3. P-박스 / S-박스

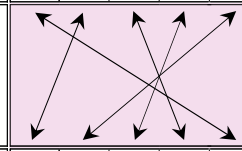
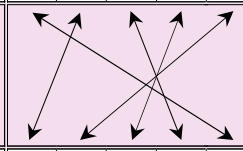
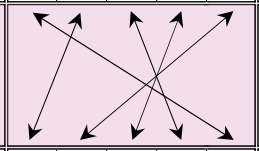
1. P-박스(전치암호)

P-박스는 전치암호의 기본 모형이다. 순열(permutation)에서 P를 따온 것이다.

[예제] 다음 평문을 전치암호를 이용하여 암호화하는 과정을 살펴본다.

평문 : 오늘밤자정에적군을공격하라

[풀이] 평문을 5문자의 그룹으로 나눈다.

	5	1	4	3	2	5	1	4	3	2	5	1	4	3	2	← 복호키
평 문	오	늘	밤	자	정	에	적	군	을	공	격	하	라	보	안	
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
																단순 P-박스
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
암호문	늘	정	자	밤	오	적	공	을	군	에	하	안	보	라	격	
	2	5	4	3	1	2	5	4	3	1	2	5	4	3	1	← 암호키

- 마지막 그룹도 같은 크기를 갖도록 마지막에 **가짜문자**를 채운다.(보안)
- 마지막 그룹 끝에 있는 "**보안**"은 가짜문자이다.

① 암호화와 복호화 과정

암호화와 복호화 과정은 표로 나타내면 다음과 같다.

암호화 ↓	2	5	4	3	1	↑ 복호화
	1	2	3	4	5	

- 암호키 : 2 5 4 3 1
- 복호키 : 5 1 4 3 2

- 먼저, 암호화에서 전치되는 것을 분석해 보면
- 2번째 문자가 1번째, 5번째 문자가 2번째, …, 1번째 문자가 5번째로 이동된 것이다.

② 암호키와 복호키 분석

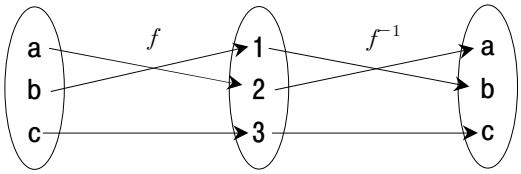
암호키 : 2 5 4 3 1	• 평문의 2번째 문자 → 암호문의 1번째 문자 • 평문의 5번째 문자 → 암호문의 2번째 문자 • 평문의 4번째 문자 → 암호문의 3번째 문자 • 평문의 3번째 문자 → 암호문의 4번째 문자 • 평문의 1번째 문자 → 암호문의 5번째 문자
복호키 : 5 1 4 3 2	• 암호문의 5번째 문자 → 평문의 1번째 문자 • 암호문의 1번째 문자 → 평문의 2번째 문자 • 암호문의 4번째 문자 → 평문의 3번째 문자 • 암호문의 3번째 문자 → 평문의 4번째 문자 • 암호문의 2번째 문자 → 평문의 5번째 문자

③ 단순 P-박스

• 단순 P-박스는 **역함수가 존재**한다.

• 역함수는 어떤 함수에서 그 함수의 결과값을 넣으면 원래 입력값이 나오는 함수이다.

• 어떤 함수(f)의 역함수(f^{-1})가 존재한다면, 그 역함수는 오직 하나이다.

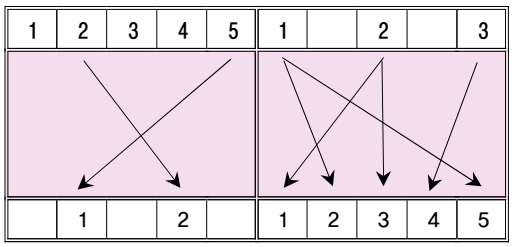


④ 축소 P-박스 / 확장 P-박스

• 축소 P-박스와 확장 P-박스는 **역함수가 존재하지 않는다.**

• 축소 P-박스에서 어떤 입력값은 암호화 과정에서 소멸된다.

• 확장 P-박스에서 어떤 입력값은 암호화 과정에서 하나 이상의 출력에 대응될 수 있다.



2. S-박스(대치암호)

① S-박스는 대치암호의 기본 모형이다.
• S는 대치(substitution)에서 인용한 것이다.

② S-박스는 m×n 구조로 대치될 수 있다.(m과 n은 반드시 같을 필요는 없다)

③ S-박스도 역함수가 존재할 수도 있고, 존재하지 않을 수도 있다.
• S-박스에서 입출력 비트 수가 같으면, 역함수가 존재하게 된다.

④ S-박스는 입출력 사이의 관계를 테이블 또는 수학적 관계로 정의한다.

[예] 역함수를 가지는 S-박스 테이블(입출력 비트 수 동일)

◉ 암호화 과정

3비트 입력

⇓

	00	01	10	11
0	011	010	001	100
1	000	111	101	110

⇓

3비트 출력

◉ 복호화 과정

3비트 입력

⇓

	00	01	10	11
0	100	010	001	000
1	011	110	111	101

⇓

3비트 출력

• 3개의 비트로 생성될 수 있는 비트열은 2^3=8이므로 8가지이다.

// 좌우측 두 테이블은 서로 역함수의 관계를 나타내고 있다.
• 좌측 테이블에서 입력값이 000이면 출력값은 011이다.(암호화)
• 우측 테이블에서 입력값이 011이면 출력값은 000이다.(복호화)
• 좌측 테이블에서 입력값이 001이면 출력값은 010이다.(암호화)
• 우측 테이블에서 입력값이 010이면 출력값은 001이다.(복호화)
:

• 좌측 테이블은 **암호** 알고리즘에 사용될 수 있고
• 우측 테이블은 **복호** 알고리즘에 사용될 수 있다.