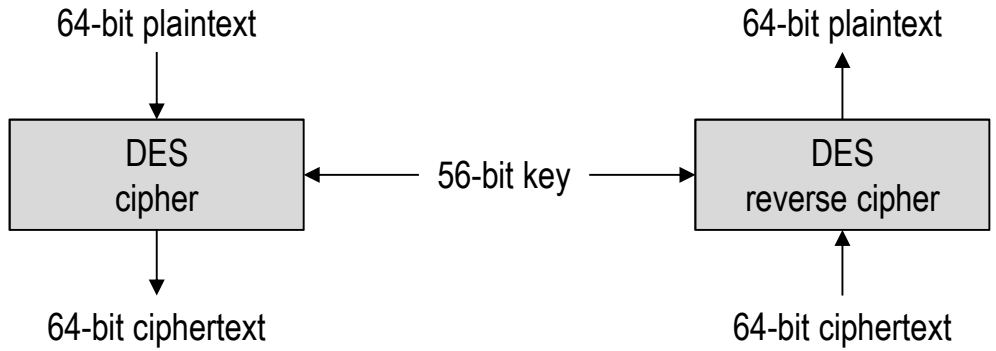
DES

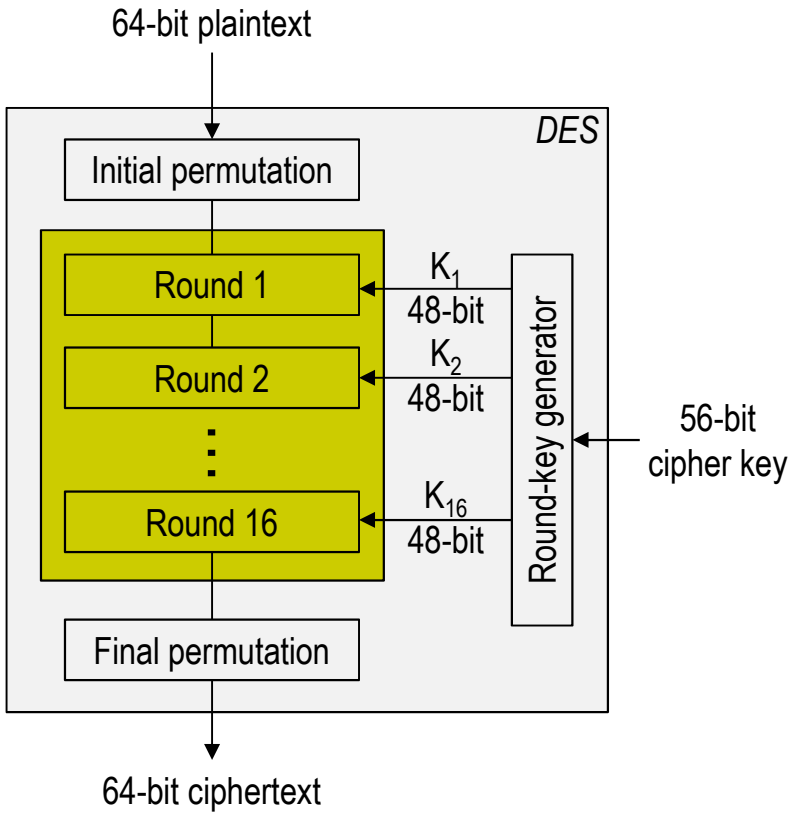
목차

DES

- DES (Data Encryption Standard)
  - 1973년 NBS(현재 NIST)는 국가 대칭키 암호시스템을 위한 제안을 요청
  - Lucifer 프로젝트를 개량한 IBM의 제안이 DES로 채택
  - 1975년 FIPS draft로 공표
  - Block cipher
    - 64비트 평문, 56비트 키 → DES 암호화 → 64비트 암호문
    - 64비트 암호문, 56비트 키 → DES 복호화 → 64비트 평문

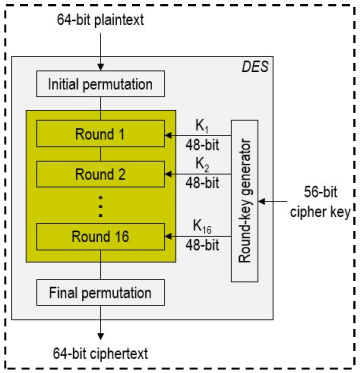


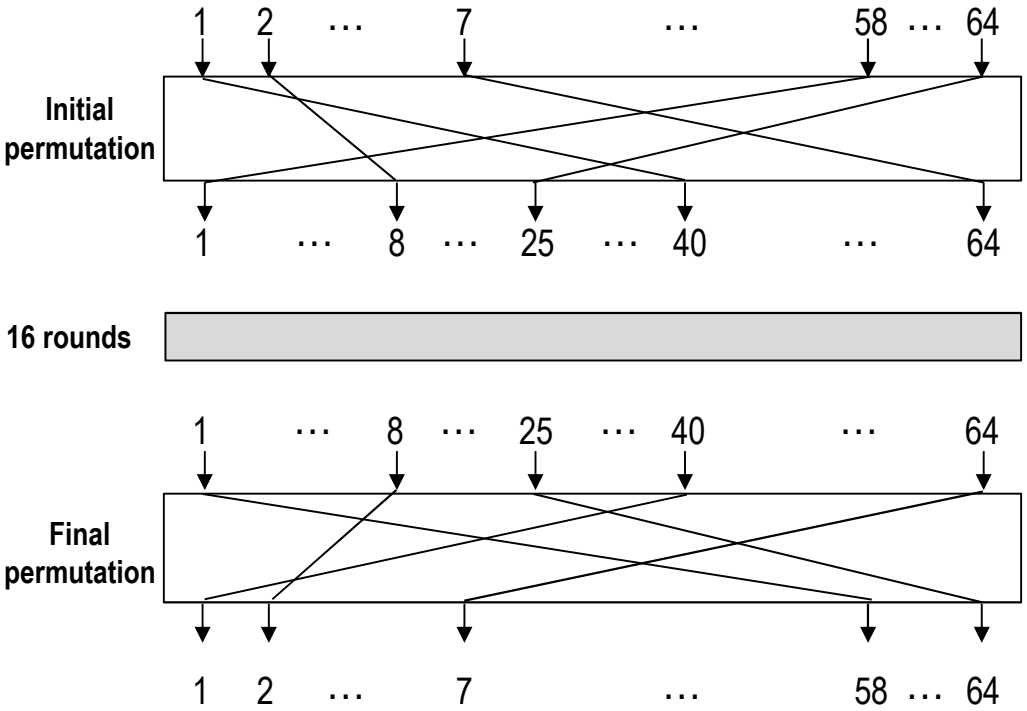
DES 구조


64-bit plaintext
DES
Initial permutation
Round 1
Round 2
Round 16
K1
48-bit
K2
48-bit
K16
48-bit
Round-key generator
56-bit
cipher key
Final permutation
64-bit ciphertext

DES 구조: initial permutation, final permutation

Reference: DES, FIPS PUB 46-3, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf





Initial permutation table
58 50 42 34 26 18 10 02
60 52 44 36 28 20 12 04
62 54 46 38 30 22 14 06
64 56 48 40 32 24 16 08
57 49 41 33 25 17 09 01
59 51 43 35 27 19 11 03
61 53 45 37 29 21 13 05
63 55 47 39 31 23 15 07

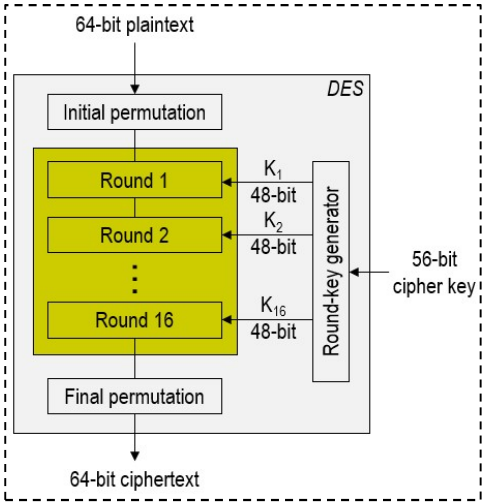
Final permutation table
40 08 48 16 56 24 64 32
39 07 47 15 55 23 63 31
38 06 46 14 54 22 62 30
37 05 45 13 53 21 61 29
36 04 44 12 52 20 60 28
35 03 43 11 51 19 59 27
34 02 42 10 50 18 58 26
33 01 41 09 49 17 57 25

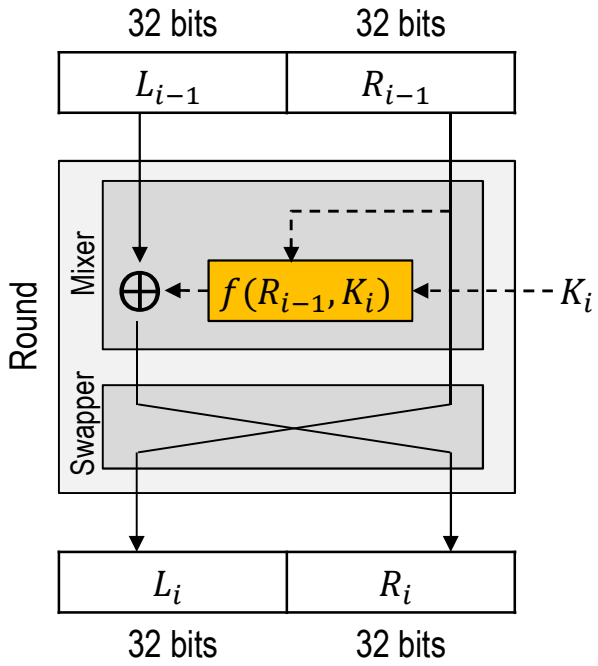
Initial permutation (IP), final permutation (IP^{-1})

- Initial permutation, final permutation은 각각 straight P-box로 64개 입력 비트 위치를 미리 정해진 규칙에 따라 변경 출력함
- 예를 들어 initial permutation에서 입력의 58번째 비트는 출력의 1번째 비트가 됨
- Initial permutation, final permutation은 서로의 inverse가 되도록 구성되었으며 DES에서 암호학적 중요성은 없음
- 암호화 키는 사용되지 않음 (즉 keyless)

DES 구조: Rounds

Reference: DES, FIPS PUB 46-3, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf



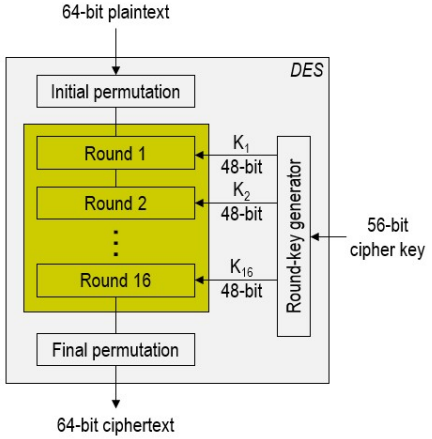


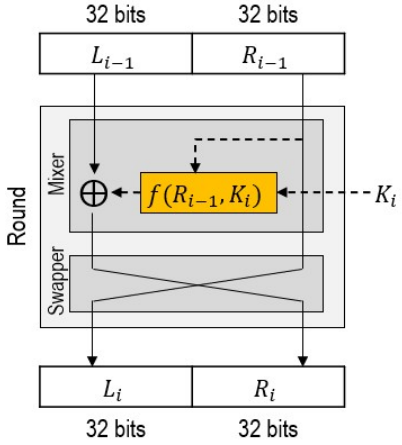
Rounds

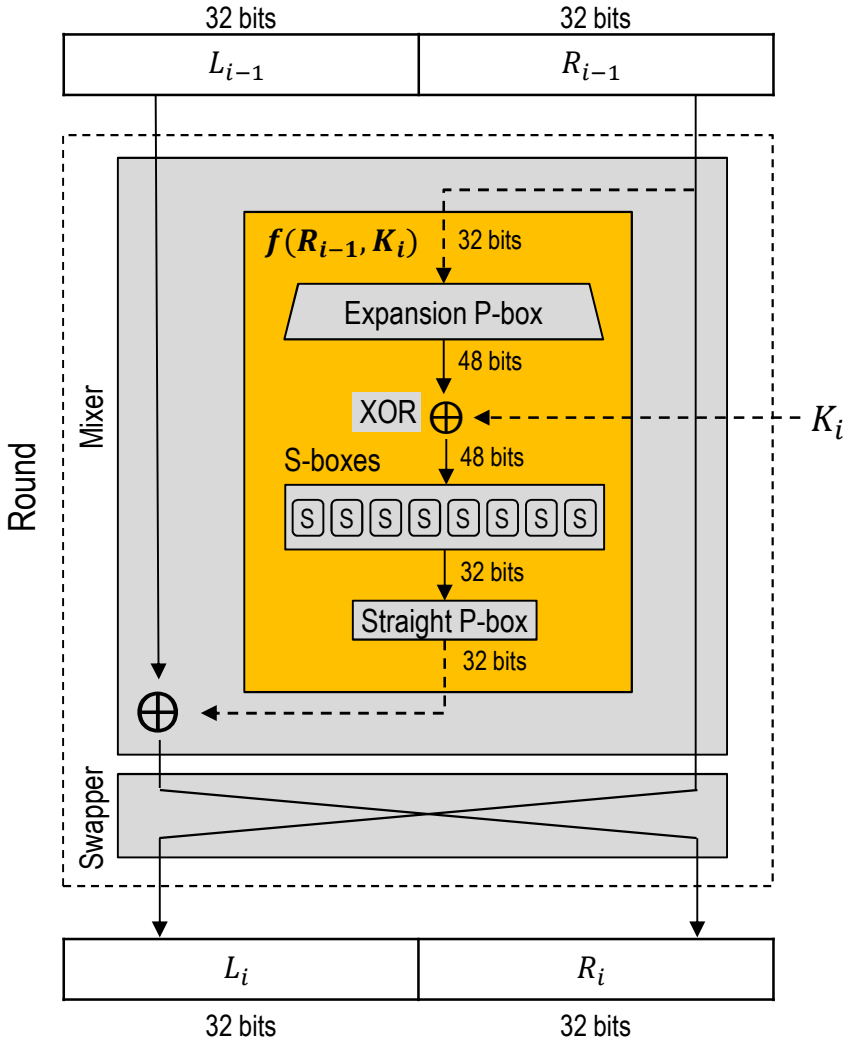
- DES는 16 라운드 사용
- 각 라운드는 하나의 Feistel cipher로 두 개의 cipher 요소(mixer와 swapper)로 구성됨. Swapper는 가역적이며 mixer는 XOR 연산으로 인해 invertible함
- 각 라운드는 이전 라운드 혹은 initial permutation으로부터 L_{i-1}, R_{i-1}를 입력 받아 L_i, R_i를 생성한 후 다음 라운드 혹은 final permutation으로 전달
- 모든 비가역적(non-invertible) 요소는 DES 함수 $f(R_{i-1}, K_i)$ 내부에 존재

DES 구조: DES Function

Reference: DES, FIPS PUB 46-3, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf







DES function

- DES의 핵심 부분으로 R_{i-1}, K_i를 입력 받아 32비트 출력을 생성하는 함수로 4가지 변환절차를 수행

① 첫번째로 **expansion P-box**를 통해 R_{i-1}의 32비트 입력을 48비트로 확장 출력

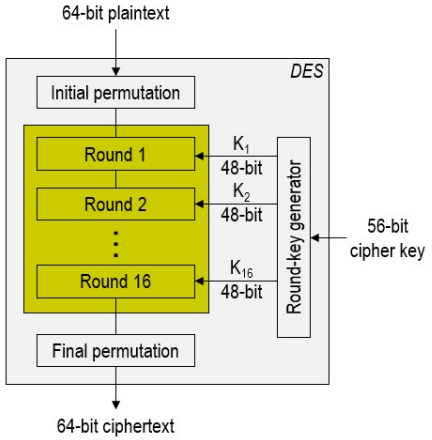
② 두번째로 **whitener (XOR)**를 통해 expansion P-box의 출력 48비트와 라운드 키 48비트에 XOR 연산을 적용하여 48비트 출력 생성

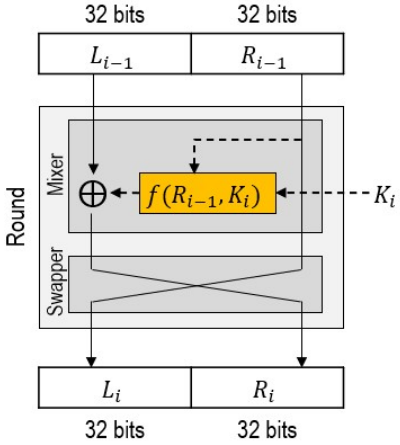
③ 세번째로 XOR 출력 48비트를 6비트씩 분리하여 **8개 S-box들**에 입력으로 넣고 32비트 출력 생성함. 각 S-box는 6비트 입력을 받아 4비트를 출력

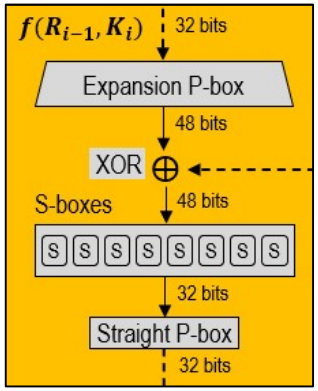
④ 네번째로 **straight P-box**를 통해 직전 8개 S-box 출력 32비트의 위치를 변환하여 32비트 출력 생성

DES 구조: DES Function – Expansion P-box

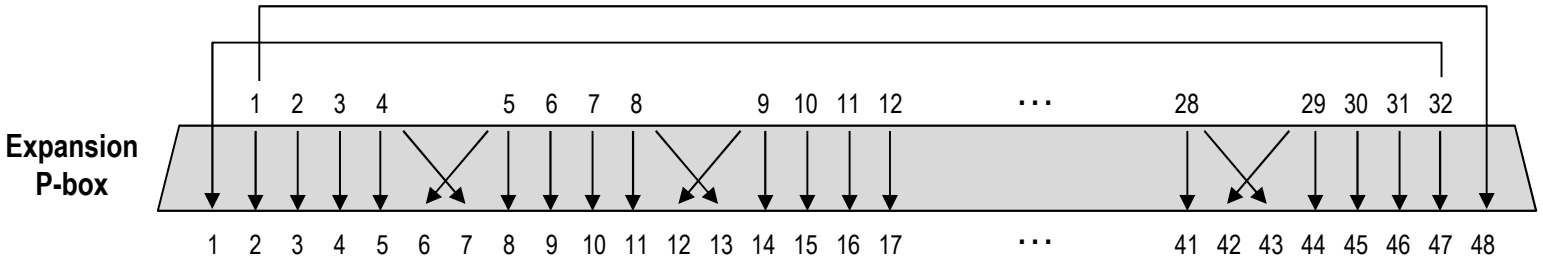
Reference: DES, FIPS PUB 46-3, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf







32x48 Expansion P-box permutation table
32 01 02 03 04 05
04 05 06 07 08 09
08 09 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 01

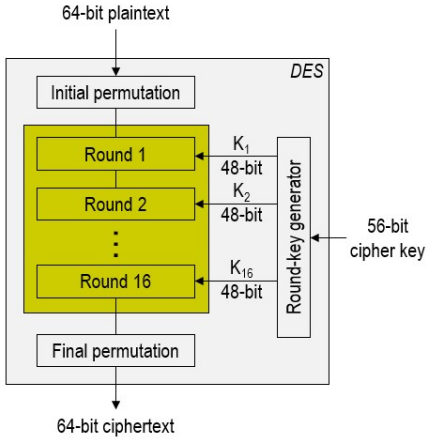


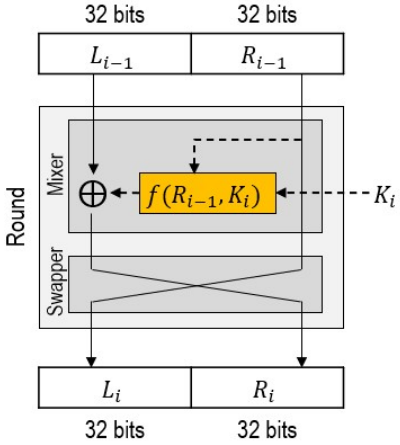
DES function – Expansion P-box

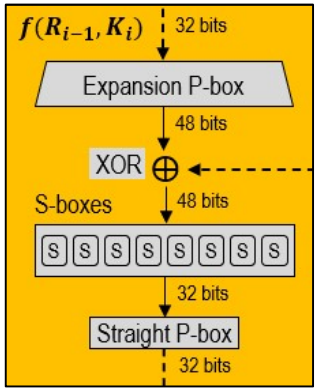
- **32x48 Expansion P-box**를 통해 R_{i-1}의 32비트 입력을 48비트로 확장 출력

DES 구조: DES Function – S-boxes

Reference: DES, FIPS PUB 46-3, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf

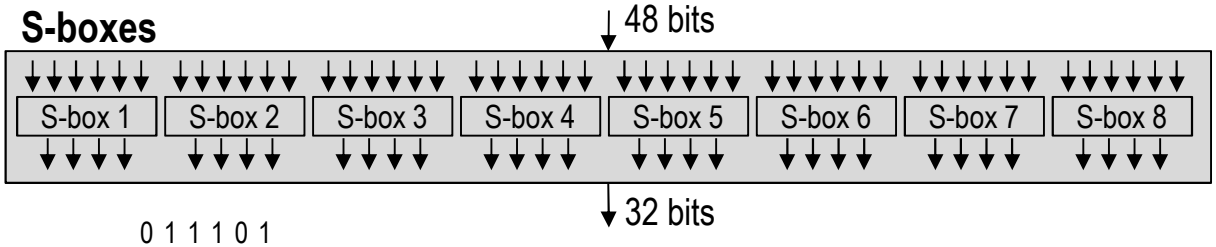


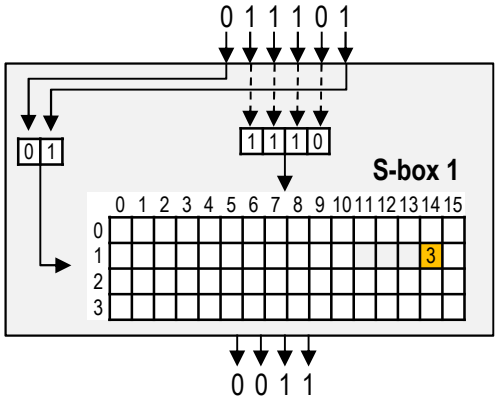


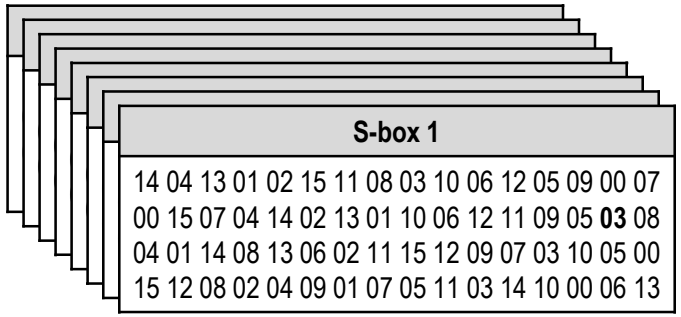


DES function – S-boxes

- XOR 출력 48비트를 6비트씩 분리하여 **8개 S-box들**에 입력으로 넣고 32비트 출력 생성함. 각 S-box는 6비트 입력을 받아 4비트를 출력

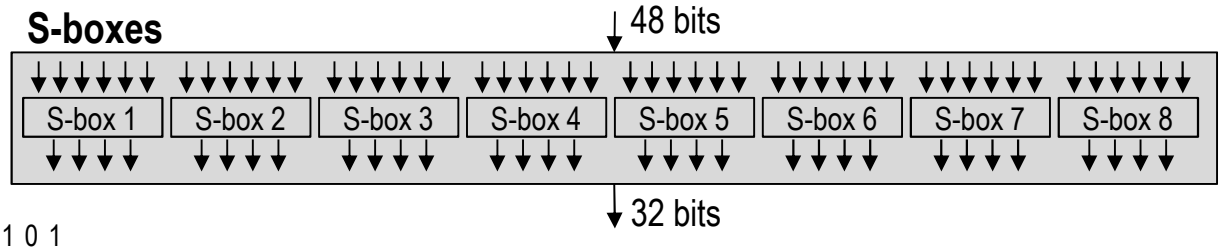


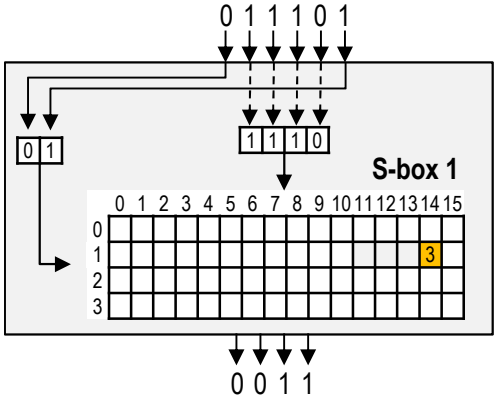




DES 구조: DES Function – S-boxes

Reference: DES, FIPS PUB 46-3, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf





S-box 1															
14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

S-box 2															
15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09

S-box 3															
10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

S-box 4															
07	13	14	03	00	06	09	10	01	02	08	05	11	12	04	15
13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

S-box 5															
02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03

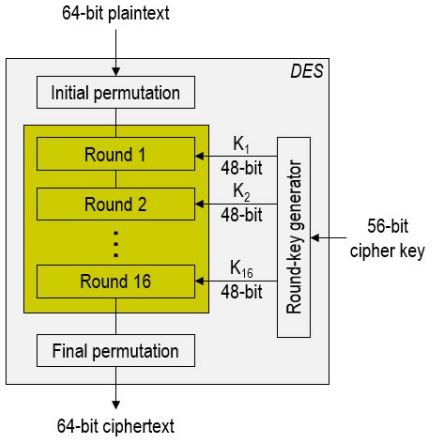
S-box 6															
12	01	10	15	09	02	06	08	00	13	03	04	14	07	05	11
10	15	04	02	07	12	09	05	06	01	13	14	00	11	03	08
09	14	15	05	02	08	12	03	07	00	04	10	01	13	11	06
04	03	02	12	09	05	15	10	11	14	01	07	06	00	08	13

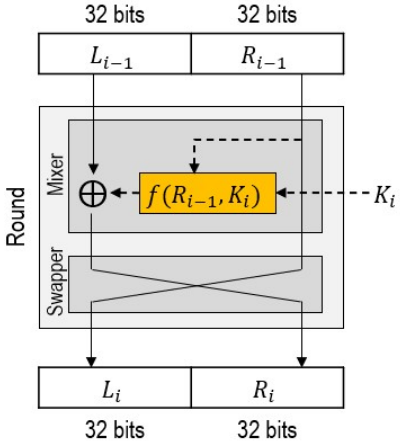
S-box 7															
04	11	02	14	15	00	08	13	03	12	09	07	05	10	06	01
13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12

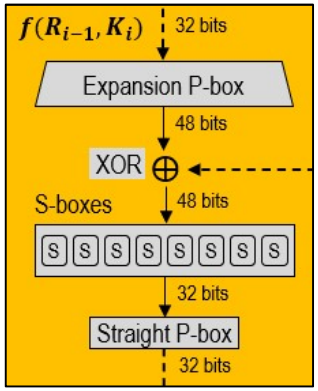
S-box 8															
13	02	08	04	06	15	11	01	10	09	03	14	05	00	12	07
01	15	13	08	10	03	07	04	12	05	06	11	00	14	09	02
07	11	04	01	09	12	14	02	00	06	10	13	15	03	05	08
02	01	14	07	04	10	08	13	15	12	09	00	03	05	06	11

DES 구조: DES Function – Straight P-box

Reference: DES, FIPS PUB 46-3, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf

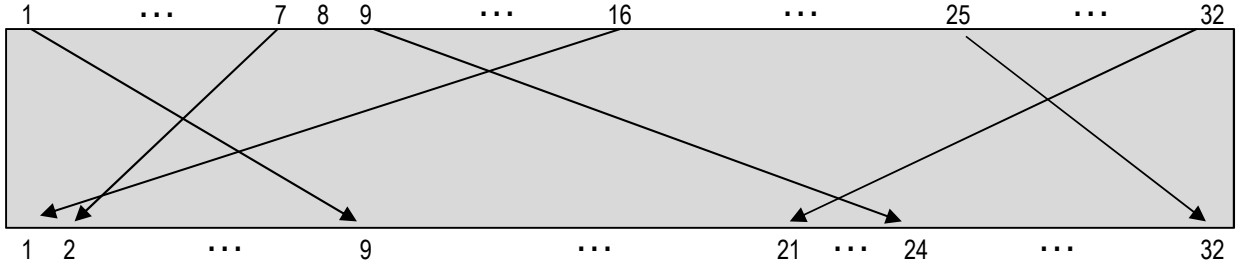






32x32 Straight P-box permutation table
16 07 20 21
29 12 28 17
01 15 23 26
05 18 31 10
02 08 24 14
32 27 03 09
19 13 30 06
22 11 04 25

Straight P-box

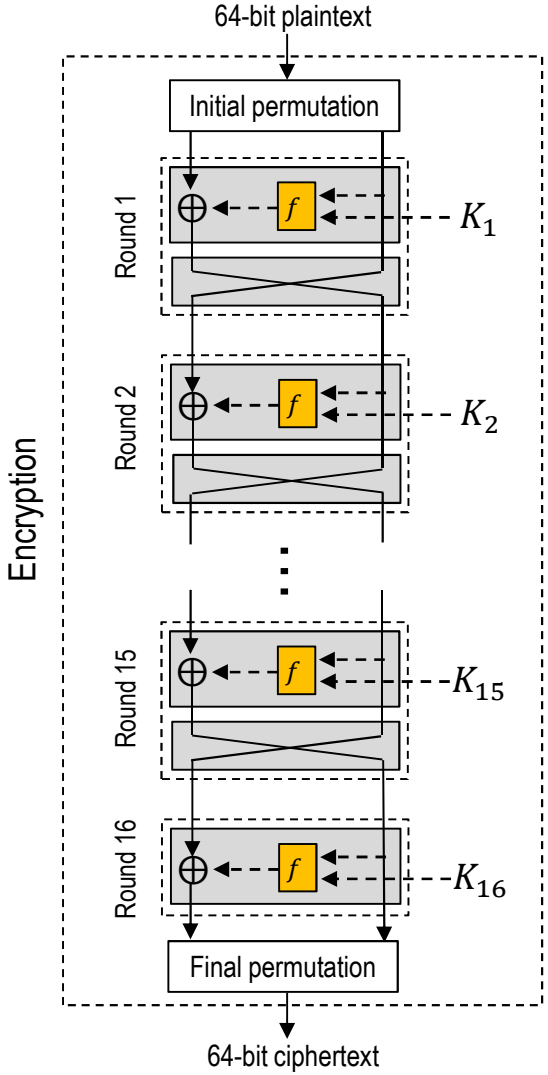


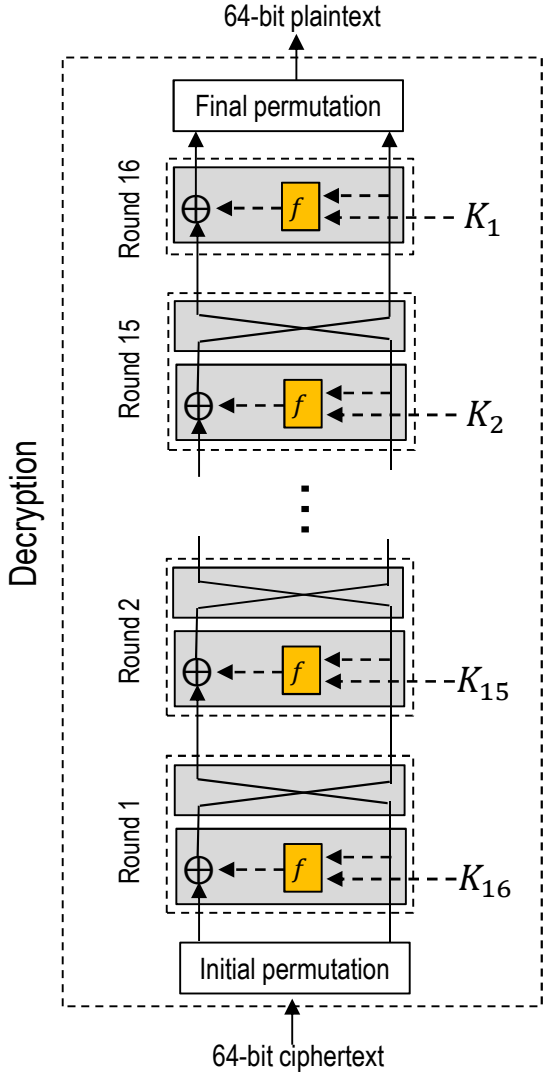
DES function – Straight P-box

- **Straight P-box**를 통해 직전 8개 S-box 출력 32비트의 위치를 변환하여 32비트 출력 생성

DES 구조: Encryption & Decryption

Reference: DES, FIPS PUB 46-3, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf



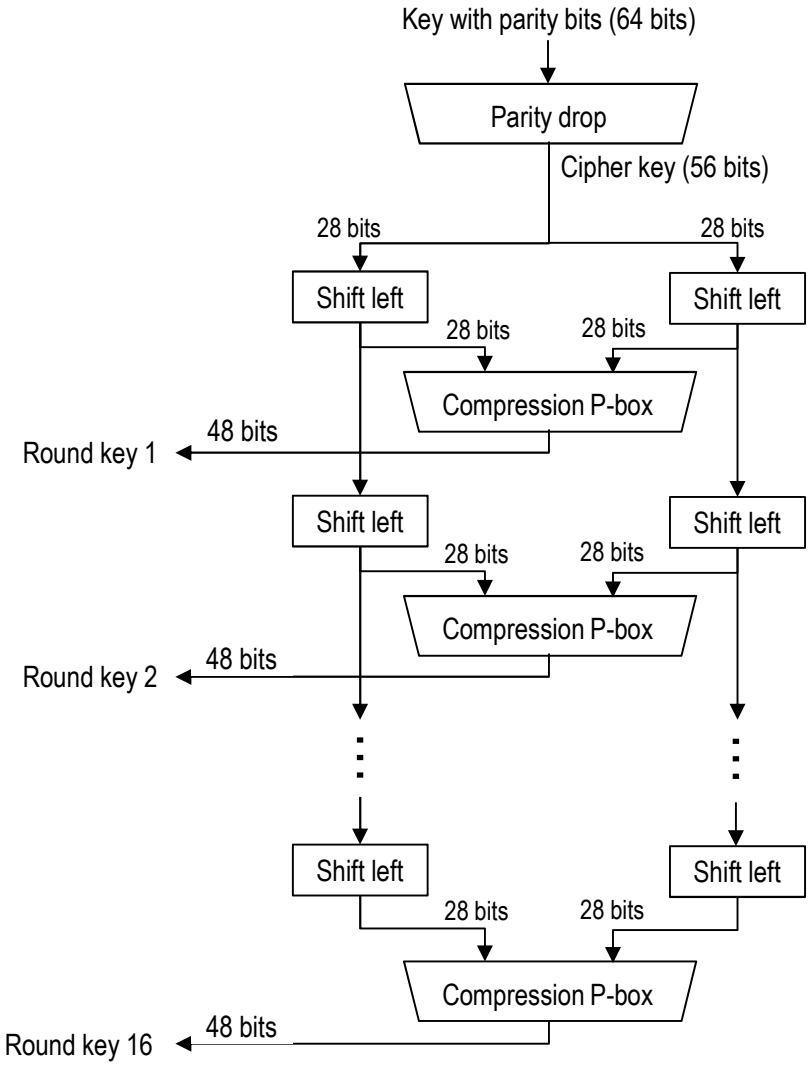


DES encryption & decryption

- Cipher와 reverse cipher를 유사하게 설계
- Cipher와 reverse cipher의 마지막 라운드(Rounds 16)에서 swapper 제외
- Cipher와 reverse cipher에서 rounds key들을 역순으로 적용

DES 구조: Key Generation

Reference: DES, FIPS PUB 46-3, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf



64x56 Parity drop permutation table
57 49 41 33 25 17 09
01 58 50 42 34 26 18
10 02 59 51 43 35 27
19 11 03 60 52 44 36
63 55 47 39 31 23 15
07 62 54 46 38 30 22
14 06 61 53 45 37 29
21 13 05 28 20 12 04

56x48 Compression P-box permutation table
14 17 11 24 01 05
03 28 15 06 21 10
23 19 12 04 26 08
16 07 27 20 13 02
41 52 31 37 47 55
30 40 51 45 33 48
44 49 39 56 34 53
46 42 50 36 29 32

DES key generation

- DES 암호화 키는 일반적으로 56비트 대신 패리티 비트((비트 8,16,24,32,40,48,56,64)가 포함된 64비트로 주어짐
- Parity drop에서는 패리티비트를 제거 및 나머지 비트들의 위치를 변경
- Shift left는 left circular shift이며 1,2,9,16 라운드에서는 한 비트 쉬프트를 수행하고, 나머지 라운드들에서는 두 비트 쉬프트 수행
- Compression P-box에서는 56비트를 입력 받아 라운드 키로 사용될 48비트를 출력

References

- Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill, 2008
- William Stallings, Cryptography and Network Security: Principles and Practice, Sixth Edition, Prentice Hall, 2014
- Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010
- 김명환, 수리암호학개론, 2019
- 정민석, 암호수학, 경문사, 2017
- 최은미, 정수와 암호론, 북스힐, 2019
- 이민섭, 정수론과 암호론, 교우사, 2008