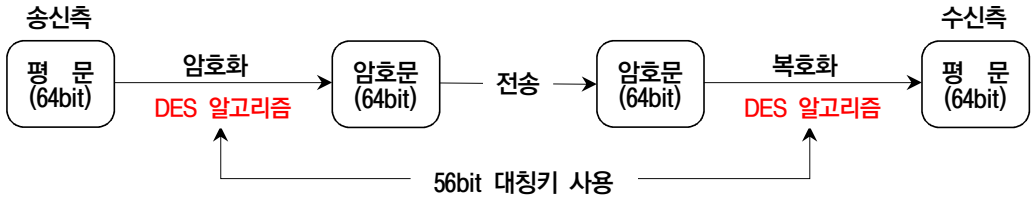
6. DES

1. DES 개요



① DES는 평문을 **64bit 블록** 단위로 나누어 암호화 한다. 암호문도 64bit이다.
→ 하지만, 실제 암호 및 복호화 키 크기는 **56bit**이다.
→ 키 구성은 56bit에 **패리티 비트 8bit**가 추가되어 전체 64bit가 된다.
→ 즉, 암호키 56bit를 **7bit**마다 끊어서 "**패리티 비트**"를 삽입하여 64bit가 된다.

② DES는 1977년 IBM에서 개발하였고, 미국 국방부가 채택하였다.

③ DES는 가장 널리 사용된 블록 암호 알고리즘이었다.
→ 하지만, 지금은 짧은 키 길이(56비트)로 더 이상 안전하지 않다.

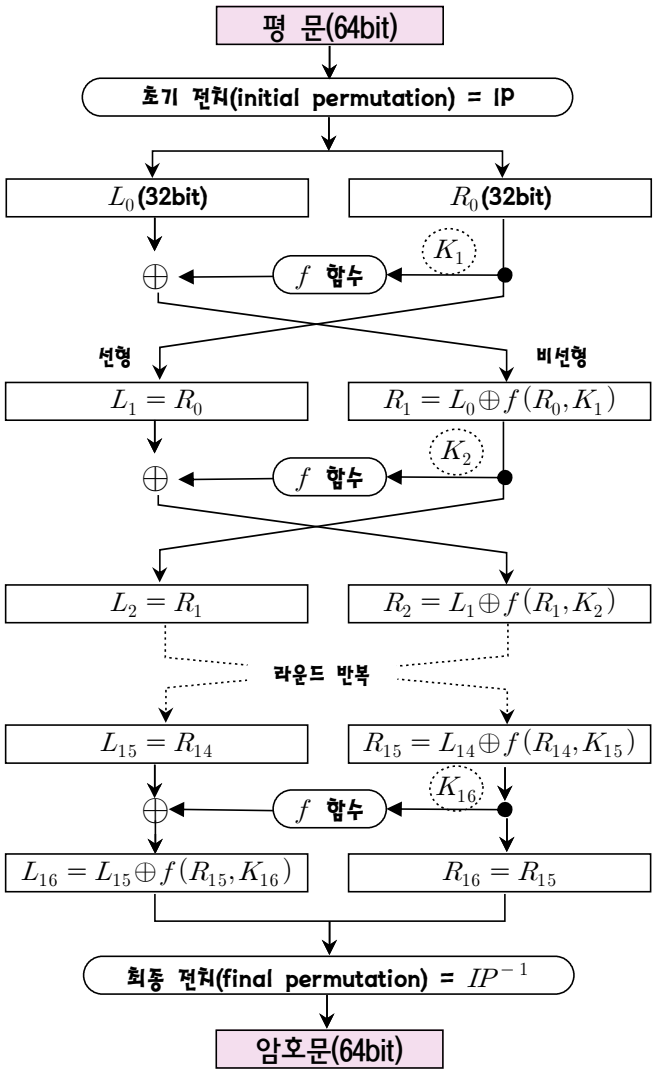
④ DES에 적용하기 위해 4개 운영모드 "ECB, CBC, CFB, OFB"가 개발되었다.

⑤ 컴퓨터 성능이 발전되어 DES의 보안성을 높이기 위해 '3중 DES'를 개발하였다.
→ '3중 DES(Triple-DES)'는 키 크기가 128bit이다.
→ '3중 DES'는 3개의 키를 사용하여 3번 반복 암호화함(암호 강도 중대)
→ '3중 DES'는 DES를 3번 반복 사용한다,

◉ **DES(Data Encryption Standard)**
• DES는 과거에 미국 정부가 인정한 암호 알고리즘이었다.
• 내부적으로는 복잡한 부분이 많이 있지만 사용하는데 특별한 문제점이 없었고,
• 컴퓨터에서 효율적으로 수행되는 장점이 있어서 20여년간 널리 사용되었다.

2. DES 구조

• DES 알고리즘의 암호화 과정이다. DES는 16 라운드가 반복된다.



• 64bit 평문 블록을 IP(초기 전치)를 이용하여 새로운 64bit 블록으로 재배열한다.

• IP에는 평문의 각 비트를 전치할 정보가 저장되어 있다.

• L_0, R_0 각 32bit씩 좌우 분리

• L_1은 오른쪽 32bit R_0을 그대로 사용한다.**(선형)**

• R_1은 R_0를 f 함수에 넣어서 처리한 그 결과 값과 L_0을 XOR 연산하여 구한다.**(비선형)**

• K_1, K_2, K_3, …, K_{16}은 암호화 과정에서 암호키를 이용하여 새로 생성한 **라운드 키**이다.

• 16라운드를 반복 진행하여 L_{16}과 R_{16}을 구한 후, 좌우를 다시 바꾼 64bit 블록(L_{16}, R_{16})에 초기 전치 IP의 거꾸로인 역전치 IP^{-1}을 적용한다.

• 초기 전치와 최종 전치의 관계는 역의 관계이다.
→ 초기 전치 : IP
→ 최종 전치 : IP^{-1}

① f 함수는 페이스텔(Feistel) 연산을 수행하는 복잡한 내부 연산이다.

② **암호** 알고리즘에 사용된 **라운드 키 순서를 거꾸로 적용**하면 **복호** 알고리즘이 된다.(F.168쪽)

③ 각 라운드는 혼합기와 스와퍼가 있다.(단, 주어진 구조는 마지막 라운드에 스와퍼가 없다)
→ 혼합기(mixer)는 f(K) 함수의 결과와 xor 연산하는 것을 지칭하고
→ 스와퍼(swapper)는 좌우측을 교환하는 기능을 말한다.
→ DES 알고리즘에서 마지막 라운드에 스와퍼를 추가하는 방법도 있다.

• DES에서 초기 전치(IP)의 기능이 무엇인지? 다음 예제를 통해 살펴본다.
• 전치는 각 비트의 자리를 서로 바꾸는 것을 말한다.

예제

아스키 코드로 구성된 문자열 "ABCDEFGH"에 대한 IP 변환 결과는?
[단, 초기 전치(IP, initial permutation)는 다음과 같다]

	1	2	3	4	5	6	7	8
IP	17	18	19	20	21	22	23	24
	41	42	43	44	45	46	47	48
	25	26	27	28	29	30	31	32
	57	58	59	60	61	62	63	64
	9	10	11	12	13	14	15	16
	49	50	51	52	53	54	55	56
	33	34	35	36	37	38	39	40
	1	2	3	4	5	6	7	8

// 64비트열을 재배열하는데
• 1번 위치에 17번째 비트를
• 2번 위치에 18번째 비트를
• 3번 위치에 19번째 비트를
놓는 방식으로
비트열의 자리를 바꾼다.

[풀이] 문자열 "ABCDEFGH"를 2진수로 변환한 후, IP를 이용하여 변환한다.

• 문자열 "ABCDEFGH"를 2진수로 변환하면, 다음처럼 64비트열이 된다.
• IP는 평문을 구성하는 비트열을 재배열 하는데 사용된다(전치암호 원리)

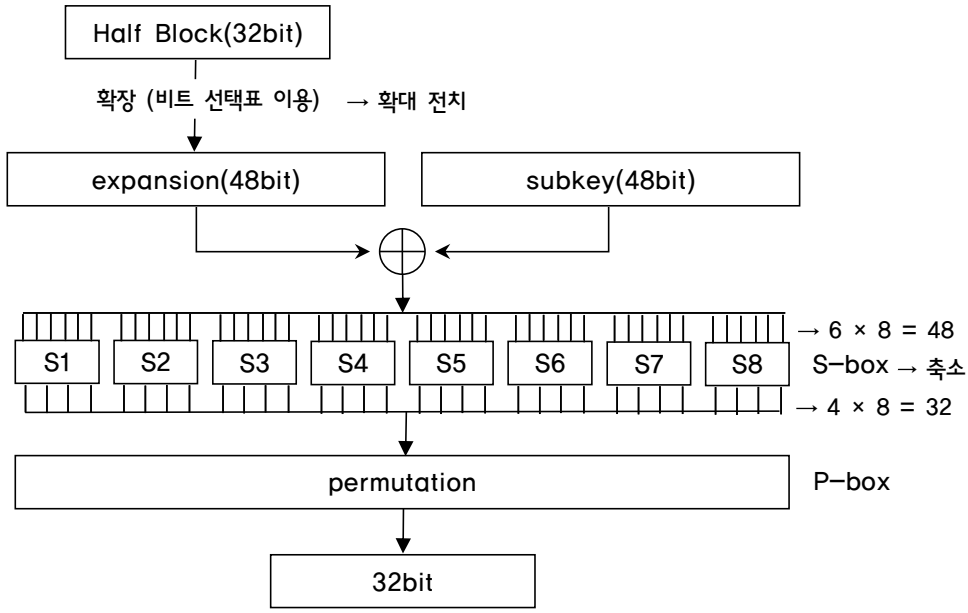
A	B	C	D	E	F	G	H
01000001	01000010	01000011	01000100	01000101	01000110	01000111	01001000

↓
↓ IP를 이용한 재배열
↓

01000011	01000110	01000100	01001000	01000010	01000111	01000101	01000001
C	F	D	H	B	G	E	A

☞ DES에서 평문 블록을 IP를 이용하여 재배열한 결과인 64비트열을 L_0, R_0 각각 32bit씩 좌우 분리한 후 16라운드 반복 암호화를 진행한다.

3. F 함수 구조



① 확장(expansion) - 확대 전치

• 32비트를 48비트로 확장한다. expansion permutation이라 한다.

② 키 혼합(key mixing)

• 확장된 키(48bit)와 subkey(48bit)를 xor 연산한다.

③ 대치(substitution) - DES에서 핵심 부분으로 복잡

• s-box는 혼돈의 역할을 수행한다. 실제로 자료를 섞어주는 역할이다.
• s-box 처리는 혼합된 48비트를 8-토막으로 나누어 다시 32비트로 변경하는 것이다.
• s-box의 각 토막은 6비트를 4비트로 축소시키는 작업을 한다.

④ 전치(permutation) - 평행 전치

• p-box 처리를 한다. p-box의 출력은 32비트이다.
• p-box 처리는 s-box로 부터 출력된 32비트를 재배열하는 것이다.(자리만 변경)

◈ **S-box : DES에서 핵심 부분, 대치(substitution)**

- S-box의 각 토막은 6비트를 4비트로 축소시키는 작업을 한다.
- S-box는 4행 16열로 구성된다.(다음 그림 참조)
- S-box는 입력값 6비트에서

  S-box의 **행**을 결정하는 비트 : 비트 위치 1과 6

  S-box의 **열**을 결정하는 비트 : 비트 위치 2, 3, 4, 5

[예제 1] 입력값이 2진수 011110일 때

입력값	0	1	1	1	1	0

↓s-box의 행 : 00이므로 0행

↓s-box의 열 : 1111이므로 15열

S-box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	**7**
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

↓0행15열의 값은 10진수로 7

↓10진수로 7을 4비트 2진수로 고치면 0111

출력값	0	1	1	1

[예제 2] 입력값이 2진수 001111일 때

입력값	0	0	1	1	1	1

↓s-box의 행 : 01이므로 1행

↓s-box의 열 : 0111이므로 7열

S-box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
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

↓1행7열의 값은 10진수로 1

↓10진수로 1을 4비트 2진수로 고치면 0001

출력값	0	0	0	1

기출문제 분석

1. 그림은 대칭키 암호 DES에서 S-Box를 통과하는 과정이다. 입력값이 $001111_{(2)}$일 때 출력 비트 ㉠은? [2018년 교육청]

입력값 | 0 | 0 | 1 | 1 | 1 | 1 |

↓

S-box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
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

↓

출력값 | ㉠ |

① $0001_{(2)}$ ② $0010_{(2)}$

③ $0110_{(2)}$ ④ $0111_{(2)}$

♤ DES 암호 : S-Box

• **입력값** | 0 | 0 | 1 | 1 | 1 | 1 | 은 1행7열의 값을 지칭 : 1

• 10진수 1을 4비트 2진수로 출력 : $0001_{(2)}$

정답 : ①

2. DES에 대한 다음의 설명 중 옳지 않은 것은? [2014년 서울 9급]

① 1970년대에 표준화된 블록 암호 알고리듬(algorithm)이다.
② 한 블록의 크기는 64비트이다.
③ 한 번의 암호화를 위해 10라운드를 거친다.
④ 내부적으로는 56비트의 키를 사용한다.
⑤ Feistel 암호 방식을 따른다.

♤ DES(Data Encryption Standard)

• 한 번의 암호화를 위해 10라운드를 거친다.(×) → DES의 16라운드를 거친다.

정답 : ③

3. DES(Data Encryption Standard)에 대한 설명으로 옳지 않은 것은? [2021년 지방 9급]

① 1970년에 미국 표준 블록 암호 알고리즘으로 채택되었다.
② 64비트 평문 블록을 64비트 암호문으로 암호화한다.
③ 페이스텔 구조(Feistel structure)로 구성된다.
④ 내부적으로 라운드(round)라는 암호화 단계를 10번 반복해서 수행한다.

♤ DES(Data Encryption Standard)

· 내부적으로 **라운드**(round)라는 암호화 단계를 **10**번 반복해서 수행한다.**(×)**
→ DES는 **16 라운드**가 반복된다.

정답 : ④