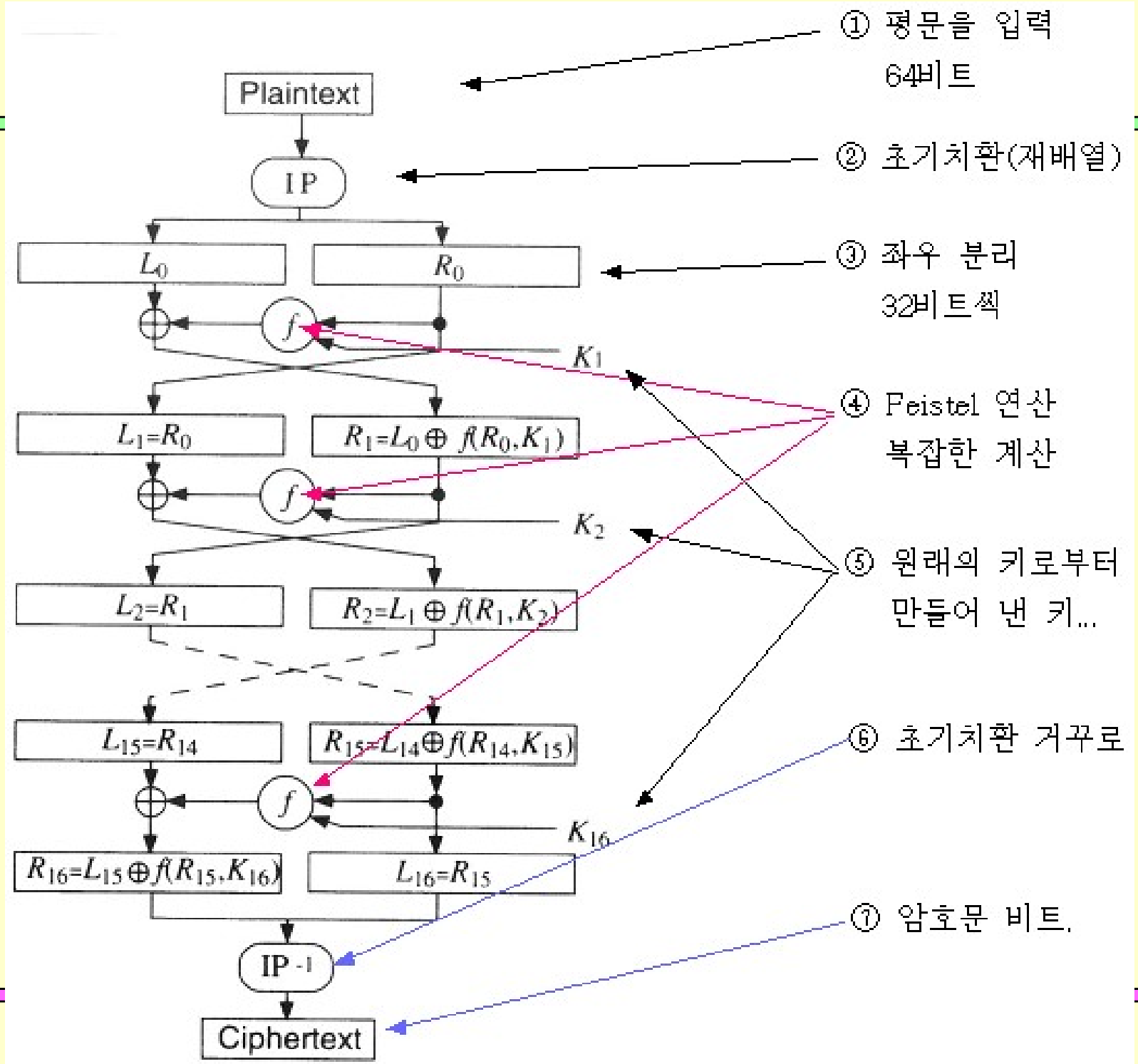


Figure 3.7 General Depiction of DES Encryption Algorithm


① 평문을 입력
64비트
Plaintext
② 초기치환(재배열)
IP
③ 좌우 분리
32비트씩
L_0
R_0
K_1
④ Feistel 연산
복잡한 계산
$L_1=R_0$
$R_1=L_0 \oplus f(R_0,K_1)$
K_2
⑤ 원래의 키로부터
만들어 낸 키...
$L_2=R_1$
$R_2=L_1 \oplus f(R_1,K_2)$
$L_{15}=R_{14}$
$R_{15}=L_{14} \oplus f(R_{14},K_{15})$
⑥ 초기치환 거꾸로
K_{16}
$R_{16}=L_{15} \oplus f(R_{15},K_{16})$
$L_{16}=R_{15}$
⑦ 암호문 비트.
IP -1
Ciphertext

DES의 기본 구조 (단일 반복 과정)

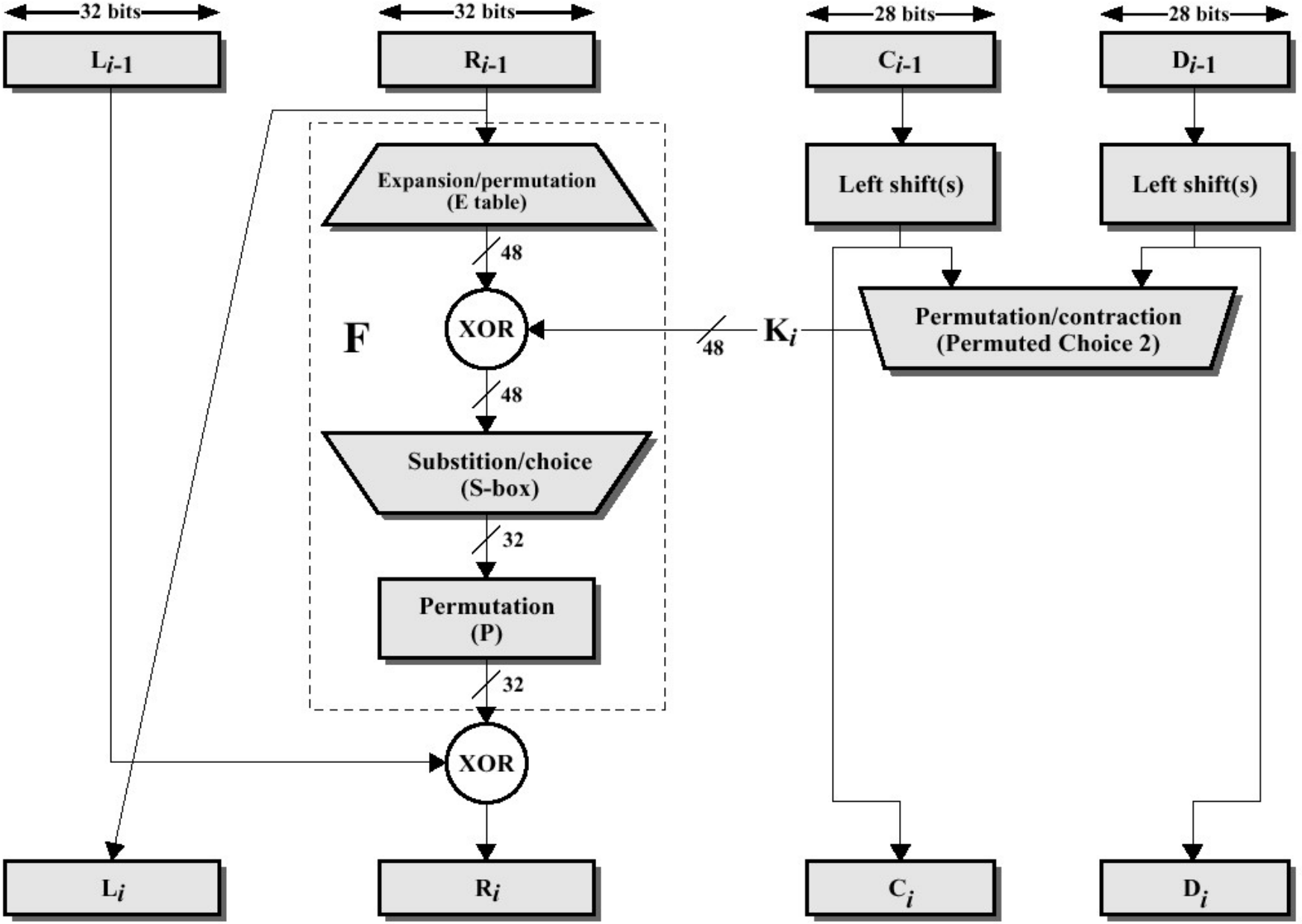
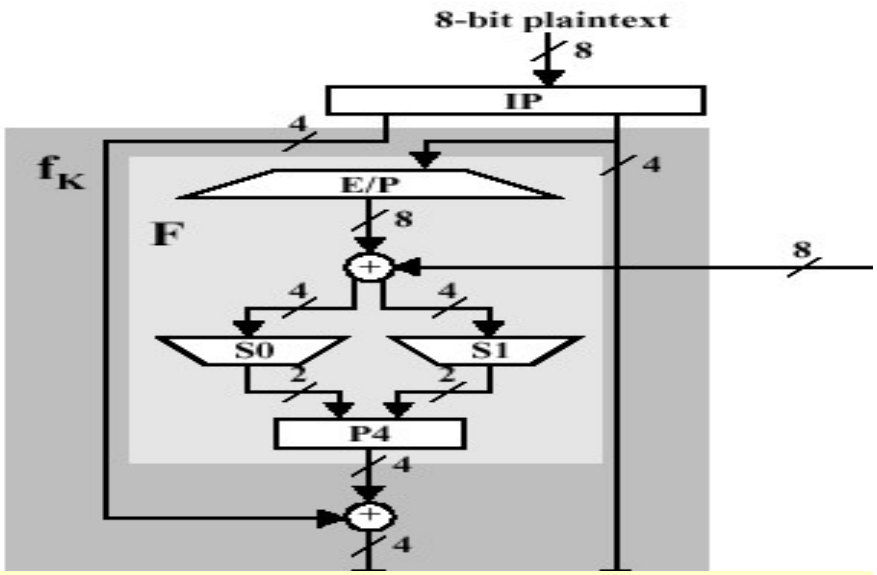
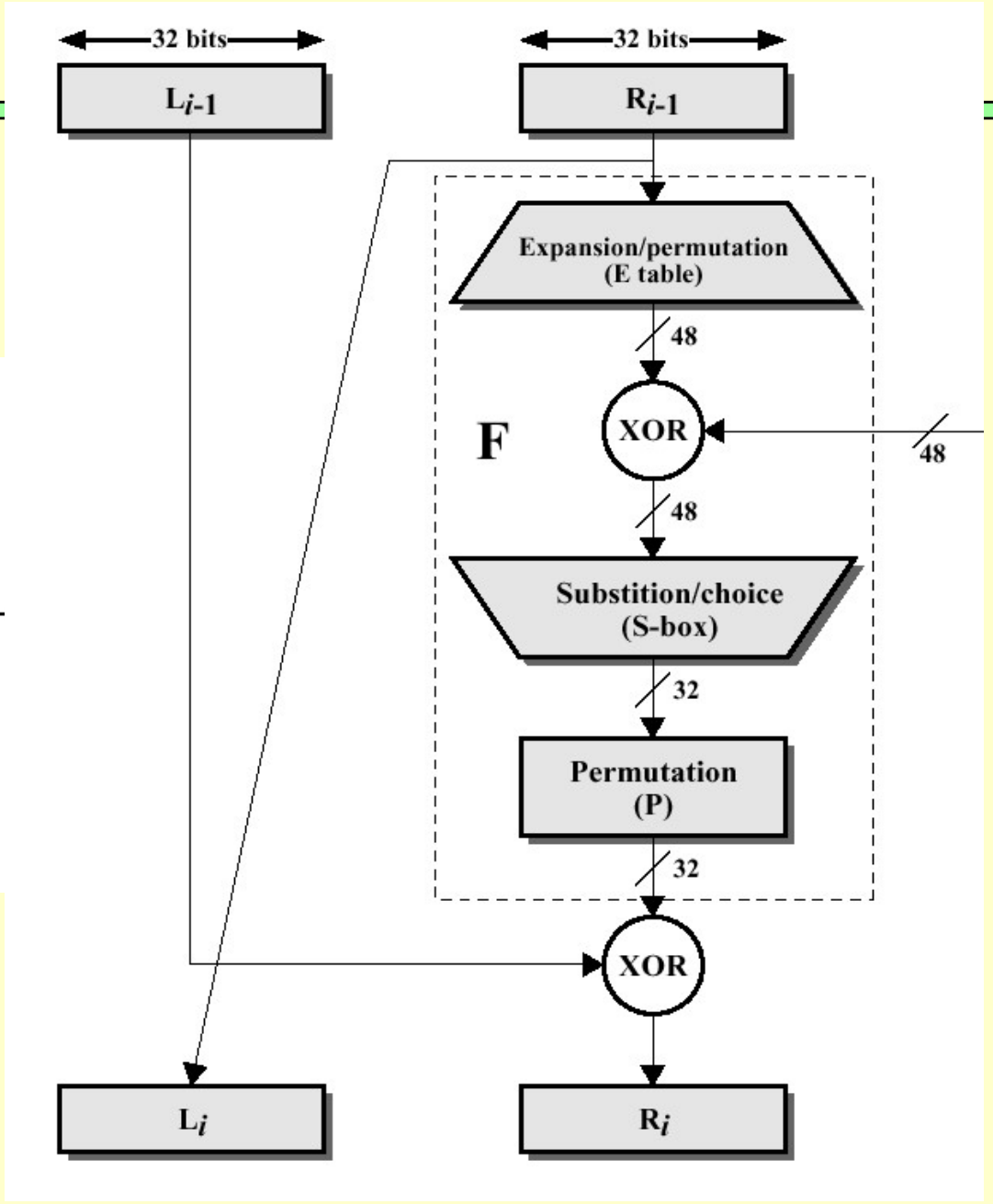


Figure 3.8 Single Round of DES Algorithm


8-bit plaintext
8
IP
4
4
f_K
E/P
F
8
8
4
4
S0
S1
2
2
P4
4
4


32 bits
32 bits
L_{i-1}
R_{i-1}
Expansion/permutation
(E table)
48
F
XOR
48
48
Substition/choice
(S-box)
32
Permutation
(P)
32
XOR
L_i
R_i

평문 : I LOVE ROSE BUT NOT DOG

I	빈칸	L	O	V	E	빈칸	R
01001001	00100000	01001100	01001111	01010110	01000101	00100000	01010010

O	S	E	빈칸	B	U	T	빈칸
01001111	01010011	01000101	00100000	01000010	01010101	01010100	00100000

N	O	T	빈칸	D	O	G	빈칸
01001110	01001111	01010100	00100000	01000100	01001111	01000111	00100000

초기순열 단계

- 64비트 평문 메시지 M

M1 M2 M3 M4 M5 M6 M7 M8
M9 M10 M11 M12 M13 M14 M15 M16
M17 M18 M19 M20 M21 M22 M23 M24
M25 M26 M27 M28 M29 M30 M31 M32
M33 M34 M35 M36 M37 M38 M39 M40
M41 M42 M43 M44 M45 M46 M47 M48
M49 M50 M51 M52 M53 M54 M55 M56
M57 M58 M59 M60 M61 M62 M63 M64

- 순열 X = IP(M)

M58 M50 M42 M34 M26 M18 M10 M2
M60 M52 M44 M36 M28 M20 M12 M4
M62 M54 M46 M38 M30 M22 M14 M6
M64 M56 M48 M40 M32 M24 M16 M8
M57 M49 M41 M33 M25 M17 M9 M1
M59 M51 M43 M35 M27 M19 M11 M3
M61 M53 M45 M37 M29 M21 M13 M5
M63 M55 M47 M39 M31 M23 M15 M7

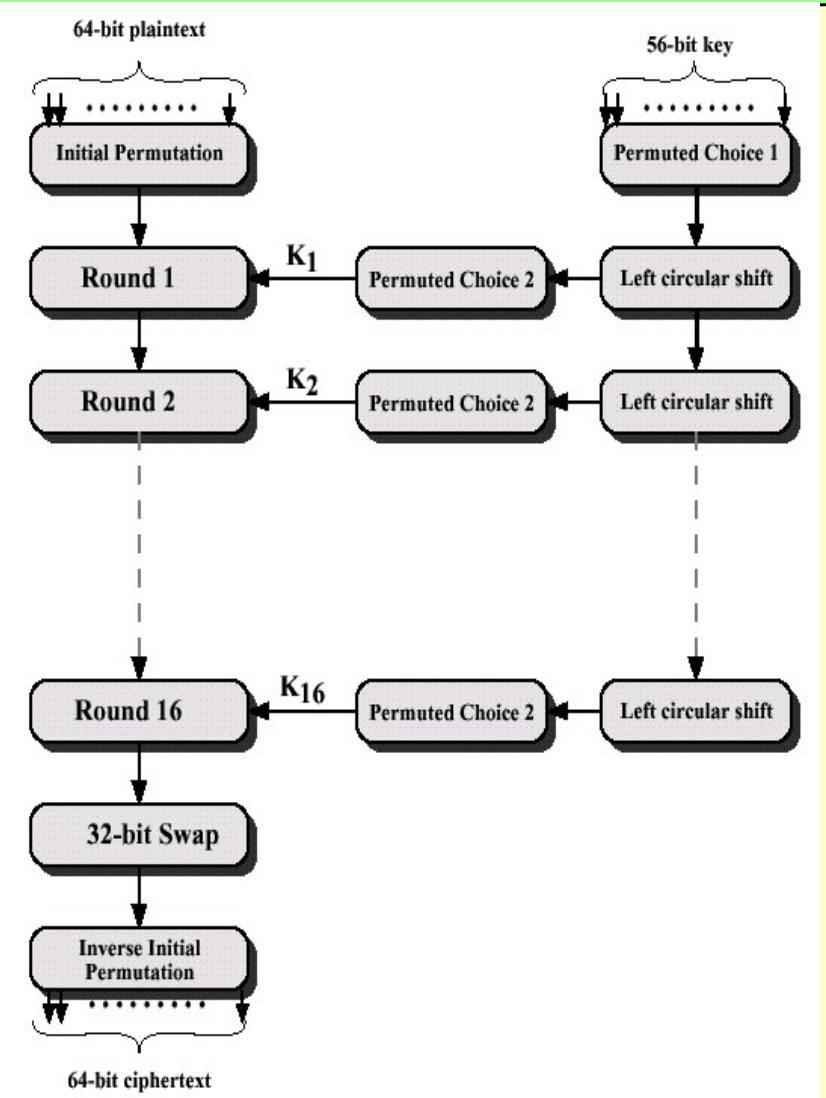


Figure 3.7 General Depiction of DES Encryption Algorithm

DES의 순열 표

- (a) 초기 순열 IP (64 → 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	61	43	35	27	19	11	3
61	63	45	37	29	21	13	5
63	55	47	39	31	23	15	7

- (b) 역초기 순열 IP^{-1} (64 → 64)

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

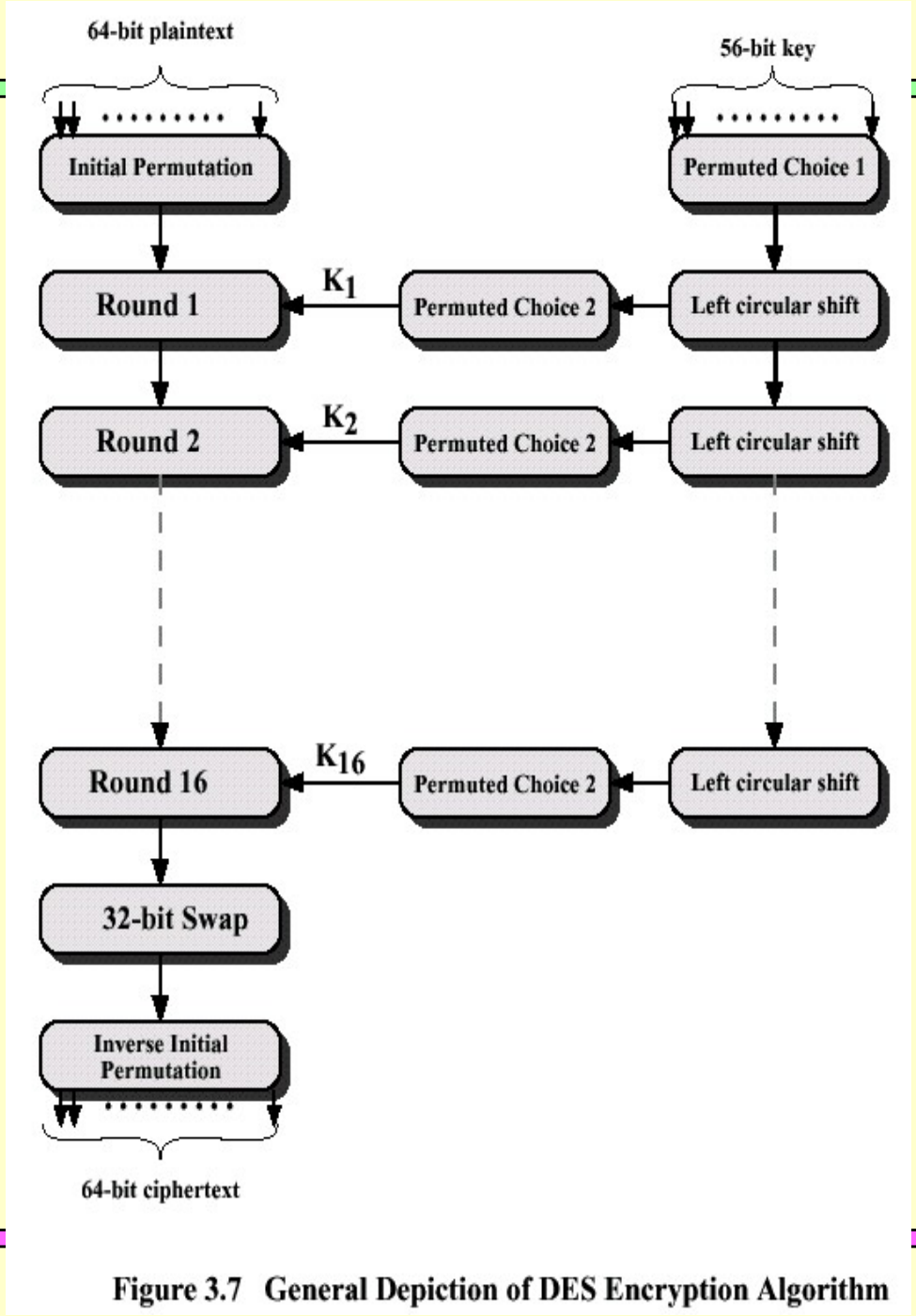


Figure 3.7 General Depiction of DES Encryption Algorithm

DES의 순열 표

(c) 확장순열(32 → 48)

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

(d) 순열함수(32 → 32)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	16	32	27	3	9
19	13	30	6	22	11	4	25

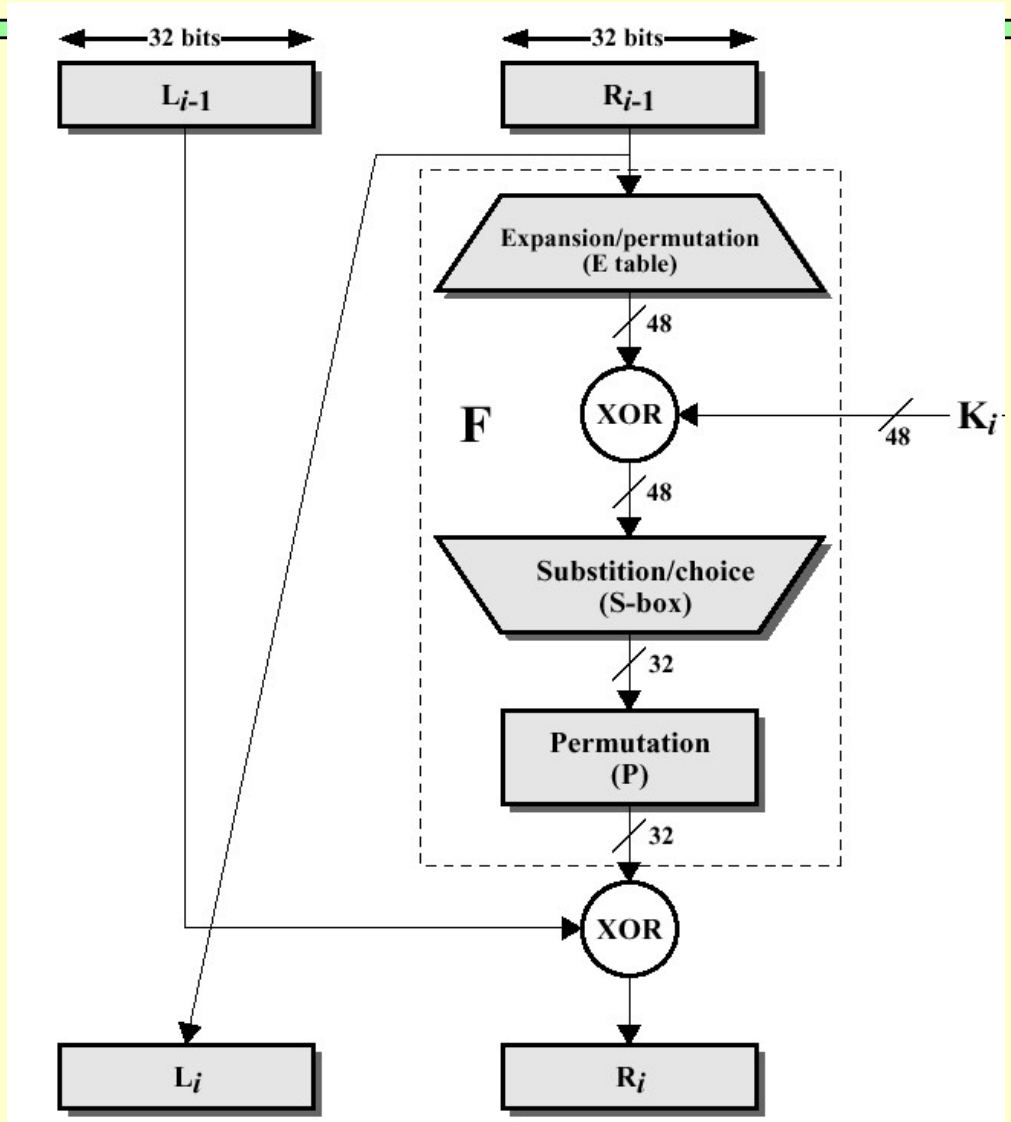
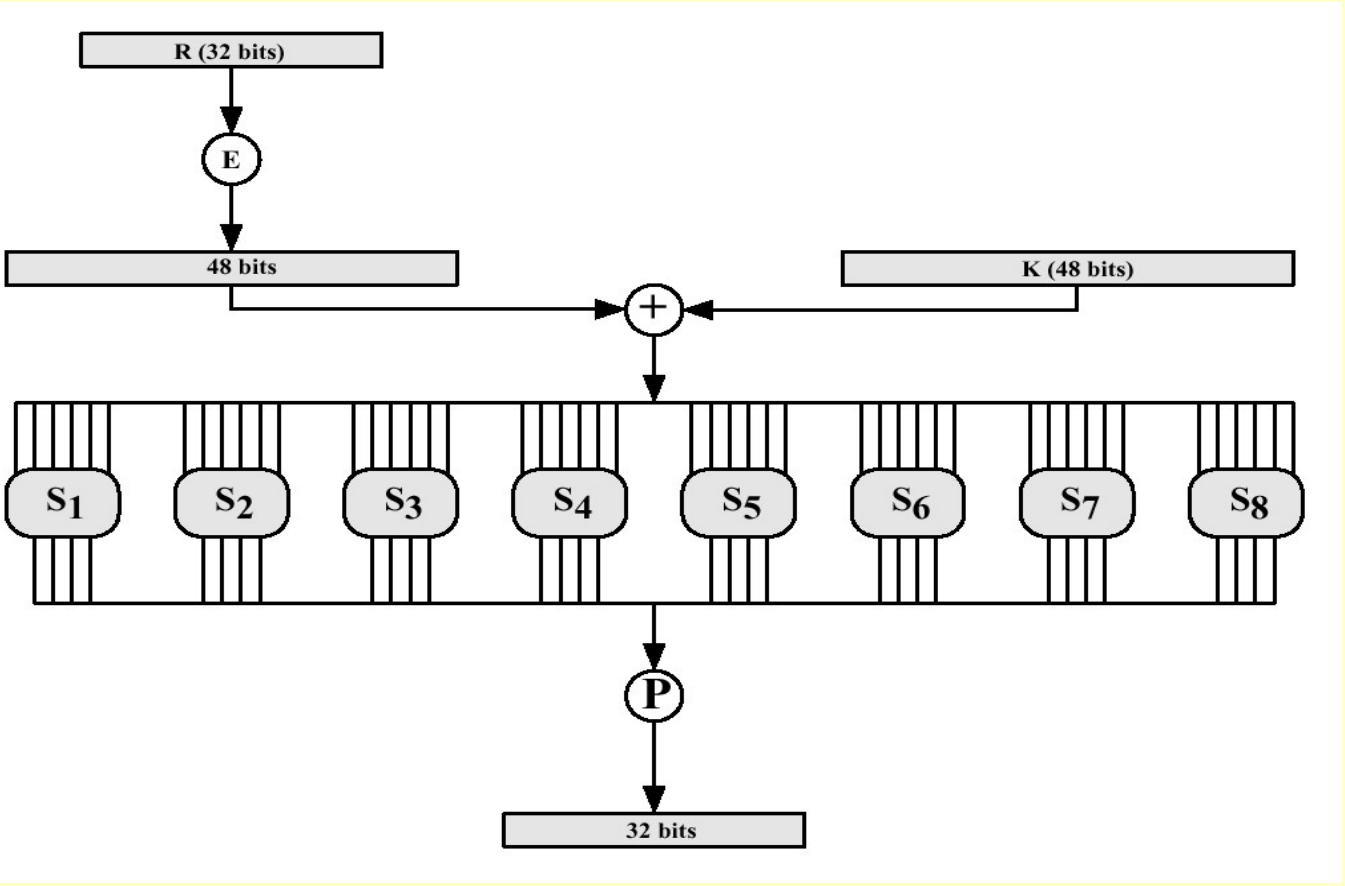


Figure 3.8 Single Round of DES

f 함수의 구성도

- 8개의 S-box로 구성
- 각 S-box는 6비트 입력, 4비트 출력 생성



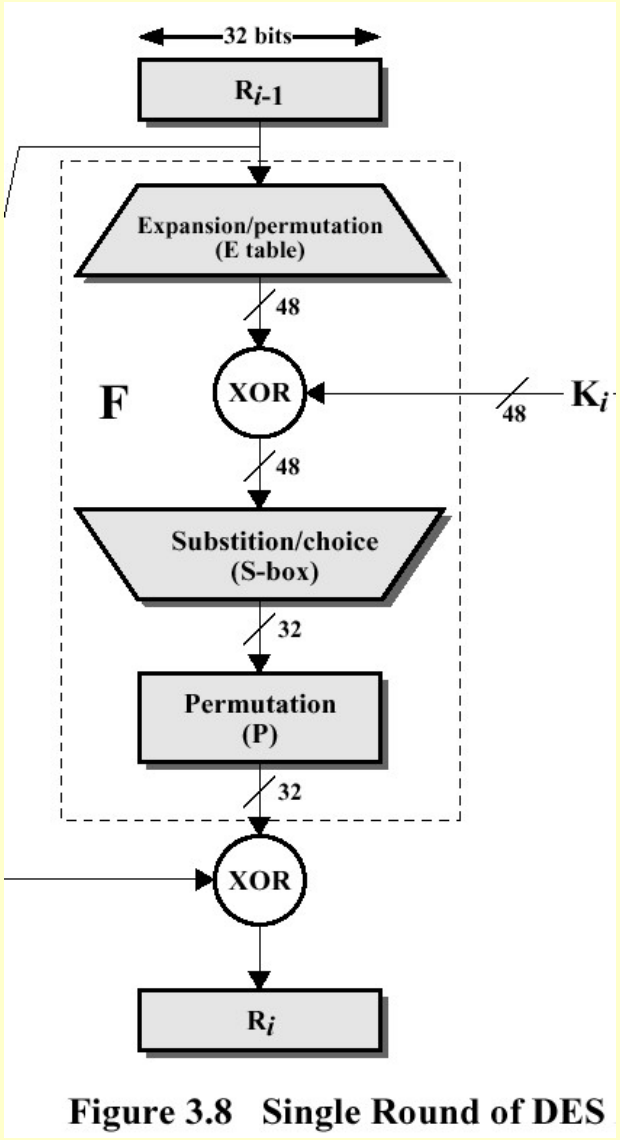


Figure 3.8 Single Round of DES

S-box Table

S1

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

❖ 예) 0 1 1 0 1 1 ------ 6비트 입력

행 (1행) 열 (13열) ➡ '011011'를 4비트로 출력 : "0 1 0 1"

Q1) 입력 110100의 출력은 ?

Q2) 입력 001001의 출력은 ?

DES의 기본 구조 (단일 반복 과정)

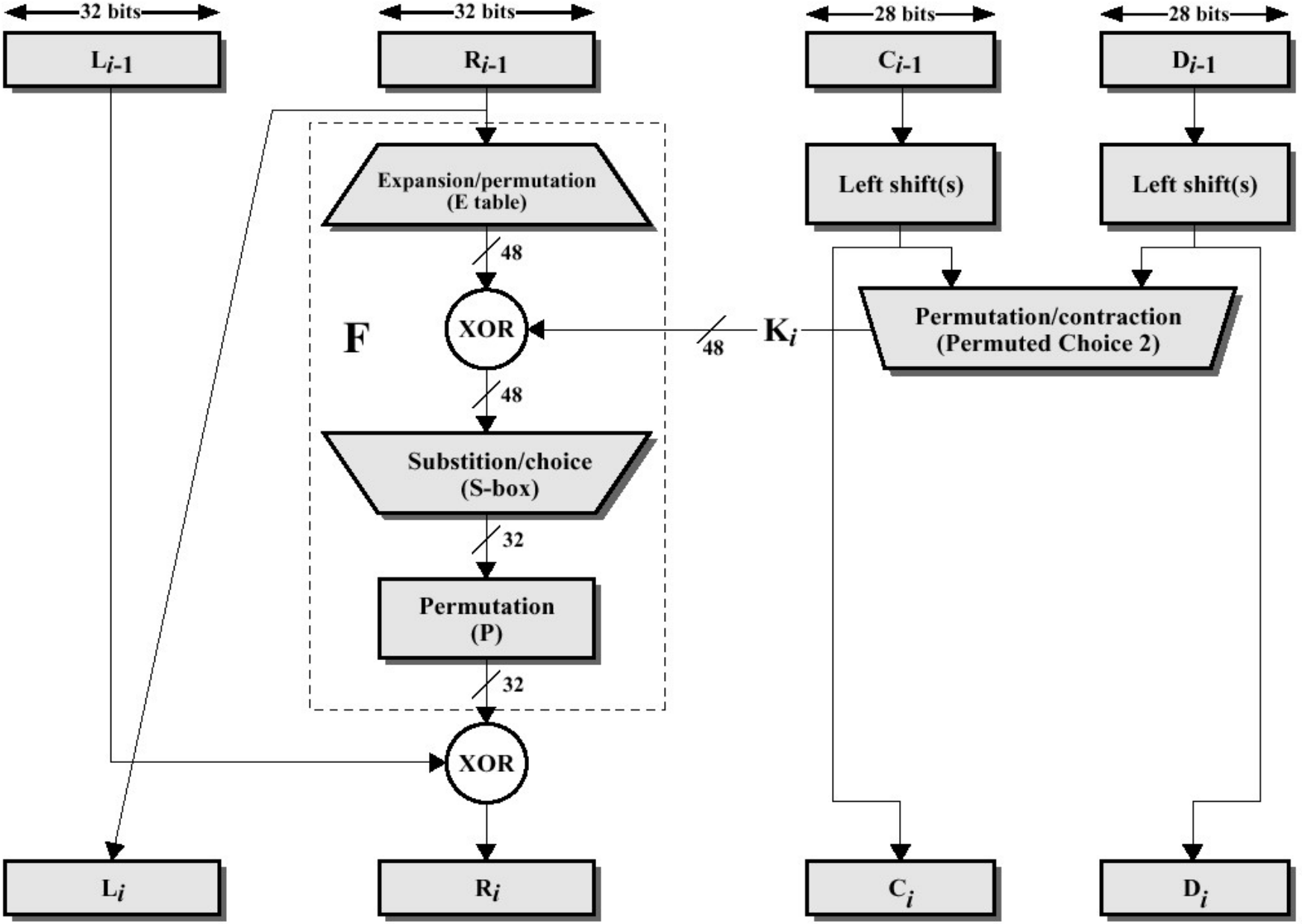
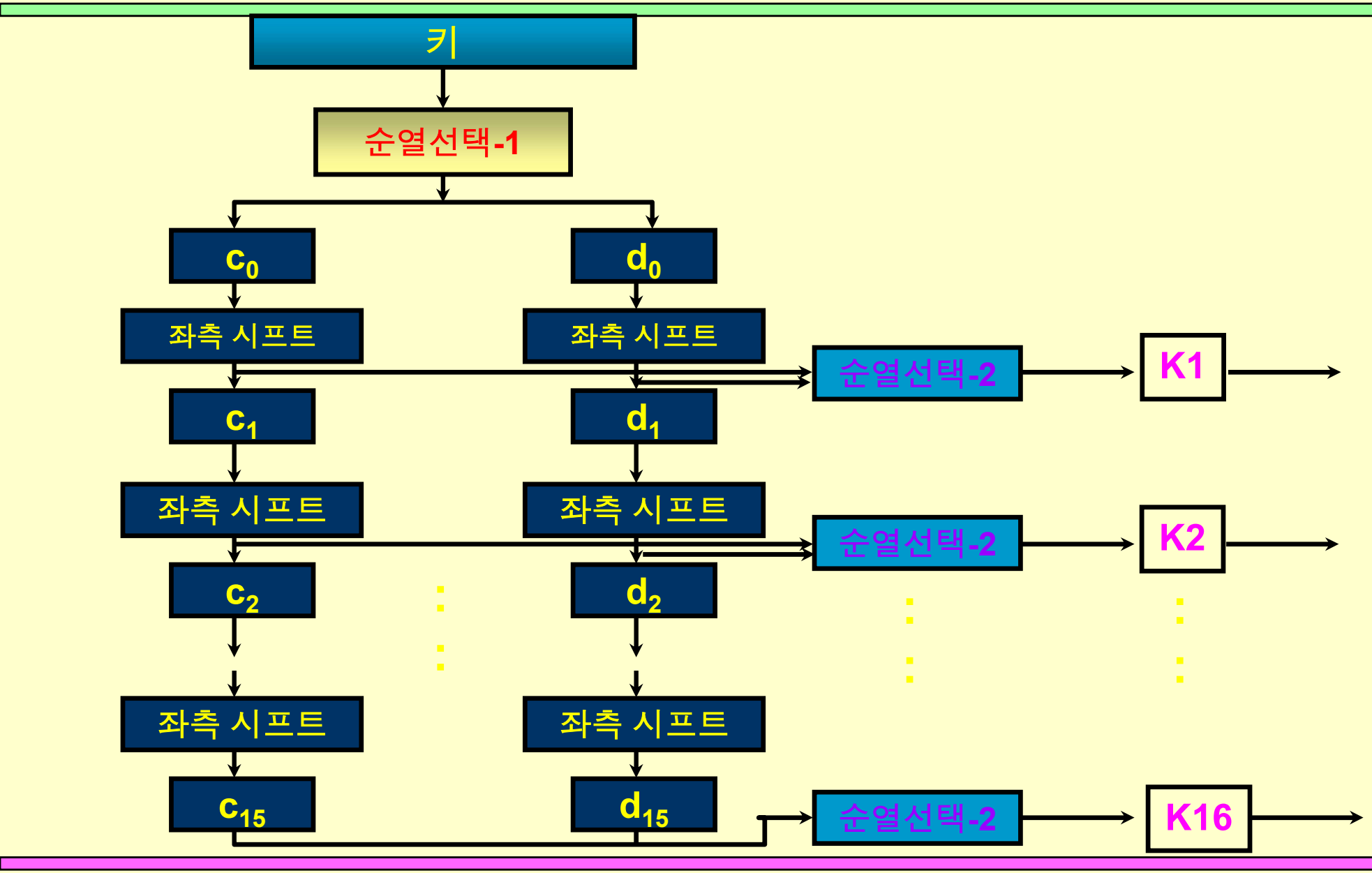


Figure 3.8 Single Round of DES Algorithm

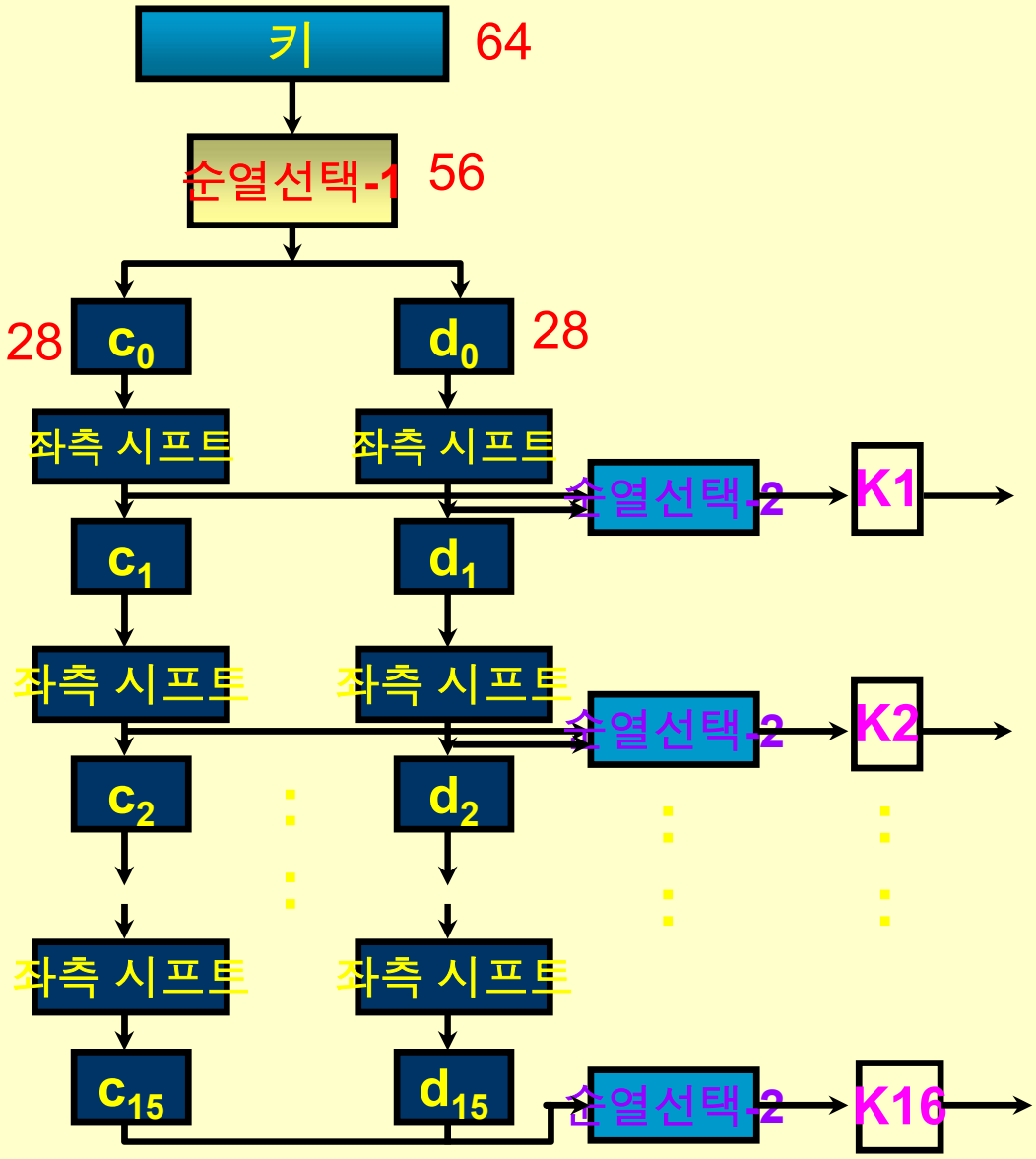
DES의 기본 구조 (키 생성부)



DES 키의 단계별 계산표

- 순열선택1 (PC-1)
  - 64➔ 56
  - C_0, D_0 : 각 28비트

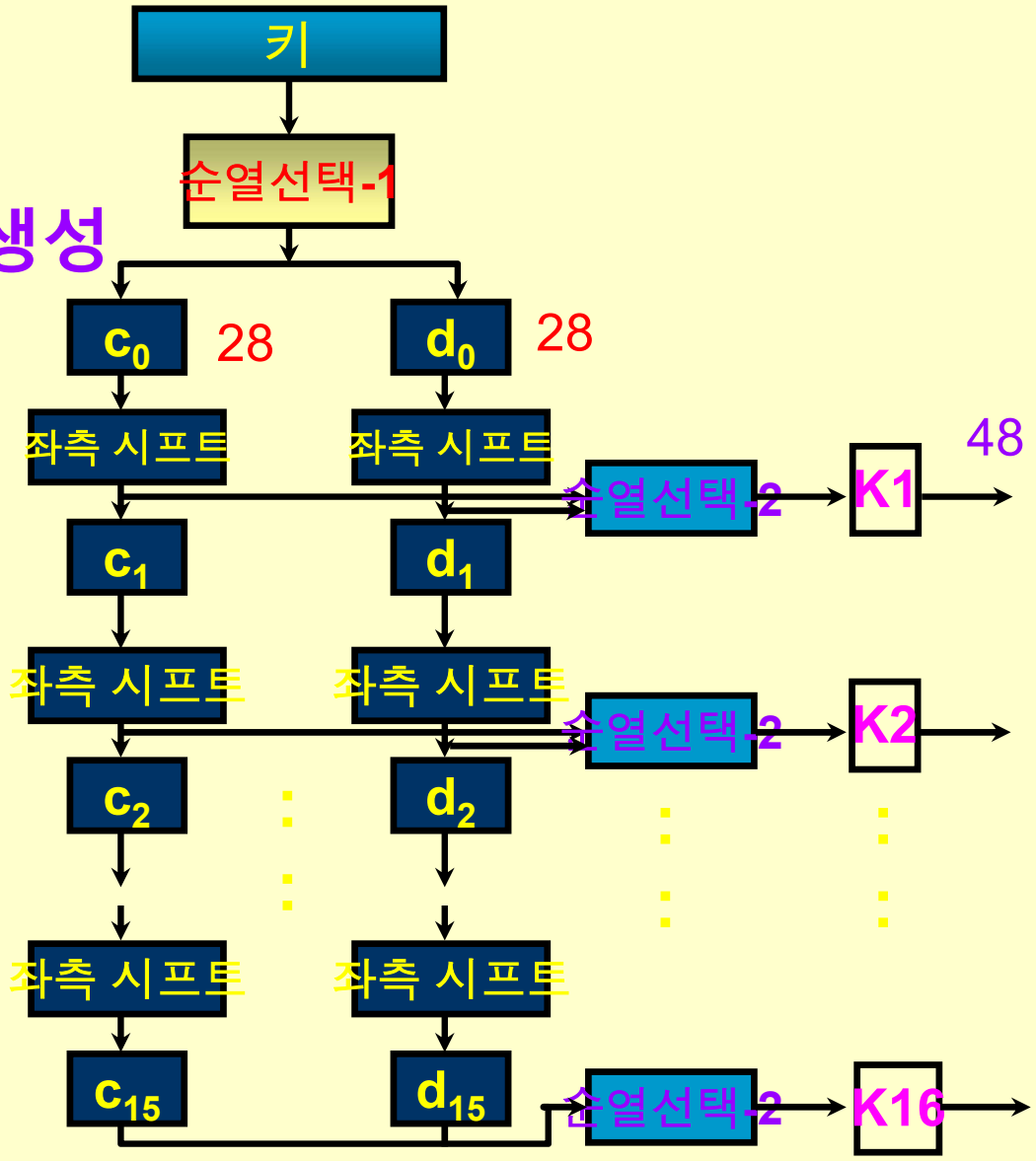
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4



DES 키의 단계별 계산표

- 순열선택2 (PC-2)
  - 56->48
  - 48비트 키 출력 생성

14	17	11	24	1	5
3	28	15	6	21	10
23	19	2	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	38
44	49	39	56	34	53
46	42	50	36	29	32



Key 쉬프트 스케줄

라운드 수	좌측 쉬프트 수
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

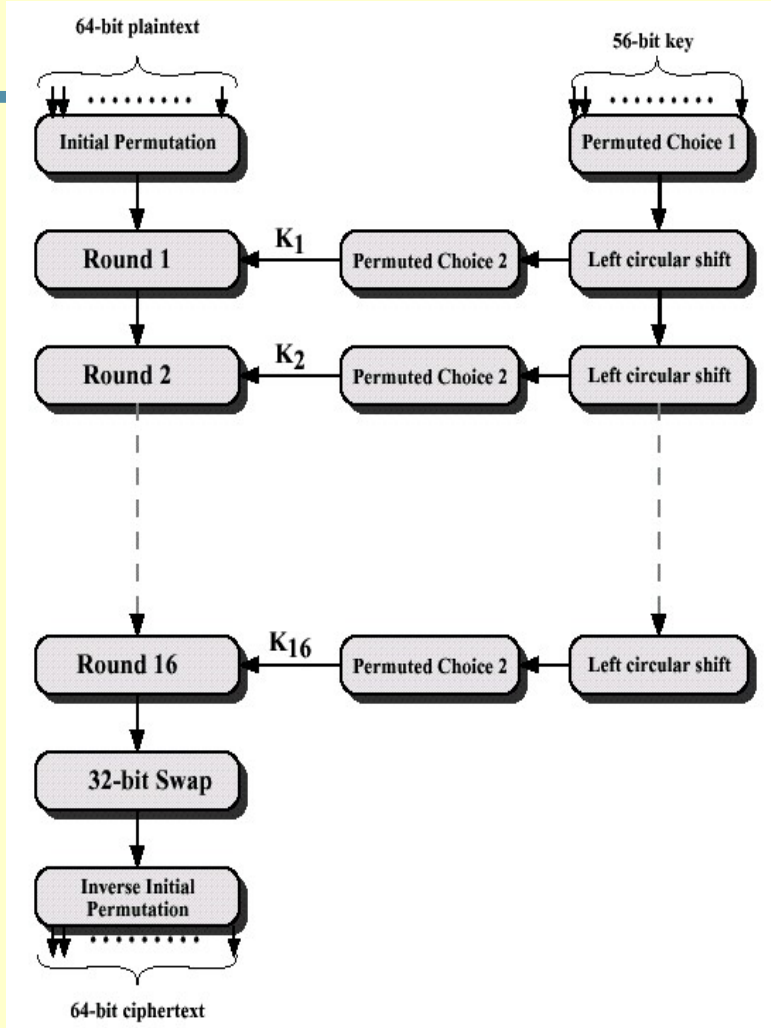


Figure 3.7 General Depiction of DES Encryption Algorithm

DES 복호화

- 서브키 역순 사용
- 암호화와 같은

  알고리즘 사용
- Feistel 구조

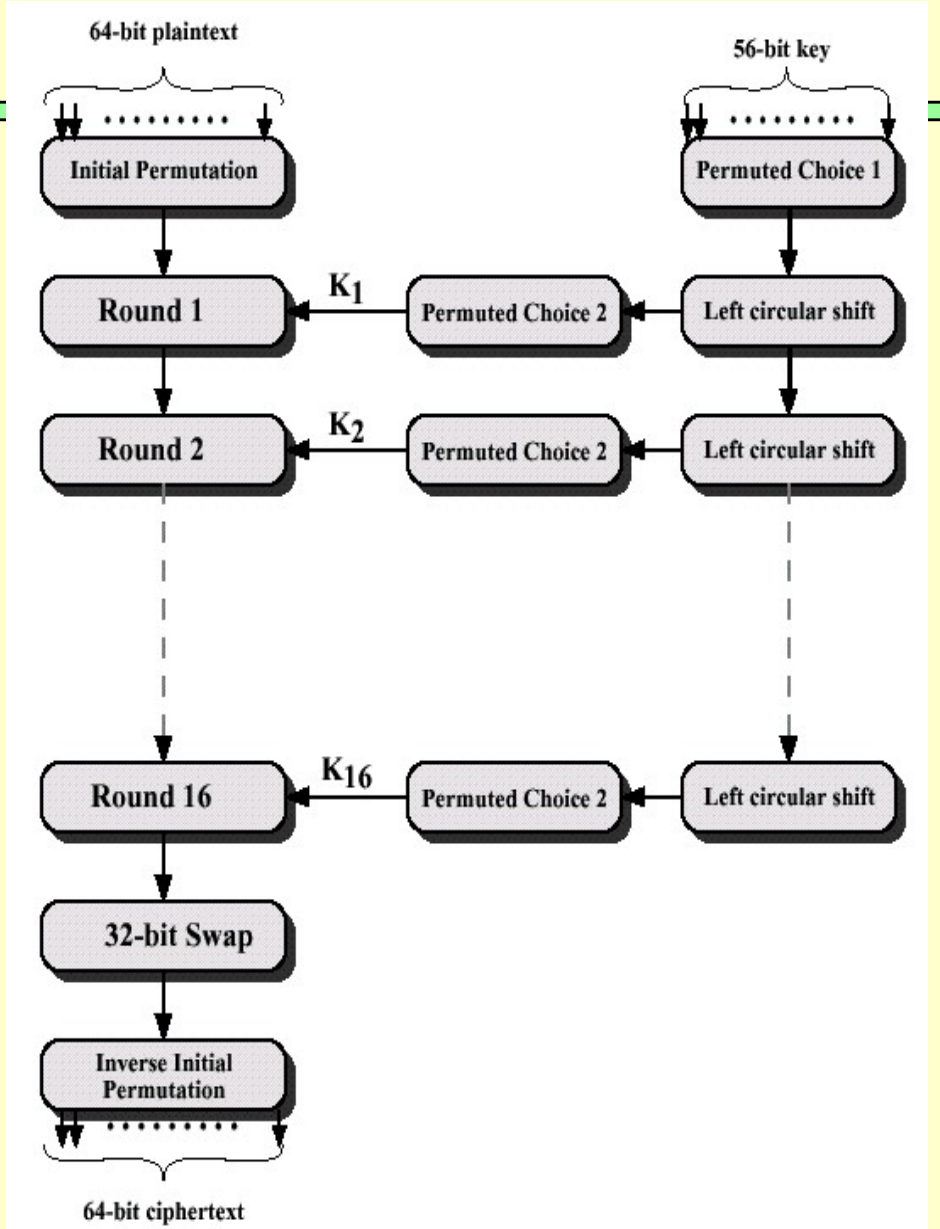


Figure 3.7 General Depiction of DES Encryption Algorithm

쇄도 효과(Avalanche Effect)

1개의 비트만 서로 다른 두 개의 평문 사용

평문1	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
평문2	10000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000

사용된 키

사용된 키	00000001	1001011	0100100	1100010	0011100	0011000	0011100	0110010

사용된 평문

평문	011010000	10000101	00101111	01111010	00010011	01110110	11101011	10100100

두개의 키는 1개의 비트만 다름

키 1	1110010	1111011	1101111	0011000	0011101	0000100	0110001	1101110
키 2	**0110010**	**1111011**	**1101111**	**0011000**	**0011101**	**0000100**	**0110001**	**1101110**

DES 쇄도 효과(Avalanche Effect) 예제

- 평문, 키, 암호화

Plaintext	02468aceeca86420
Key	0f1571c947d9e859
Ciphertext	da02ce3a89ecac3b

DES 예제

Plaintext	02468aceeca86420
Key	0f1571c947d9e859
Ciphertext	da02ce3a89ecac3b

Round	K_i	L_i	R_i
IP		5a005a00	3cf03c0f
1	1e030f03080d2930	3cf03c0f	Bad22845
2	0a31293432242318	Bad22845	99e9b723
3	230723118201d0c1d	99e9b723	0bae3b9e
4	05261d3824311a20	0bae3b9e	42415649
5	3325340136002c25	42415649	18b3fa41
6	123a2d0d04262a1c	18b3fa41	9616fe23
7	021f120b1c130611	9616fe23	67117cf2
8	1c10372a2832002b	67117cf2	C11bfc09
9	04292a380c341f03	C11bfc09	887fbc6c
10	2703212607280403	887fbc6c	600f7e8b
11	2826390c31261504	600f7e8b	F596506e
12	12071c241a0a0f08	F596506e	738538b8
13	300935393c0d100b	738538b8	C6a62c4e
14	311e09231321182a	C6a62c4e	56b0bd75
15	283d3e0227072528	56b0bd75	75e8fd8f
16	2921080b13143025	75e8fd8f	25896490
IP^{-1}		da02ce3a	89ecac3b

DES 쇄도효과: 평문 변화

Plaintext	02468aceeca86420
Key	0f1571c947d9e859
Ciphertext	da02ce3a89ecac3b

Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 acaca55ed16c3653	37
6	18b2fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682v2cefbc	32
8	67117cf2c11bf609 2b2cefbc99f91153	33

Round		δ
9	c11bfc09887fbc6c 99f911532eed7d94	32
10	887fbc6c600f7e8b 2eed7d94d0f23094	34
11	600f7e8bf596506e d0f23094455da9c4	37
12	f596506e738538b8 455da9c47f6e3cf3	31
13	738538b8c6a62c4e 7f6e3cf34bc1a8d9	29
14	6a62c4e56b0bd75 4bc1a8d91e07d409	33
15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
16	75e8fd8f25896490 1ce2e6dc365e5f59	32
IP^{-1}	da02ce3a89ecac3b 057cde97d7683f2a	32

DES 쇄도효과
: 키 변화

Plaintext	02468aceeca86420
Key	0f1571c947d9e859 1f1571c947d9e859
Ciphertext	da02ce3a89ecac3b

Round		δ
	02468aceeca86420 02468aceeca86420	0
1	3cf03c0fbad22845 3cf03c0f9ad628c5	3
2	bad2284599e9b723 9ad628c59939136b	11
3	99e9b7230bae3b9e 9939136b768067b7	25
4	0bae3b9e42415649 768067b75a8807c5	29
5	4241564918b3fa41 5a8807c5488dbe94	26
6	18b3fa419616fe23 488dbe94aba7fe53	26
7	9616fe2367117cf2 aba7fe53177d21e4	27
8	67117cf2c11bfc09 177d21e4548f1de4	32

Round		δ
9	c11bfc09887fbc6c 548f1de471f64dfd	34
10	887fbc6c600f7e8b 71f64dfd4279876c	36
11	600f7e8bf596506e 4279876c399fdc0d	32
12	f596506e738538b8 399fdc0d6d208dbb	28
13	738538b8c6a62c4e 6d208dbbb9bdeeaa	33
14	c6a62c4e56b0bd75 b9bdeeaad2c3a56f	30
15	56b0bd7575e8fd8f d2c3a56f2765c1fb	33
16	75e8fd8f25896490 2765c1fb01263dc4	30
IP^{-1}	da02ce3a89ecac3b ee92b50606b62b0b	30

쇄도 효과(Avalanche Effect)

- 평문이나 키의 작은 변화가 암호문에 대하여 중요한 변화 발생

(a) 평문상의 변화		(b) 키상의 변화	
반복	상이한 비트수	반복	상이한 비트수
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

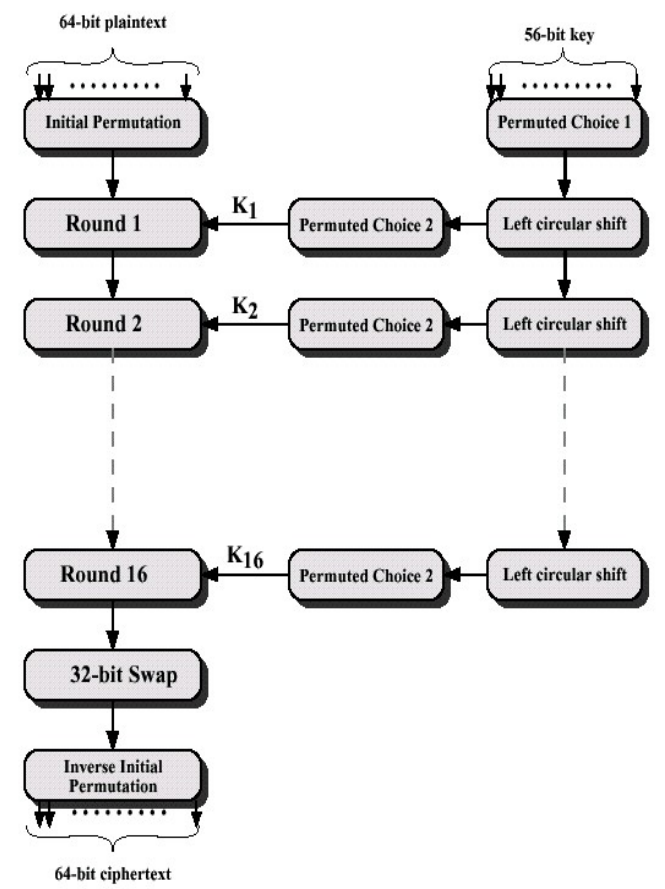


Figure 3.7 General Depiction of DES Encryption Algorithm

DES 키에 대한 고찰

56 비트 키 사용에 대한 우려

❖ 미 정부의 채택 이후 DES의 보안 수준에 대한 우려가 지속.

- 알고리즘의 성질을 이용한 암호 해독의 가능성
  - s - box의 약점에 대한 공격 가능성 주장 제기됨
  - back door에 대한 의문 ; 약점을 발견한 사람은 없음
- 키 길이에 관한 우려
  - Key Search Machine (기지 평문 공격)

Cost	Expected search Time
$ 100,000	35 hours
$1,000,000	3.5 hours
$10,000,000	21 minutes

❖ Brute force Attack

- 1970년대/80년대 : low computing power
- 90년대 : high computing power

Key size	Number of Alternative Keys	One Encryption per micro sec	10^6 Encryption per micro sec
32bits	$2^{23} = 4.3 * 10^9$	35.8 minutes	2.15ms
56bits	$2^{56} = 7.2 * 10^{16}$	1142years	10.01h
128bits	$2^{128} = 3.4 * 10^{38}$	10^{24}years	$5.4 * 10^{18}$ years

DES 알고리즘의 성질에 대한 우려

- DES 알고리즘 자체 성질을 이용한 해독 가능성
- 8개의 치환 표 또는 S-box
- S-box의 경우
  - 전체 알고리즘에 대한 설계기준이 공개된 적이 없다.
  - S-box의 약점에 대해 알고 있는 공격자가 해독할 수 있게 설계 됐을 가능성에 대한 의혹 제기
  - 수년간 S-box의 수많은 정규성과 예측 못할 동작이 발견
  - 그럼에도 S-box에 대하여 치명적인 약점을 발견한 사람은(적어도 그러한 발견이 공개된 적은)아직까지 없다.

- 비우호적인 국가에 의해 사용될 수 있다는 염려
- 미국 정부는 암호화 소프트웨어의 수출을 막고 있음
- 미국 수출 허용 기준인 40비트의 키
  - Michael Wienerd의 key search machine으로 0.2초만에 해독 가능
- 소프트웨어의 프리버전은 BBS나 웹사이트 등에서 쉽게 입수

DES암호 공격

- DES Challenge I
  - 1997년 2월에는 RSA사에서 개최(10,000달러 상금)
  - 78,000대의 컴퓨터를 이용하여 96일
  - 인터넷상에서 14,000명 이상의 사용자들이 공동으로 참가
  - 가능한 72천조 개의 키 중에서 고작 18천조 개의 시험을 통해 그 키가 발견
  - 72,000,000,000,000,000 (72천조)개
- DES Challenge II
  - 1998년 7월
  - 250,000달러의 전용칩을 제작하여 56시간
- DES Challenge III
  - 1999년 1월 18일 1만 여대의 컴퓨터와 전용칩을 이용
  - 22시간 15분만에 해독