Data Encryption Standard(DES)

컴퓨터공학부 김상원

https://youtu.be/zej1OyGGnlU

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

DES 개요

DES 주요특징

DES 알고리즘

DES의 한계

DES개요

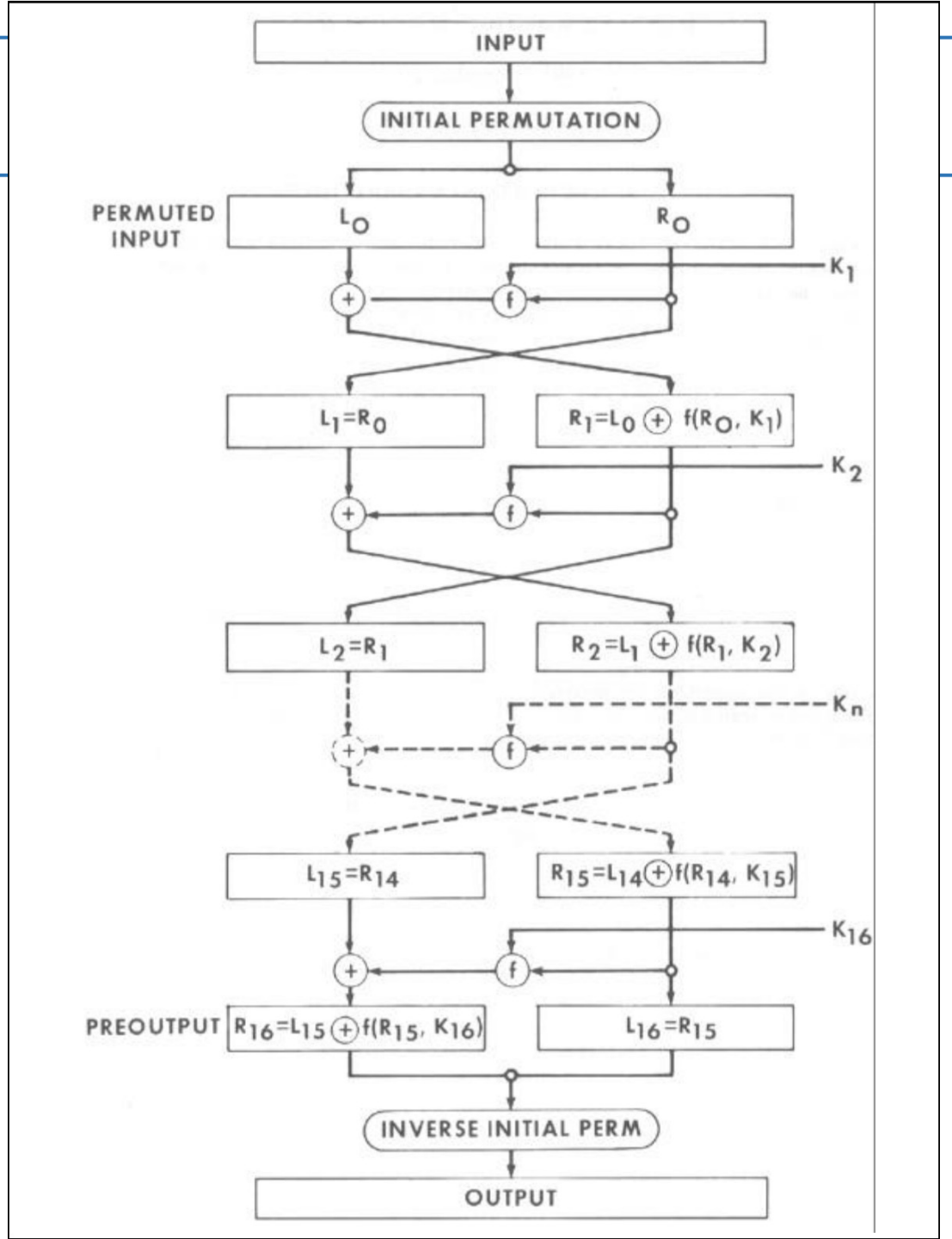
1972년에 미국 NBS (National Bureau of Standards, 오늘날의 NIST)는 암호 기술의 필요성을 절감하고 미국 정부 규모의 표준적인 암호 알고리즘을 개발하기로 했다. 이에 1974년 8월 27일, IBM에서 루시퍼 암호 알고리즘을 제안했고, 이를 수정하여 1975년 3월 17일에 **DES**를 발표했다.

DES(Data Encryption Standard)는 64비트의 평문을 46비트의 암호문으로 만드는 블록암호 시스템으로 64비트의 키를 사용한다. **데이터 암호화 표준**이라고 한다. 64비트의 키(외부 키)중에서 56비트는 실제의 키(내부 키)가 되고 나머지는 거사용 비트로 사용된다.

DES의 주요 특징

- DES의 구조 : 파이스텔 암호(Feistel cipher)
- 64 bit block length
- 56 bit key length(+8 Parity Bit)
- 16 rounds
- 48 bits of key used each round (subkey)
- 암호 알고리즘의 안정성은 주로 “S-boxes”에 달려있다.

DES 알고리즘


INPUT
INITIAL PERMUTATION
PERMUTED INPUT
L_0
R_0
K_1
$L_1=R_0$
$R_1=L_0 \oplus f(R_0, K_1)$
K_2
$L_2=R_1$
$R_2=L_1 \oplus f(R_1, K_2)$
K_n
$L_{15}=R_{14}$
$R_{15}=L_{14} \oplus f(R_{14}, K_{15})$
K_{16}
PREOUTPUT
$R_{16}=L_{15} \oplus f(R_{15}, K_{16})$
$L_{16}=R_{15}$
INVERSE INITIAL PERM
OUTPUT

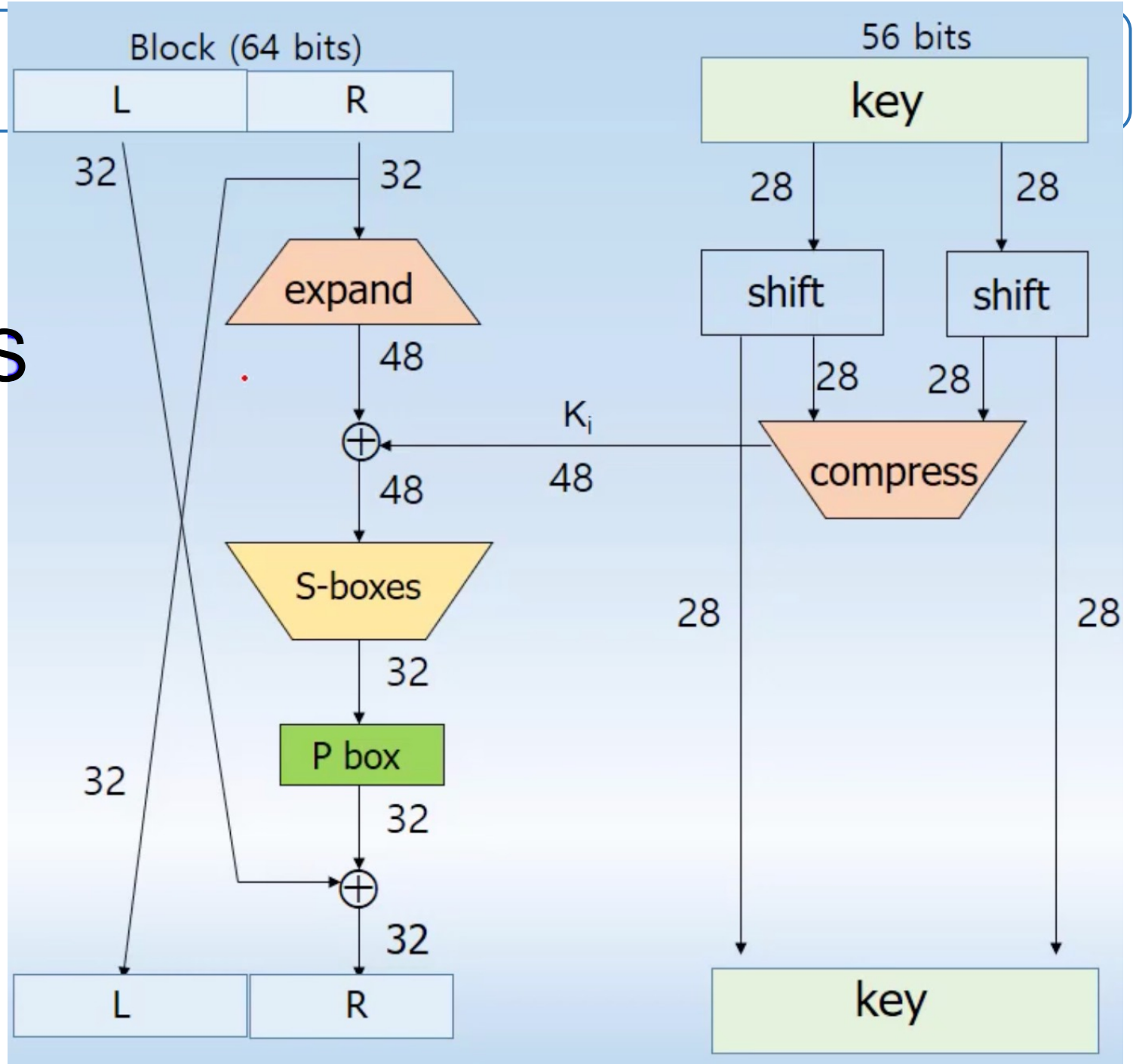
DES 알고리즘

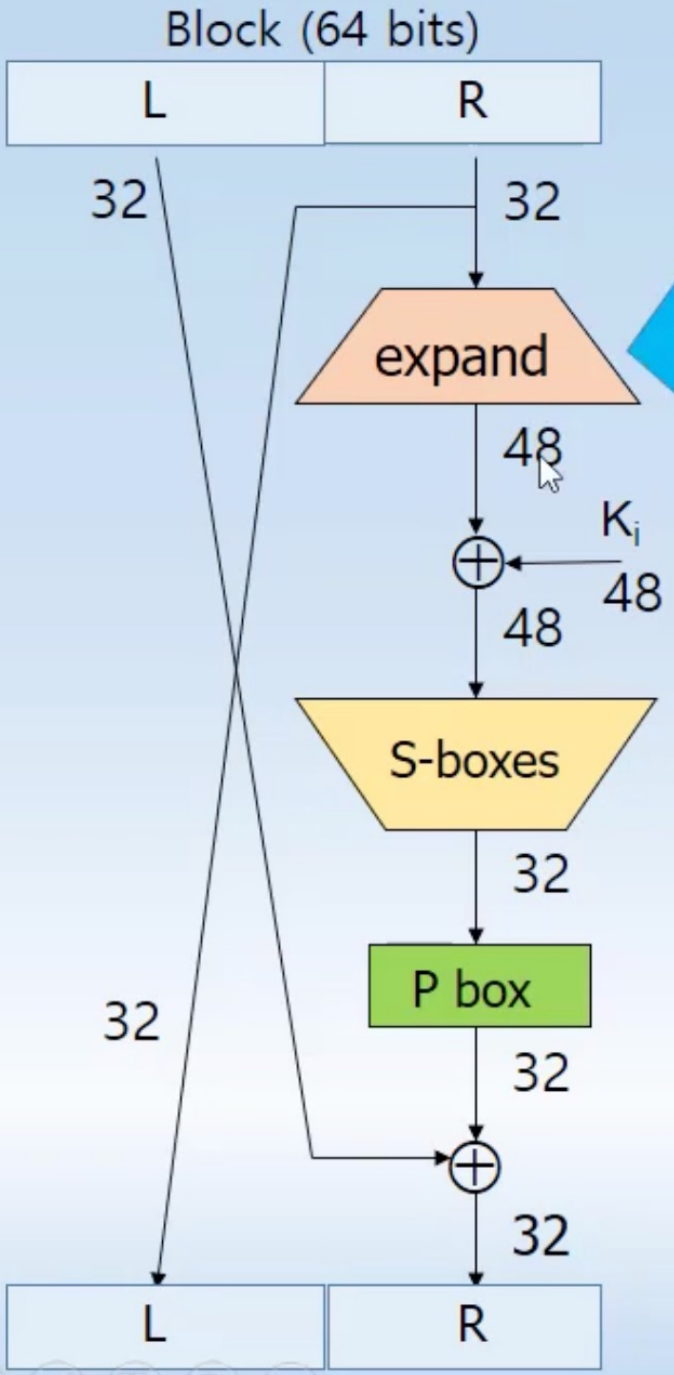
- Initial Permutation

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

One Round of DES





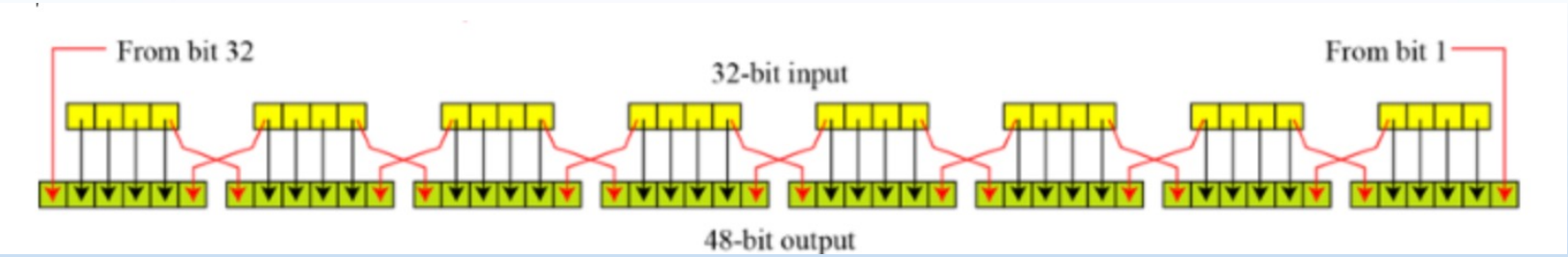
Input 32 bits

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Expand permutation

output 48 bits

31	0	1	2	3	4	3	4	5	6	7	8
7	8	9	10	11	12	11	12	13	14	15	16
15	16	17	18	19	20	19	20	21	22	23	24
23	24	25	26	27	28	27	28	29	30	31	0



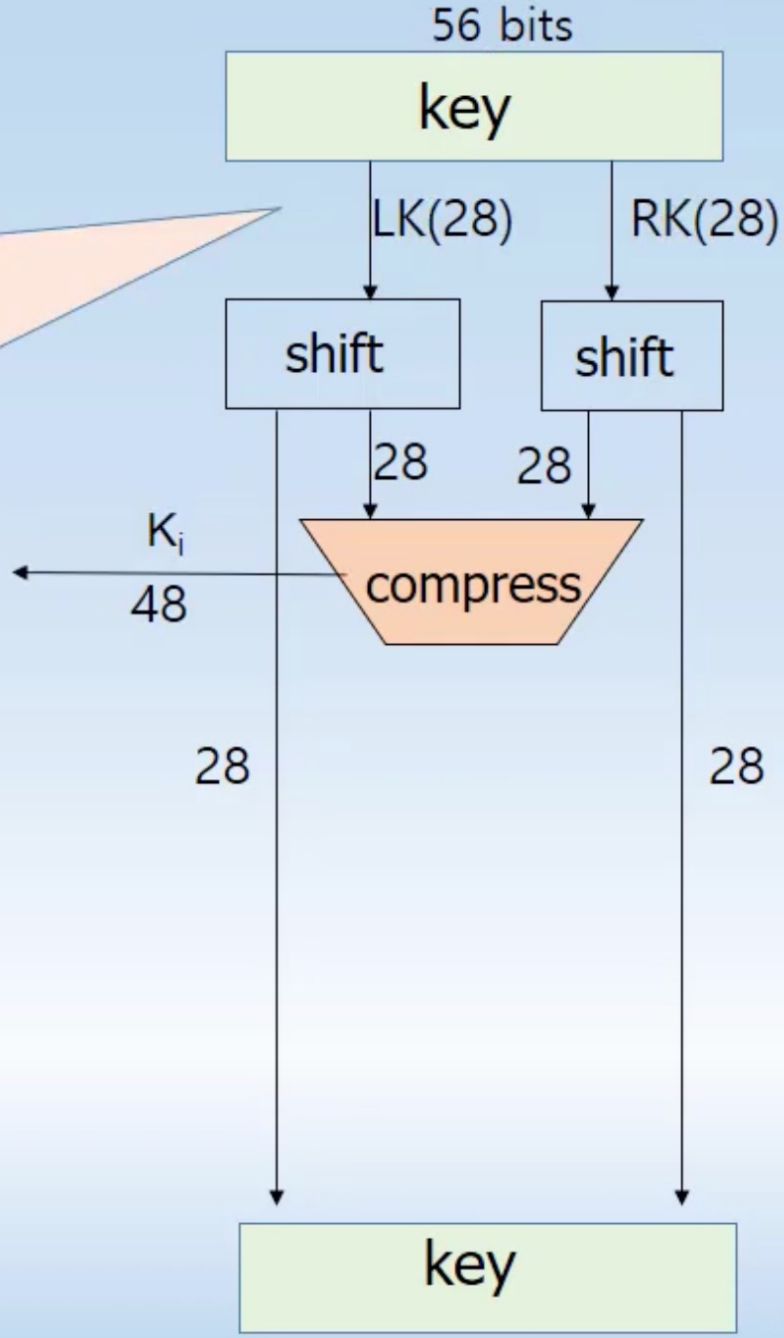
56 bits (0,1,2,...,55) key

Left half key bits: LK (28bits)

49	42	35	28	21	14	7
0	50	43	36	29	22	15
8	1	51	44	37	30	23
16	9	2	52	45	38	31

Right half key bits: RK (28bits)

55	48	41	34	27	20	13
6	54	47	40	33	26	19
12	5	53	46	39	32	25
18	11	4	24	17	10	3



For rounds i=1,2,...,16

Let LK = (LK circular shift left by r_i)

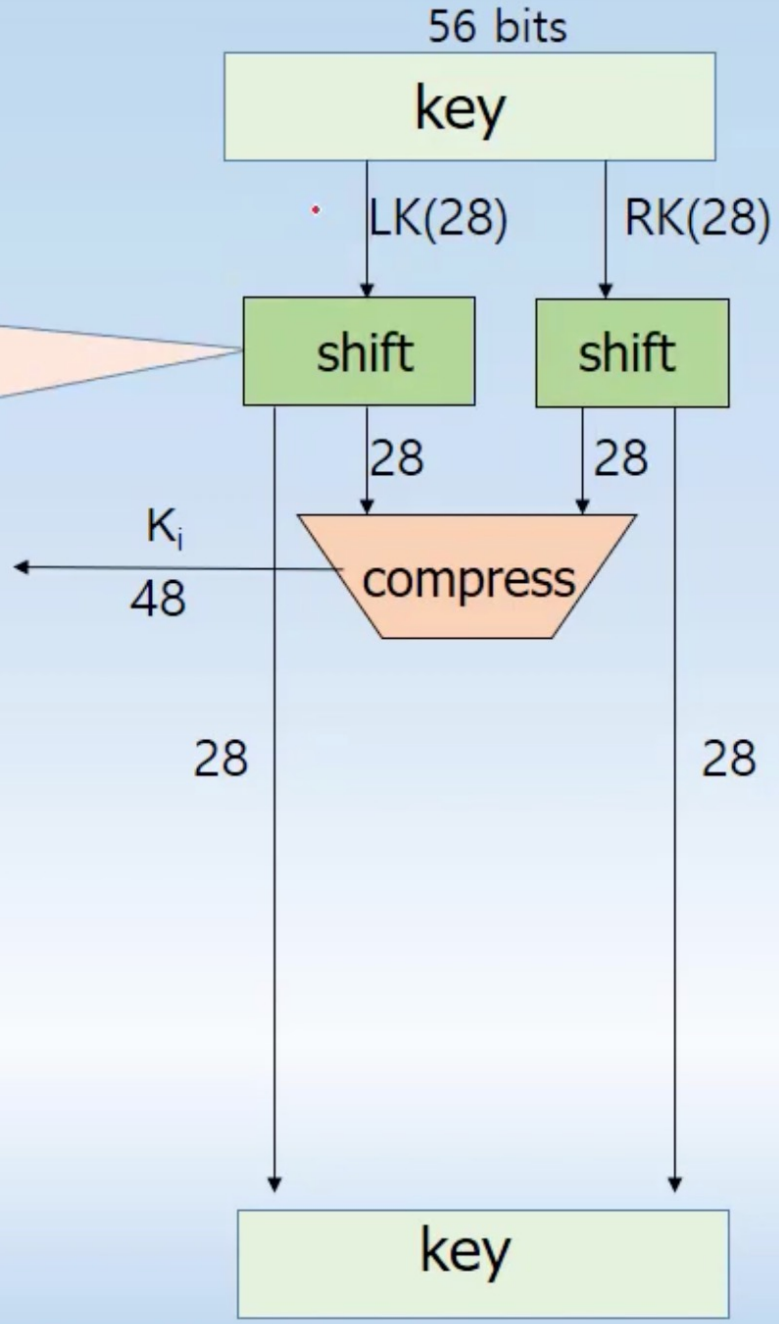
Let RK = (RK circular shift left by r_i)

For rounds 1, 2, 9, 16,

r_i is 1

For all other rounds,

r_i is 2



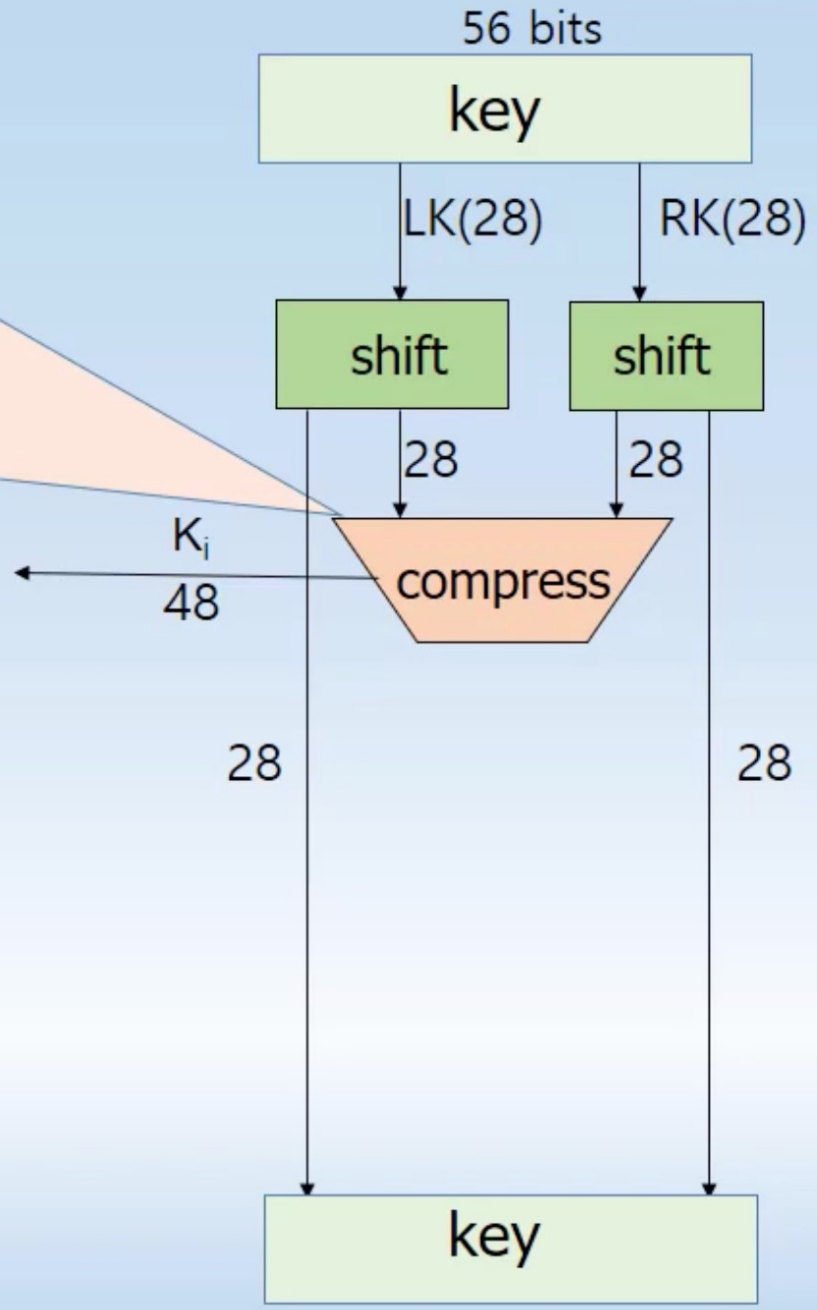
Left half of subkey K_i is of LK bits

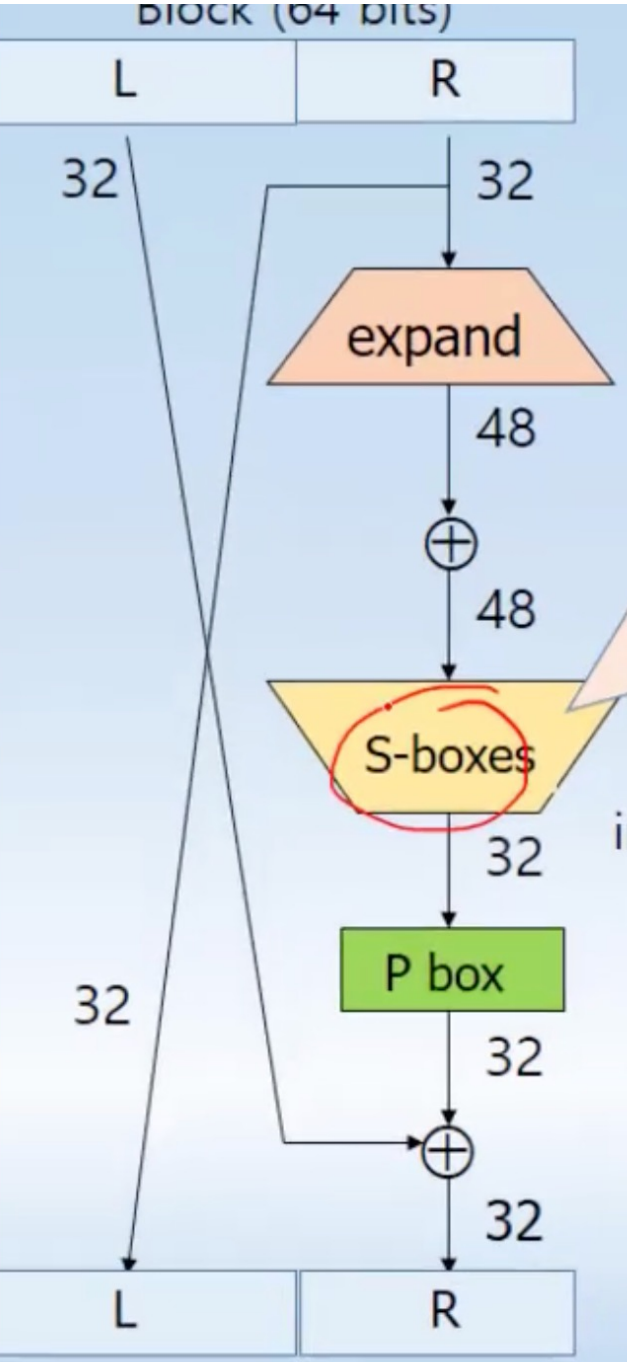
13	16	10	23	0	4	2	27	14	5	20	9
22	18	11	3	25	7	15	6	26	19	12	1

Right half of subkey K_i is RK bits

12	23	2	8	18	26	1	11	22	16	4	19
15	20	10	27	5	24	17	13	21	7	0	3

(bits 8,17,21,24 of LK omitted each round
bits 6,9,14,25 of RK omitted each round)





input bits (0,5)

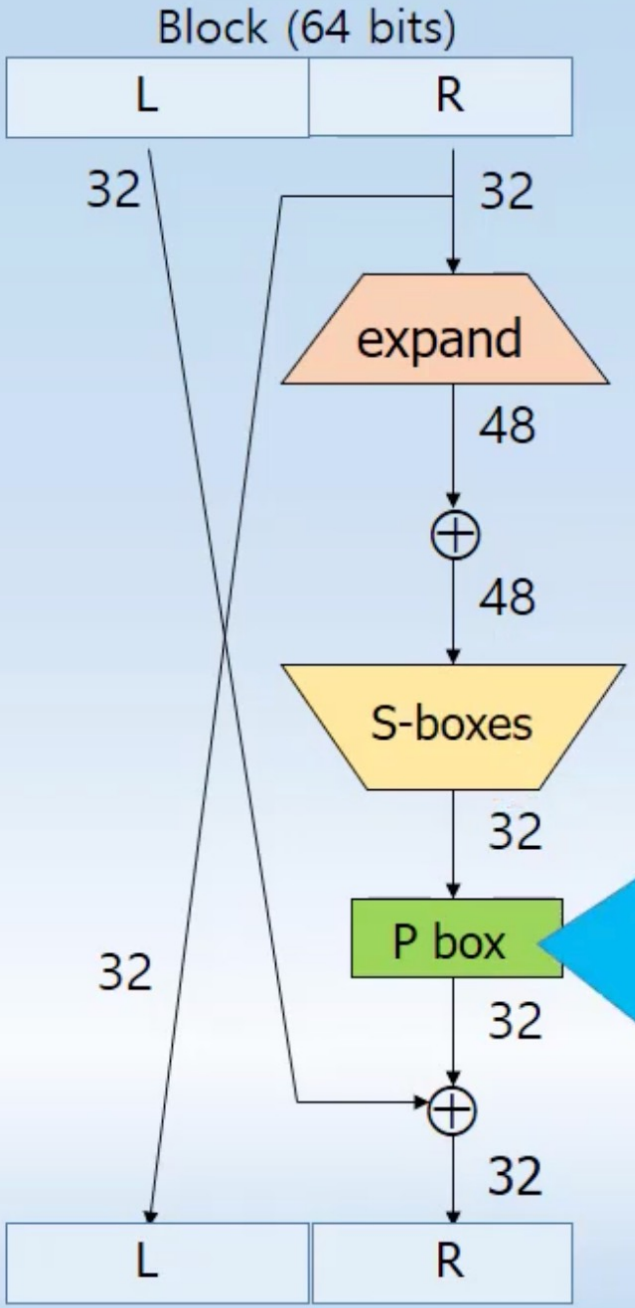
8개의 "substitution boxes"(S-boxes)

각 S-box는 6 bits를 4 bits로 매핑 (8x6=48 ⇒ 8x4=32bits)

첫번째 S-box의 치환 테이블

input bits(1,2,3,4)

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	1110	0001	1101	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111	1111	0010
11	1111	1100	1000	0010	0111	1101	0001	0110	1011	0011	1110	0101	1010	0000	1001	0100



Input 32 bits

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

permutation

output 32 bits

15	6	19	20	28	11	27	16	0	14	22	25	4	17	30	9
1	7	23	13	31	26	2	8	18	12	29	5	21	10	3	24

DES 알고리즘

- Feistel 네트워크의 16라운드를 모두 완료하면 결과적으로 왼쪽과 오른쪽 절반이 교체됩니다.
- 그런 다음 교체된 절반이 결합되어 64비트 블록을 형성합니다.
- 64비트 블록은 FP(Final Permutation)라는 고정 순열 테이블을 사용하여 다시 순열됩니다.
- 최종 순열의 출력은 암호화 또는 복호화 데이터입니다.

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

DES의 한계

- DES는 현재 취약한 것으로 알려져 있다. 56비트의 키 길이는 현재 컴퓨터 환경에 비해 너무 짧다는 것이 하나의 원인이며, DES에 백도어가 포함되어 있어 특수한 방법을 사용하면 정부 기관에서 쉽게 해독할 수 있을 것이라는 주장도 제기되었다. 1998년에 전자 프론티어 재단(EFF)에서는 56시간 안에 암호를 해독하는 무차별 대입 공격 하드웨어를 만들었으며, 1999년에는 22시간 15분 안에 해독하는 하드웨어를 만들었다.

- DES를 세 번 반복해서 사용하는 Triple-DES는 DES에 비해 안전한 것으로 알려져 있으며, 또한 현재는 DES 대신 AES(Advanced Encryption Standard)가 새 표준으로 정해져 사용되고 있다.

Q & A