# 블록암호 : DES

1871005 강예준

한성대학교 HANSUNG UNIVERSITY

유튜브 주소 : https://youtu.be/nZjfuFE5C7U

CryptoCraft LAB
https://crypto.modoo.at

# Contents



CryptoCraft LAB

# 01. 블록암호란?

# 01. 블록암호란?

- 블록암호
  - 평문을 블록 단위로 나눠서 암호화하는 대칭키 암호 시스템

# 01. 블록암호란?

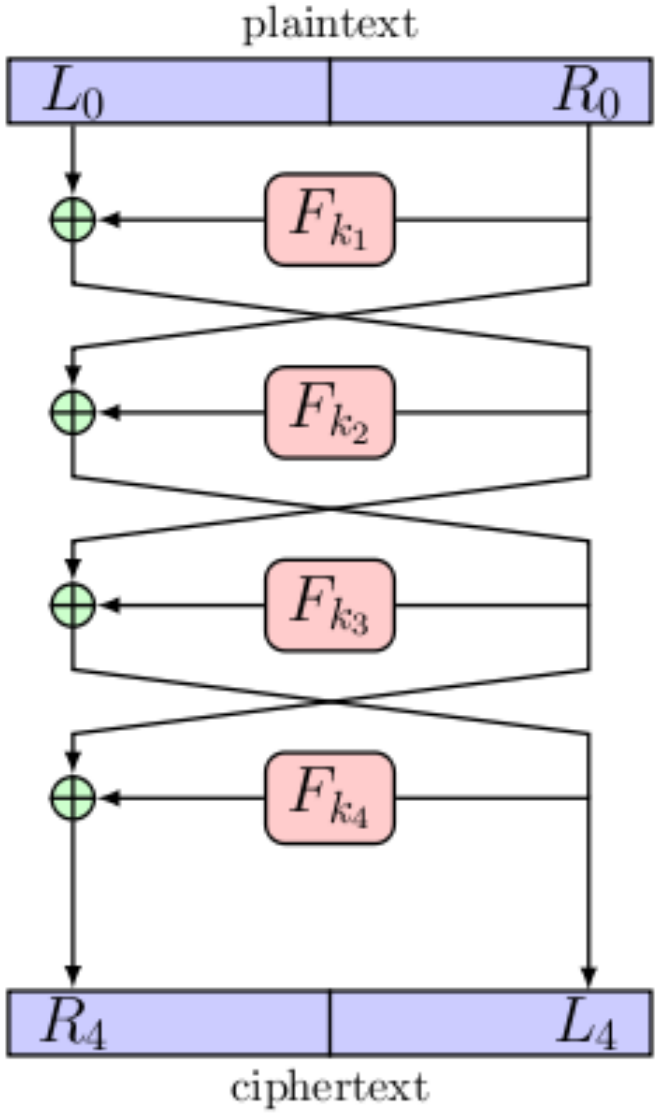
- 혼돈 (Confusion)
  - 평문과 암호문의 관계를 없애는 성질

- 확산(Diffusion)
  - 평문을 이루는 하나의 비트가 암호문의 여러 개의 비트에 영향을 끼치는 성질

# 01. 블록암호란?

- Feistel 구조
  - 평문의 블록을 좌우로 나눈다.
  - 암호화하는 특정 계산 함수를 반복한다.
  - 출력값은 다음 라운드의 입력값이 된다.
  - DES, SEED, BLOWFISH 등

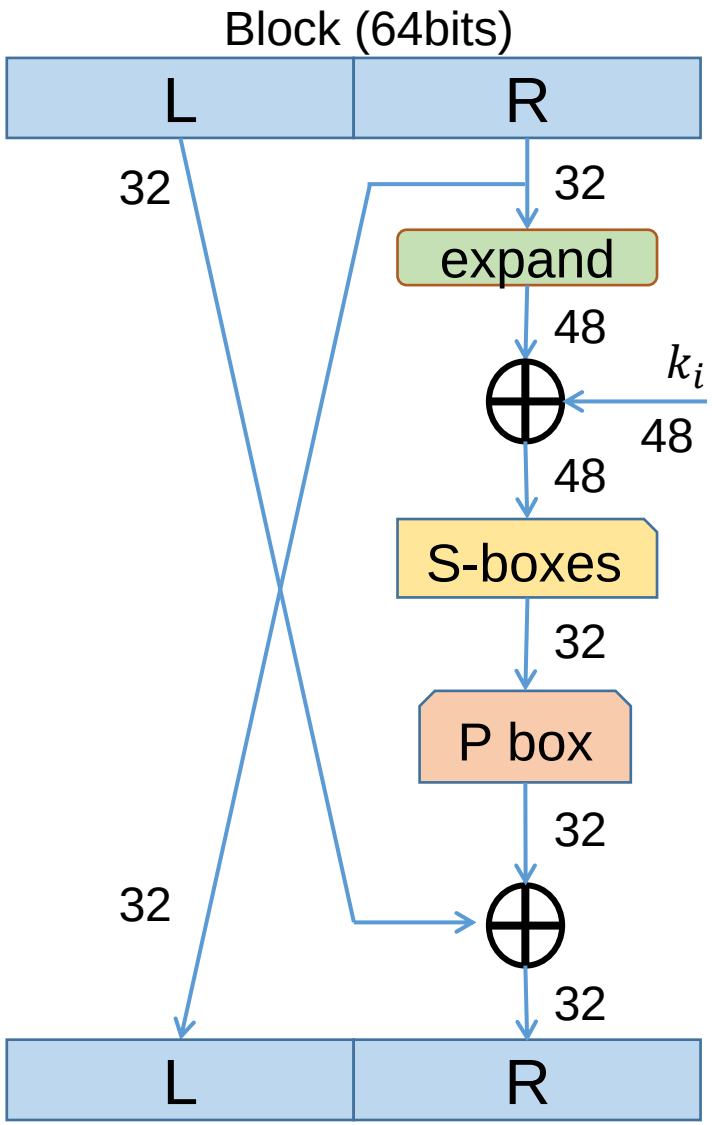
- SPN 구조



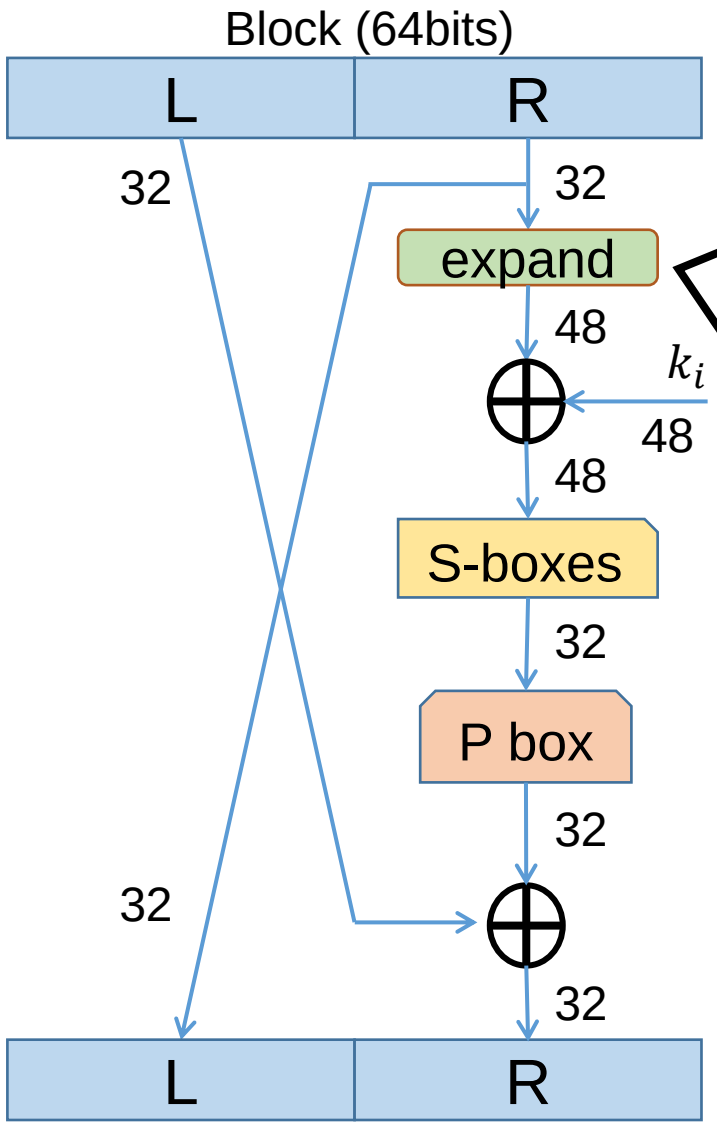
# 02. DES의 구조

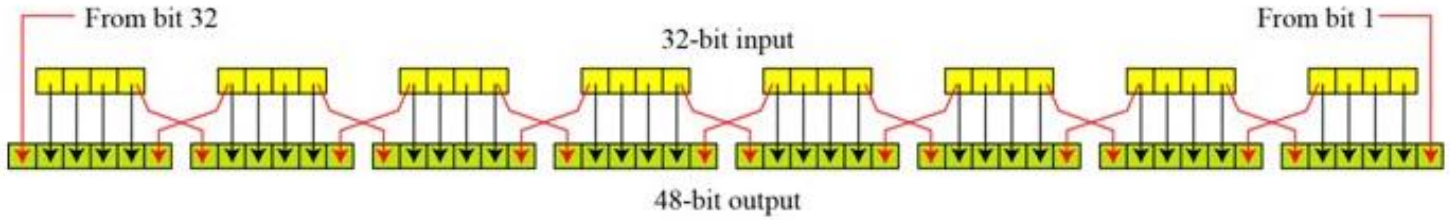
# 02. DES

- DES (Data Encryption Standard)
  - Feistel 구조
  - 블록의 길이 : 64 bit
  - 키의 길이 : 56 bit
  - 16 라운드
  - S-box가 핵심
  - 복호화는 암호화의 역순



# 02. DES



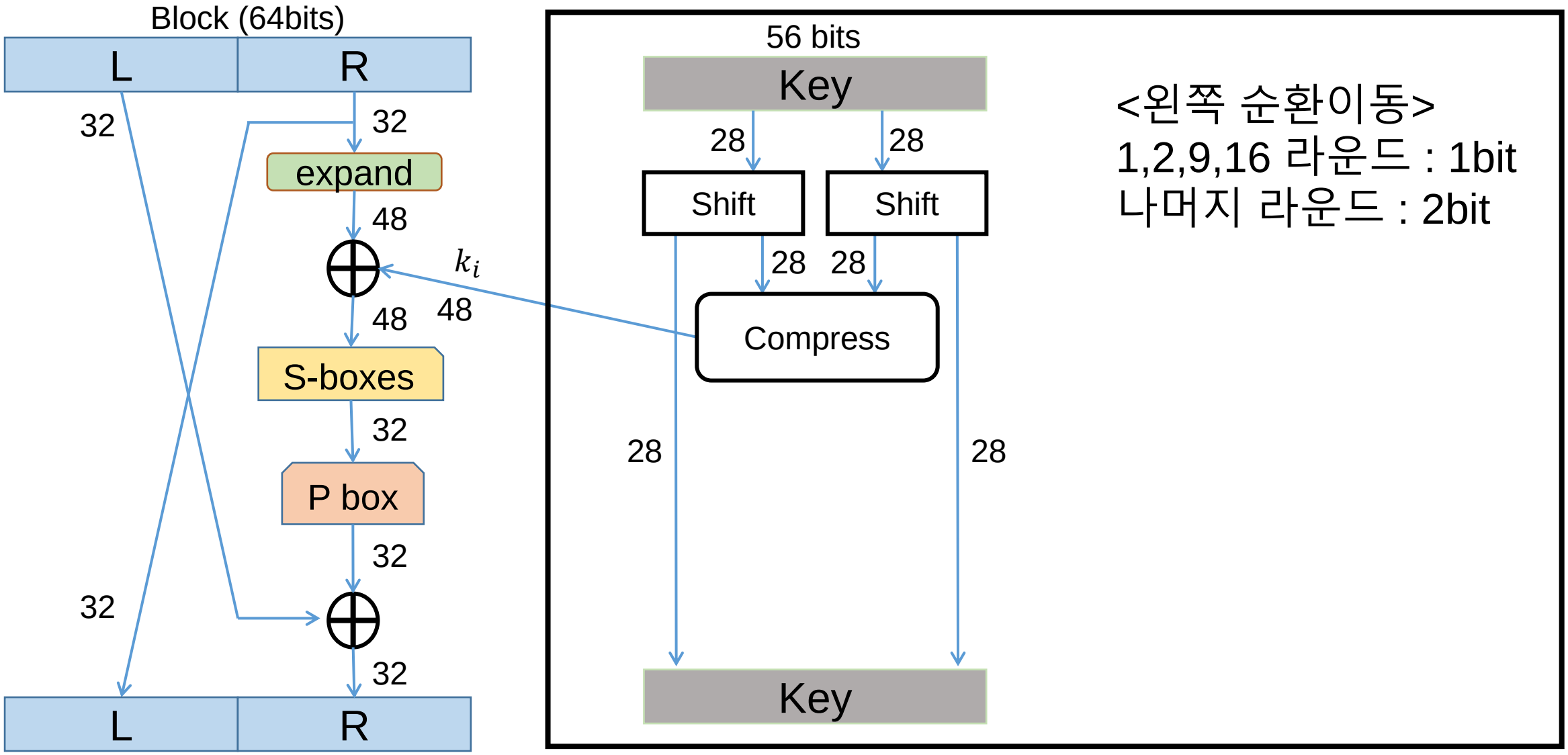

Input 32 bits

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

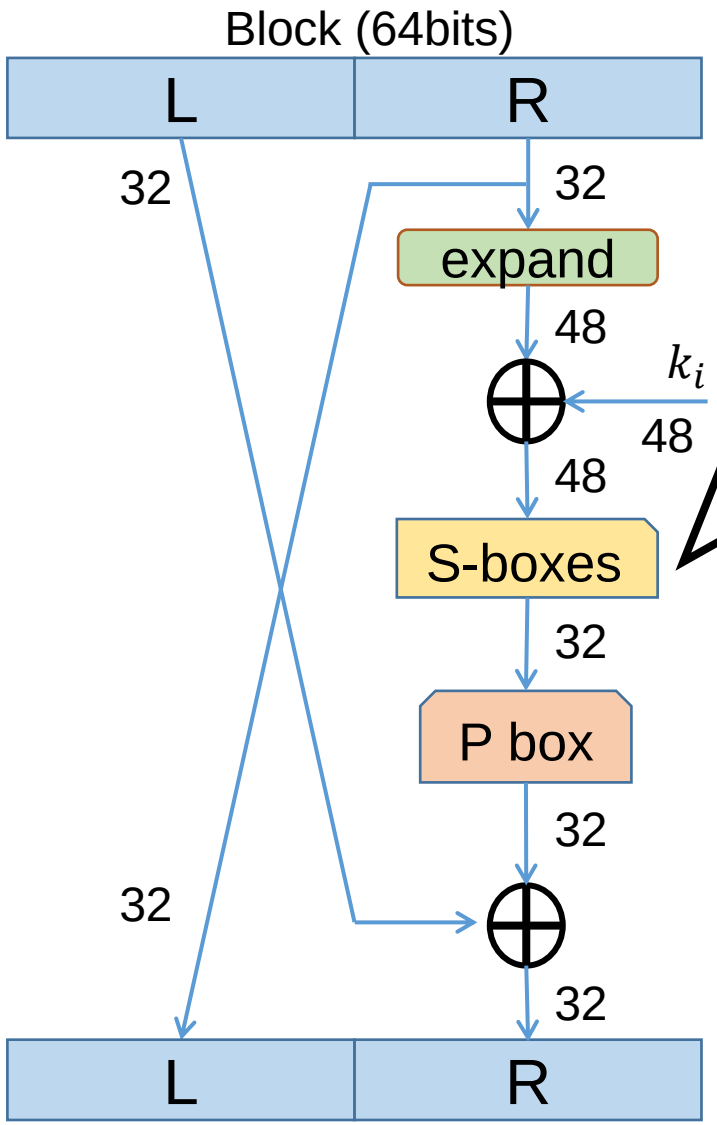
Output 48 bits

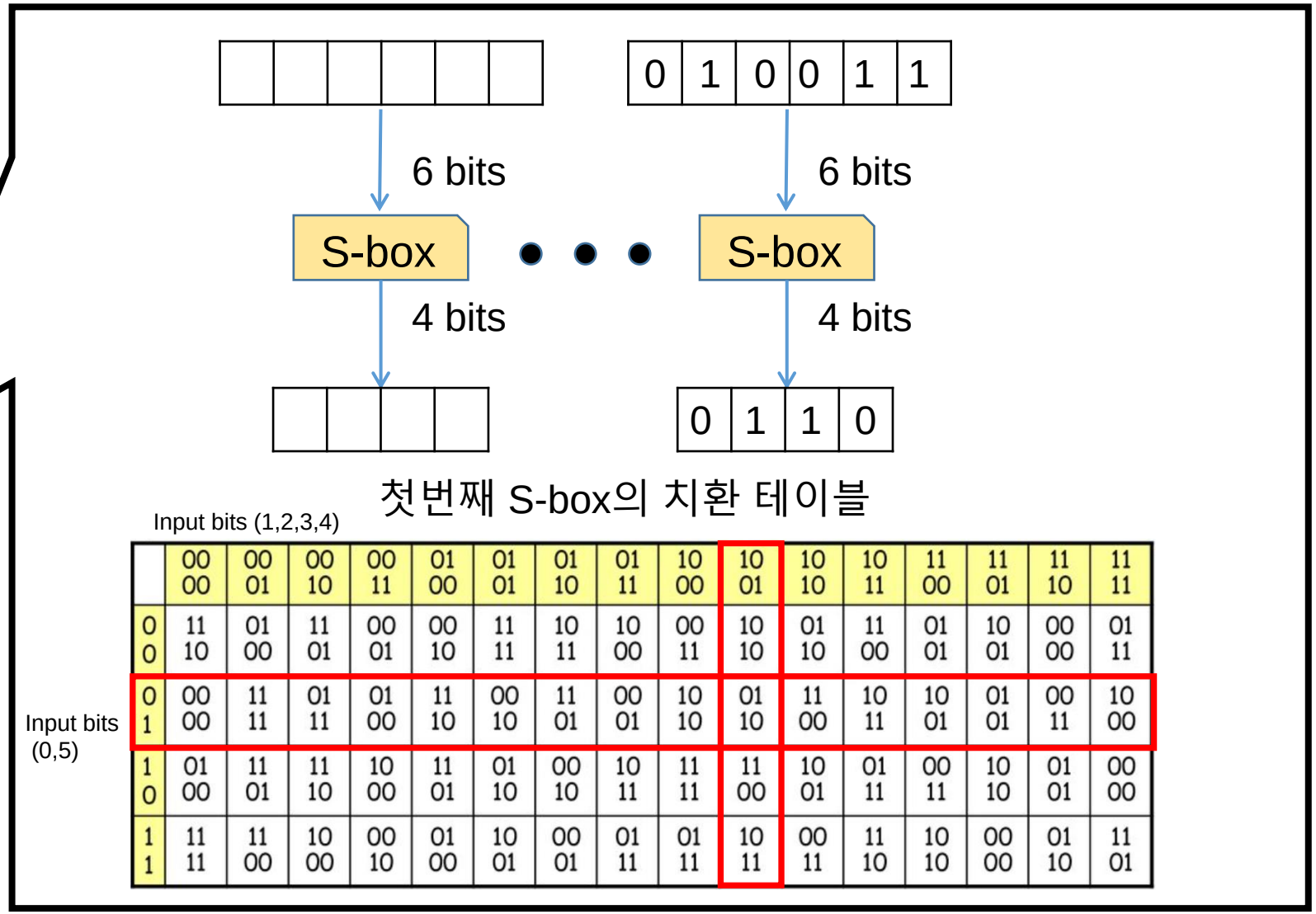
| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 31 | 0 | 1 | 2 | 3 | 4 | 3 | 4 | 5 | 6 | 7 | 8 |
| 7 | 8 | 9 | 10 | 11 | 12 | 11 | 12 | 13 | 14 | 15 | 16 |
| 15 | 16 | 17 | 18 | 19 | 20 | 19 | 20 | 21 | 22 | 23 | 24 |
| 23 | 24 | 25 | 26 | 27 | 28 | 27 | 28 | 29 | 30 | 31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

# 02. DES


Block (64bits)
L
R
32
32
expand
48
$k_i$
48
48
S-boxes
32
P box
32
32
32
L
R
56 bits
Key
28
28
Shift
Shift
28
28
Compress
28
28
Key
<왼쪽 순환이동>
1,2,9,16 라운드 : 1bit
나머지 라운드 : 2bit

# 02. DES



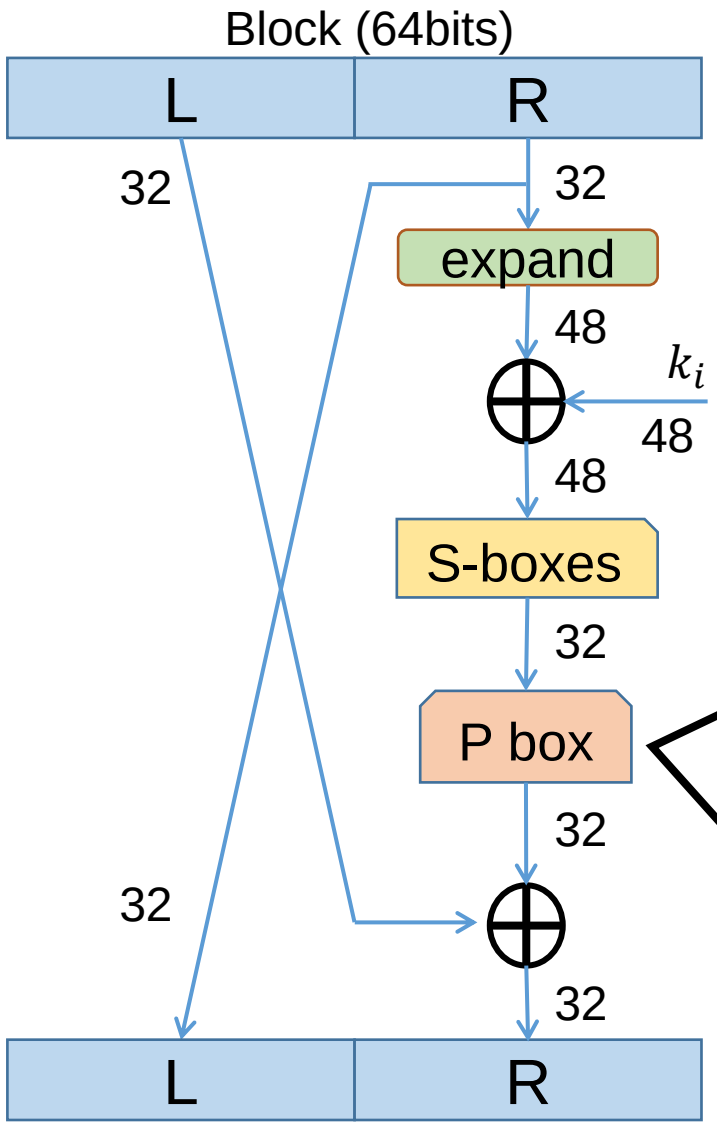

첫번째 S-box의 치환 테이블

Input bits (1,2,3,4)

Input bits (0,5)

| | 00 00 | 00 01 | 00 10 | 00 11 | 01 00 | 01 01 | 01 10 | 01 11 | 10 00 | 10 01 | 10 10 | 10 11 | 11 00 | 11 01 | 11 10 | 11 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 0 | 11 10 | 01 00 | 11 01 | 00 01 | 00 10 | 11 11 | 10 11 | 10 00 | 00 11 | 10 10 | 01 10 | 11 00 | 01 01 | 10 01 | 00 00 | 01 11 |
| 0 1 | 00 00 | 11 11 | 01 11 | 01 00 | 11 10 | 00 10 | 11 01 | 00 01 | 10 10 | 01 10 | 11 00 | 10 11 | 10 01 | 01 01 | 00 11 | 10 00 |
| 1 0 | 01 00 | 11 01 | 11 10 | 10 00 | 11 01 | 01 10 | 00 10 | 10 11 | 11 11 | 11 00 | 10 01 | 01 11 | 00 11 | 10 10 | 01 01 | 00 00 |
| 1 1 | 11 11 | 11 00 | 10 00 | 00 10 | 01 00 | 10 01 | 00 01 | 01 11 | 01 11 | 10 11 | 00 11 | 11 10 | 10 10 | 00 00 | 01 10 | 11 01 |

# 02. 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 |

● 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 |

# 03. DES의 안전성

# 03. DES의 안전성

- DES (Data Encryption Standard)
  - 전사 조사 공격이외에 알려진 공격은 없음
  - 컴퓨터 성능 발전으로 현대에는 더 이상 전사 공격으로부터 안전하지 못함

- Triple DES
  - DES의 문제점인 짧은 키 길이를 늘리기 위해 생김
  - DES 알고리즘은 그래도 사용
  - 속도가 DES보다 3배 느림
  - 블록 크기 64bit는 너무 작음

- AES (Advanced Encryption Standard)

# 감사합니다!