4. 대칭키 암호구조

1. 합성 암호(product cipher)

합성 암호는 전치, 대치, 기타 구성요소(주로 xor 연산)를 결합한 복합적인 암호이다.

확산 (diffusion)	• 확산은 암호문과 **평문** 사이의 관계를 알기 어렵게 한다. • 확산은 암호문에 대한 통계시험을 통해 평문을 찾으려는 공격을 좌절시킨다. • 즉, 암호문을 갖고서 평문을 찾기가 어렵다는 것이다. • 확산은 평문의 특정 1bit가 변경되었을 때 • 암호문에 있는 특정 비트나 모든 비트가 바뀔 수 있다.
혼돈 (confusion)	• 혼돈은 암호문과 **키** 사이의 관계를 알기 어렵게 한다. • 혼돈은 암호문을 이용하여 비밀키를 찾으려는 공격을 좌절시킨다. • 즉, 혼돈은 비밀키 발견을 어렵게 하기 위한 것이다.(키 추론의 어려움) • 여기서, 비밀키는 대칭키 암호 알고리즘에서 대칭키를 의미한다. • 키의 특정 1bit가 변경되었을 때, 암호문은 거의 모든 비트가 변경된다. • 각 라운드 키의 각 비트가 암호문의 여러 비트에 영향을 준다는 것이다.

• 확산과 혼돈을 위해 P-박스(전치)와 S-박스(대치), 그리고 라운드 키를 사용한다.
• 공격자는 암호문을 이용하여 평문 또는 암호에 사용된 키를 찾는 것이 목적이다.
• 암호에 확산과 혼돈을 같이 적용하면 평문 또는 키를 찾기가 어렵게 된다.

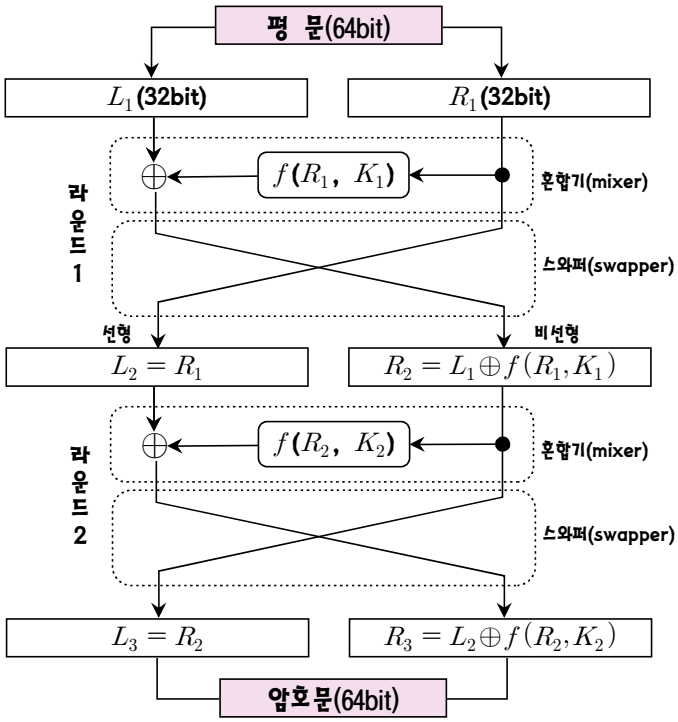
2. 라운드(round)

① 라운드는 합성 암호를 반복적으로 적용하는 것이다,
• 하나의 라운드에서 P-박스와 S-박스 그리고 기타 구성요소가 적용된다.
• 기타 구성요소가 적용되는 부분에서 라운드 키가 사용된다.(주로 xor 연산)
• 실제로, 합성 암호는 2라운드 이상 반복된다.(DES는 16라운드)

② 라운드 키는 각 라운드에서 사용될 서로 다른 키이다.
• 라운드 키는 비밀키로부터 키 생성 알고리즘에 의해 내부적으로 생성된다.
• 블록 암호 알고리즘이 16라운드이면, 16개의 라운드 키가 생성된다.
• n라운드 암호에서 평문은 n번 암호문으로 변경된다고 한다.

3. Feistel 구조

다음은 2 라운드를 가지는 Feistel 구조이다.



① Feistel 구조는 평문을 같은 크기의 2부분으로 분할하여 암호화 한다.(L_1, R_1)

② 각 라운드에서 입력의 반은 선형 변환되고, 나머지 반은 비선형 변환된다.

→ 입력의 반은 전혀 변환되지 않는다.(선형 변환)

③ 각 라운드에는 혼합기(mixer)와 스와퍼(swapper)가 있다.

→ 혼합기는 $f()$ 함수의 결과와 xor 연산하는 것을 말하고

→ 스와퍼는 좌우측을 교환하는 기능을 가진다.

④ K_1과 K_2는 라운드 키이다.

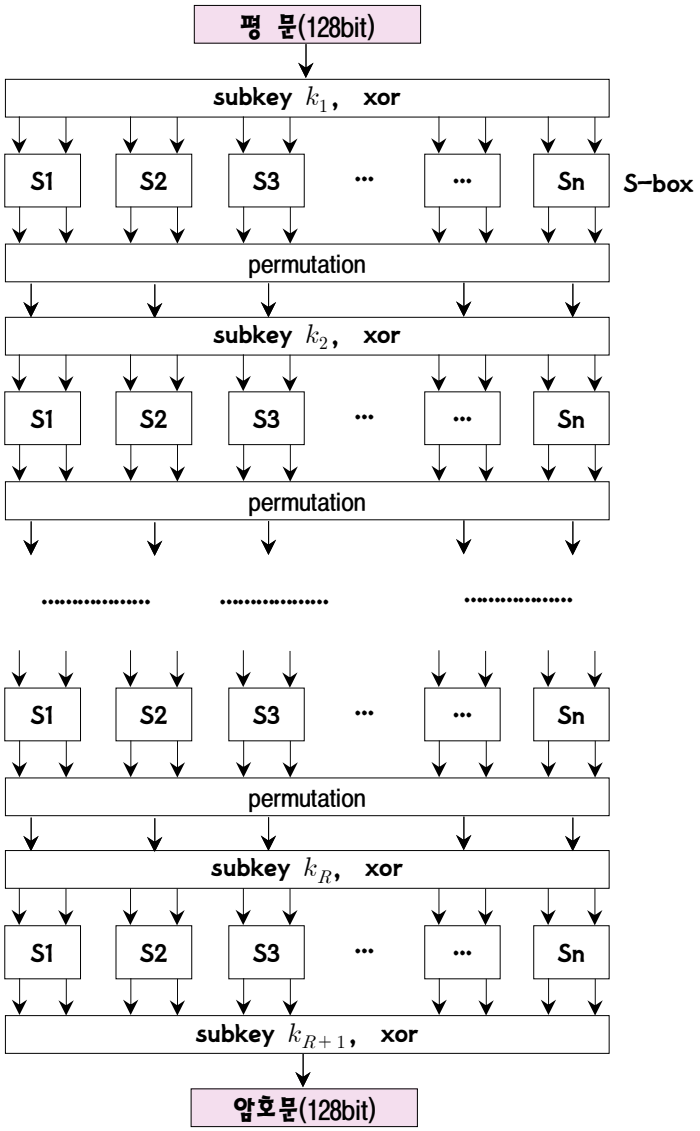
→ 라운드 키는 비밀키로부터 키 생성 알고리즘에 의해 내부적으로 생성된다.

→ **라운드 키**는 **암복호화**에서 **역순**으로 사용된다.(암복호화는 서로 역관계)

⑤ 전체 라운드 수는 알고리즘에 따라 다르다.

→ 알고리즘의 충분한 안전성을 획득하기 위해서는 라운드 수가 증가되어야 한다.

4. SPN(Substitution Permutation Network) 구조



- SPN 구조는 평문과 암호문을 같은 크기의 2부분으로 분할하지 않는다.
- SPN 구조는 **역함수**가 **존재하는 구성요소만을 사용**한다.(**암호**의 한 요소는 **복호**의 한 요소에 **대응**)
- SPN 구조는 각 라운드에서 xor 연산과 역이 존재하는 S-박스, P-박스가 적용된다.
- SPN도 역시 혼돈(confusion)과 확산(diffusion) 이론을 바탕으로 한 구조이다.
- SPN 구조는 각 라운드에서 입력이 모두 비선형변환 되므로 라운드 수가 줄어든다.
- **라운드 키**는 암복호화에서 **역순**으로 사용된다.**(Feistel 구조와 같음)**

// 대칭키 암호구조 정리

구 분	특 징
Feistel 구조	① 평문을 같은 크기의 **2부분으로 분할**하여 암호화 한다. • 분리된 반쪽에 라운드 키를 적용하여 비선형변환하고, • 이를 나머지 반쪽과 XOR 연산을 수행한 후에 서로 치환한다. ② 각 라운드에서 **입력의 반만 비선형변환** 된다. • 입력의 반은 전혀 변환되지 않는다. • 충분한 안전성을 얻기 위해서는 라운드 수가 증가되어야 한다. • 따라서, 하드웨어 구현 시 동작 속도가 느려진다. ③ 암호 알고리즘과 복호 알고리즘에 **동일한 구성요소를 사용**한다. ④ **역함수**가 존재하는 구성요소와 존재하지 않는 구성요소를 **모두 사용**할 수 있다. • 축소 P-박스와 확장 P-박스는 역함수가 존재하지 않는다. ⑤ 암호 알고리즘과 복호 알고리즘은 서로 역관계이다. ⑥ **라운드 키**는 **암복호화**에서 **역순**으로 사용된다. ⑦ 라운드 함수는 Substitution과 Permutation을 통하여 혼돈과 확산 수행한다. ⑧ 적용 알고리즘 : **DES**, SEED, BLOWFISH, FEAL, LOKI, KASUMI, CAST-128
SPN 구조	① 평문을 같은 크기의 2부분으로 분할하지 않는다. ② 각 라운드에서 입력이 **모두 비선형변환** 되므로 라운드 수가 줄어든다. • 따라서, 하드웨어의 동작 속도가 빠르게 된다. • 스마트카드와 RFID 환경에서 효율적으로 구현할 수 있다. ③ **역함수**가 **존재하는 구성요소만을 사용**한다. • 축소 P-박스와 확장 P-박스는 역함수가 없으므로 사용 불가능하다. ④ **라운드 키**는 **암복호화**에서 **역순**으로 사용된다. ⑤ 라운드 함수는 Substitution과 Permutation을 통하여 혼돈과 확산 수행한다. ⑥ 적용 알고리즘 : **AES**, ARIA, SHARK, SAFER, SERPENT, CRYPTON
기타 구조	• **대수적 성질**을 이용하는 구조이다. • 내부적으로 모듈러 연산, XOR 연산 등을 사용한다. • 적용 알고리즘 : IDEA, SKIPJACK, BEAR, LION

// **대칭키 암호시스템**에서 **암복호** 알고리즘은 기본적으로 **비슷**하게 설계한다.

DES	Feistel 구조가 적용된 DES는 **암호** 알고리즘에 사용된 **라운드 키 순서를 거꾸로 적용**하면 **복호** 알고리즘이 된다.**(Forouzan 암호학 168쪽)**
AES	SPN 구조가 적용된 AES의 **복호** 알고리즘은 **암호** 알고리즘에 사용된 **라운드 키 순서가 거꾸로 적용**된다는 것 외는 **암호** 알고리즘과 **비슷**하다.**(Forouzan 암호학 194쪽)**

• 통상적으로, 암복호 알고리즘은 비슷하다.**(Forouzan 암호학 194쪽)**

기출문제 분석

1. Feistel 암호 방식에 대한 설명으로 가장 옳지 않은 것은? [2018년 서울 9급]

① Feistel 암호 방식의 암호 강도는 평문 블록의 길이, 키의 길이, 라운드의 수에 의하여 결정된다.
② Feistel 암호 방식의 복호화 과정과 암호화 과정은 동일하다.
③ AES 암호 알고리즘은 Feistel 암호 방식을 사용한다.
④ Feistel 암호 방식은 대칭키 암호 알고리즘에서 사용된다.

♤ **Feistel 암호 방식**

- AES 암호 알고리즘은 Feistel 암호 방식을 사용한다.**(×)**
  → AES 암호 알고리즘은 SPN(Substitution Permutation Network) 구조이다.

정답 : ③

2. 일정 크기의 평문 블록을 반으로 나누고 블록의 좌우를 서로 다른 규칙으로 계산하는 페이스텔(Feistel) 암호 원리를 따르는 알고리즘은? [2017 경기 추가 9급]

① DES(Data Encryption Standard)
② AES(Advanced Encryption Standard)
③ RSA
④ Diffie－Hellman

♤ **DES(Data Encryption Standard)**

- DES는 평문을 64bit 블록 단위로 나누어 암호화 한다. 암호문도 64bit이다.
- DES는 페이스텔(Feistel) 암호 원리를 따르는 알고리즘이다.
  → 평문 64bit 블록을 L_0, R_0 각 32bit씩 좌우로 분리
  → 분리된 각 부분에 대해 선형과 비선형을 반복적으로 적용해 나간다.
  → 즉, 각 라운드에서 입력의 반은 선형 변환되고, 나머지 반은 비선형 변환된다.

정답 : ①

3. 블록암호 알고리즘을 구성하는 데 사용되는 페이스텔(Feistel) 구조와 SPN 구조에 대한 설명으로 가장 옳은 것은? [2022년 서울 7급]

① 정상적으로 복호화 과정이 수행되기 위해서 페이스텔 구조의 라운드 함수는 가역적(invertible)이어야 한다.
② 페이스텔 구조를 사용하는 대표적인 블록암호 알고리즘으로 AES가 있다.
③ SPN 구조는 Shannon의 혼동(confusion)과 확산(diffusion)이론을 바탕으로 한 구조이다.
④ SPN 구조의 암호화 과정은 최소 2라운드 반복 수행해야 전체 평문이 암호화된다.

♤ **페이스텔(Feistel) 구조와 SPN 구조**

① 정상적으로 복호화 과정이 수행되기 위해서 **페이스텔 구조**의 라운드 함수는 **가역적**(invertible)이어야 한다.**(×)**
→ **페이스텔 구조**는 **역함수**가 **존재하는 구성요소**와 **존재하지 않는 구성요소**를 **모두 사용**할 수 있다.
→ 축소 P-박스와 확장 P-박스는 역함수가 존재하지 않는다.
→ **역함수**를 갖는 함수를 **가역함수**(invertible function) 또는 **일대일** 대응함수라고 한다
→ **SPN 구조**는 **역함수**가 **존재하는 구성요소만을 사용**한다.
→ **SPN 구조** : 축소 P-박스와 확장 P-박스는 역함수가 없으므로 사용 불가능하다.
② 페이스텔 구조를 사용하는 대표적인 블록암호 알고리즘으로 AES가 있다.**(×)**
→ 페이스텔 구조를 사용하는 대표적인 블록암호 알고리즘으로 DES가 있다.
→ AES는 SPN 구조이다.
③ SPN 구조는 Shannon의 **혼동**(confusion)과 **확산**(diffusion) 이론을 바탕으로 한 구조이다.**(○)**
→ **대칭키 암호**는 Shannon의 **혼동**(confusion)과 **확산**(diffusion) 이론을 바탕으로 한 구조이다.
→ **SPN 구조**와 **페이스텔 구조**는 모두 **혼동**과 **확산** 이론을 바탕으로 한 구조이다.
→ **확산**은 암호문과 **평문** 사이의 관계를 알기 어렵게 한다.
→ **혼돈**은 암호문과 **키** 사이의 관계를 알기 어렵게 한다.
④ **SPN 구조**의 암호화 과정은 최소 2라운드 반복 수행해야 전체 평문이 암호화된다.**(×)**
→ AES는 암호키 크기에 따라 10, 12, 14 라운드로 구현된다.

종류	암호키	라운드	라운드 키 수
AES-128	128bit	10	11
AES-192	192bit	12	13
AES-256	256bit	14	15

• 일반적으로 SPN 구조는 암호키 크기에 따라 서로 다른 라운드로 구현된다.
• 라운드 수가 너무 적으면 암호 안전성에 문제가 발생될 수 있고, 쉽게 해독될 수 있다.

정답 : ③

4. 다음은 AES(Advanced Encryption Standard) 암호에 대한 설명이다. 옳지 않은 것은? [2015년 서울 9급]

① 1997년 미 상무성이 주관이 되어 새로운 블록 암호를 공모했고, 2000년 Rijndael을 최종 AES 알고리즘으로 선정하였다.

② 라운드 횟수는 한 번의 암·복호화를 반복하는 라운드 함수의 수행횟수이고, 10/12/14 라운드로 이루어져 있다.

③ 128비트 크기의 입 · 출력 블록을 사용하고, 128/192/256 비트의 가변크기 키 길이를 제공한다.

④ 입력을 좌우 블록으로 분할하여 한 블록을 라운드 함수에 적용시킨 후에 출력값을 다른 블록에 적용하는 과정을 좌우 블록에 대해 반복적으로 시행하는 SPN(Substitution-Permutation Network) 구조를 따른다.

♤ AES(Advanced Encryption Standard)

- AES 알고리즘 구조는 SPN(Substitution Permutation Network) 구조이다.
- SPN 구조는 입력을 좌우 블록으로 분할하지 않는다.
- SPN은 각 라운드에서 입력이 전부 비선형변환 된다.
- 입력을 좌우 블록으로 분할하는 구조는 Feistel 구조이다.

정답 : ④

5. AES(Advanced Encryption Standard)에 대한 설명으로 옳지 않은 것은? [2017년 법무부 9급]

① 128, 192, 256비트 길이의 키를 사용할 수 있다.

② Feistel 구조를 사용한다.

③ 128비트 크기의 블록 대칭키 암호 알고리즘이다.

④ 미국 NIST(National Institute of Standards and Technology)의 공모에서 Rijndael이 AES로 채택되었다.

♤ AES(Advanced Encryption Standard)

- Feistel 구조를 사용한다.(×)
  → AES 알고리즘 구조는 SPN(Substitution Permutation Network) 구조이다.

정답 : ②