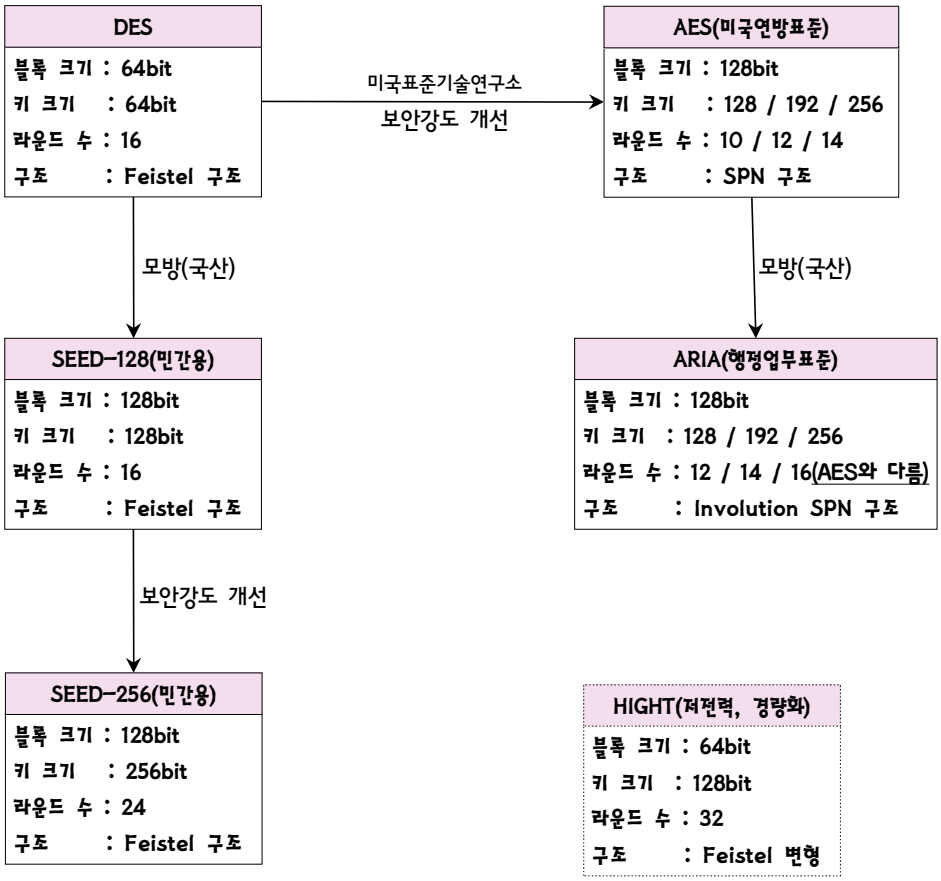
8. 기타, 대칭키 암호

대칭키 암호 알고리즘을 정리하면 다음과 같다.



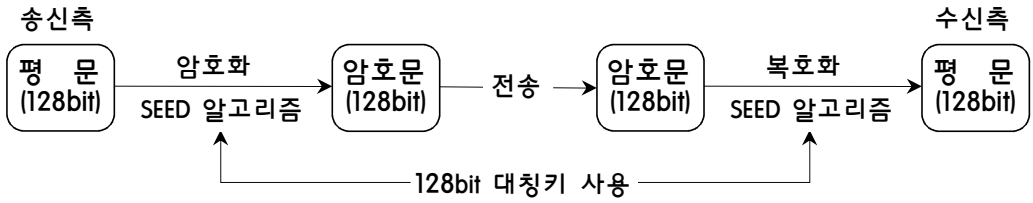
// IDEA(International Data Encryption Algorithm)

- IDEA는 스위스에서 발표된 블록암호 알고리즘이다.(1991년)
- IDEA는 유럽에서 많이 사용되고 있다.
- IDEA의 3가지 주된 연산은 XOR, add mod 216, multiply mod 216+1이다.

블록 크기	• 64bit
비밀키 크기	• 128bit
라운드 수	• 8 라운드
알고리즘 구조	• 기타 구조(S-box를 사용하지 않음)

1. SEED

SEED는 1999년 한국인터넷진흥원과 국내 암호전문가들이 만든 순국산 알고리즘이다.



◈ SEED 설계 사양

알고리즘 구조	• 페이스텔 구조(Feistel structure) / 페이스텔 암호(Feistel cipher)
입출력 블록 크기	• 평문을 128bit 블록 단위로 처리하고, 128bit 블록 암호문을 출력
암호화 키 크기	• 128bit
라운드 수	• 16 라운드
안전성	• 선형공격과 차분공격에 안전하다.
효율성	• 암호화, 복호화 속도는 '3중 DES'보다 빠름

◈ SEED 특징

① SEED는 128bit 블록암호 알고리즘이다. 평문을 128bit 블록 단위로 나누어 암호화한다.
→ 평문/암호문의 블록 크기와 암호화 키 크기가 모두 128bit이다.
② SEED는 우리나라 민간용으로 다양한 분야에서 정보를 보호하기 위해 사용되고 있다.
→ 인터넷 뱅킹, 전자상거래, 무선통신, 지적재산권 보호, 데이터 저장, VPN, e-mail 등
③ SEED는 다른 블록암호 알고리즘에 비해 상대적으로 빠르다.
④ SEED는 무료로 제공하고 있다.(SEED는 원시코드를 e-mail을 통해 배포한다)
→ 2009년 5월까지 3,000여개 이상의 국내외 기업 및 학교에 e-mail로 배포되었다.
⑤ 현재 배포되는 SEED 원시코드는 32비트 프로세서에 맞도록 C와 Java로 구현되었다.

◈ SEED 256

- 2009년에 알고리즘 활용 강화를 위해 256bit 키를 지원하는 SEED 256을 개발하였다.
- 구분하기 위해 “SEED 128 / SEED 256”으로 각각 표기한다.
- 한국인터넷진흥원은 “SEED 128 / SEED 256”을 이용한 제품 생산 및 판매와 관련된 지적재산권에 대하여 사용료를 요구하지 않는다.

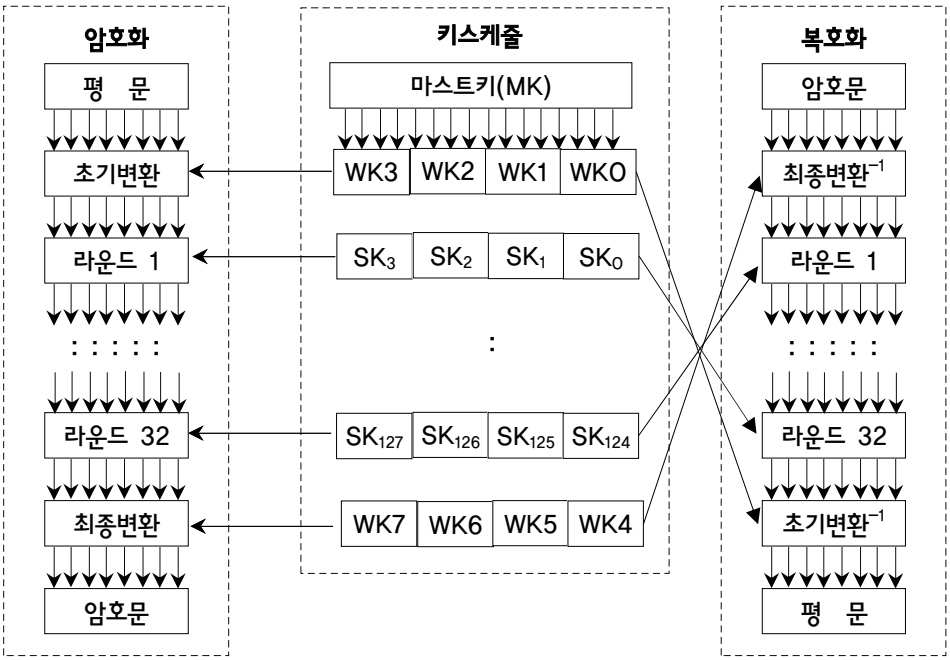
2. HIGHT(HIGh security and light weigHT)

① HIGHT는 2005년 KISA와 고려대가 공동 개발한 64bit 초경량 블록암호이다.
② HIGHT는 경량화를 요구하는 컴퓨팅 환경에서 기밀성을 제공하기 위해 개발되었다.
→ RFID, 사물인터넷 등에 적용 가능
③ HIGHT는 안전성과 효율성을 동시에 고려하는 정교한 설계 논리에 기반하고 있다.
④ HIGHT는 제한된 자원을 가지는 환경에서 구현될 수 있도록 설계하였다.
→ 8비트 단위의 기본적인 연산인 XOR, 덧셈, 순환이동만으로 알고리즘을 설계하였다.
→ HIGHT는 SEED, AES 등에 비해 간단한 알고리즘 구조로 설계되었다.

// HIGHT의 기본 사양

블록 크기	• 64bit(64bit 평문으로 부터 64bit 암호문을 출력한다)
비밀키 크기	• 128bit(마스트키, 암호키)
라운드 수	• 32 라운드
알고리즘 구조	• 일반화된 Feistel 변형 구조

// HIGHT 전체 구조(참고 사항)



• WK는 화이트닝키, SK는 서브키를 나타낸다.

3. ARIA(Academy Research Institute Agency)

① 아리아(ARIA)는 우리나라 국가보안기술연구소에서 개발한 **블록암호** 알고리즘이다.
② ARIA는 Academy(학계)-Research Institute(연구소)-Agency(정부기관)의 첫 글자이다.
→ 아리아라는 이름은 이들의 공동 개발 노력을 함축적으로 나타낸 것이다.
③ ARIA는 2004년 12월부터 우리나라 **행정업무용** 국가표준암호로 사용되고 있다.
→ 2004년 지식경제부의 국가표준(KS)으로 지정, 표준번호 KS X 1213:2004
→ ARIA 문의 및 보급신청 : aria@ensec.re.kr
④ ARIA에서 사용하는 대부분의 연산은 XOR 같은 단순한 바이트 단위 연산이다.
⑤ ARIA는 경량 환경 및 하드웨어에서 효율성 있도록 개발되었다.

// ARIA 기본 사양

블록 크기	• 128bit(128bit 평문으로 부터 128bit 암호문을 출력한다)
비밀키 크기	• 128, 192, 256bit (AES와 같은 규격)
라운드키 크기	• 128bit
라운드 수	• 12, 14, 16 라운드 (키 크기에 따라 결정됨)
알고리즘 구조	• Involution SPN 구조(암호화와 복호화 과정이 같은 구조)

4. IDEA(International Data Encryption Algorithm)

① IDEA는 스위스에서 발표된 블록암호 알고리즘이다.(1991년)
→ IDEA는 유럽에서 많이 사용되고 있다.
② IDEA의 3가지 주된 연산은 XOR, add mod 216, multiply mod 216+1이다.
→ IDEA는 초당 177Mbit의 신속한 처리가 가능하다.
③ IDEA는 안전한 암호 알고리즘으로 평가되었다.
→ 하지만, IDEA는 0이 많이 포함된 키에 대해서는 취약성을 가진다.
④ IDEA는 기존의 PES(Proposed Encryption Standard)를 개량한 것이다.
→ PES는 1990년 Xuejia Lai, James Messey가 만들었다.

// IDEA의 기본 사양

블록 크기	• 64bit
비밀키 크기	• 128bit
라운드 수	• 8 라운드
알고리즘 구조	• 기타 구조(S-box를 사용하지 않음)

5. Blowfish(블로피시)

① Blowfish는 대칭키 블록 암호이다.
→ 1993년 Bruce Schneier(브루스 슈나이어)가 개발하였다.

② Blowfish는 퍼블릭 도메인(public domain)이다.
→ 퍼블릭 도메인은 저작권이 소멸된 저작물을 지칭한다.
→ 현재, Blowfish는 특허가 없다. 누구든지 자유롭게 사용할 수 있다.(특허 포기)

// Blowfish 사양

- 블록 크기 : 64비트
- 키 길이 : 가변 키 길이, 32bit에서 최대 448bit
- 알고리즘 구조 : 16라운드 페이스텔 암호로 S-박스 이용

Blowfish / DES / IDEA 비교 - 32비트 프로세서(팬티엄)

알고리즘	라운드 수	clock cycle/라운드	clock cycle 수/바이트 암호
Blowfish	16	9	18
DES	16	18	45
IDEA	8	50	50

출처 http://www.schneier.com/blowfish.html

- Blowfish는 32비트 프로세서에서 1byte 당 18클럭 사이클의 속도로 암호화 한다.
- Blowfish는 DES, IDEA에 비해 빠르다.

- Blowfish는 구조가 단순하고, 구현이 쉽고, 알고리즘 강도 결정이 용이하다.

6. RC4(Rivest Cipher 4)

- RC4는 Ronald Rivest에 의해 설계된 **바이트 단위의 스트림 암호** 방식이다.(1987년)
- RC4는 **유사난수**를 연속적으로 생성하여 암호화하려는 평문과 **xor** 연산한다.
- RC4는 평문 1byte와 암호키 1byte를 **xor** 연산한다.(암호문 1byte 생성)
- RC4에서 암호키는 1~256byte 중 어떤 값이라도 된다.
- RC4 알고리즘은 랜덤 치환에 기초해서 만들어진다.
- 하나의 바이트를 출력하기 위해서 8번에서 16번의 기계연산이 필요하다.
- 응용 : WEP, SSL 등의 프로토콜에서 사용

7. RC5

① RSA 개발자인 Ron Rivest가 개발한 **블록암호** 알고리즘이다.(1994년)
② RC5는 하드웨어 및 소프트웨어에 적합하다.(기본 연산 +, -, xor, rotate만 사용)
③ RC5는 **가변적인 암호키** 길이를 사용한다.
→ 56bit, 64bit, 72bit의 암호문에 대한 해독 작업 프로젝트를 실시하고 있다.
→ 현재 56bit, 64bit의 암호문에 대한 해독은 성공하였다.(상금 지급)
④ RC5는 가변적 라운드 수를 적용한다.
⑤ RC5는 워드 크기가 다른 프로세서에 적용할 수 있다.
⑥ RC5는 속도를 빠르게 하기 위해 단순화시켰다.
⑦ RC5는 제한된 메모리를 사용하는 시스템에도 적합하다.

기출문제 분석

1. 블록암호 알고리즘에 대한 설명으로 옳지 않은 것은? [2017년 국가 7급]

① IDEA - 상이한 대수 그룹으로부터의 세 가지 연산을 혼합하는 방식
② Blowfish - 키의 크기가 가변적이므로 안전성과 성능의 요구에 따라 유연하게 사용
③ SEED - 1999년 KISA와 국내 암호전문가들이 개발한 128비트 블록암호
④ ARIA - 국가보안기술연구소 주관으로 64비트 블록암호로 128비트 암호화키만 지원

♤ **블록암호 알고리즘 – ARIA**

- ARIA - 국가보안기술연구소 주관으로 64비트 블록암호로 128비트 암호화키만 지원**(×)**
→ ARIA는 128bit 블록암호로 128, 192, 256bit 암호키를 지원(AES와 같은 규격)

정답 : ④

2. 다음 지문에서 설명하는 것은? [2017년 서울 9급]

- **국내의 학계, 연구소, 정부 기관이 공동으로 개발한 블록 암호이다.**
- **경량 환경 및 하드웨어 구현을 위해 최적화된 Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘이다.**

---

① ARIA ② CAST ③ IDEA ④ LOKI

♤ **ARIA(Academy Research Institute Agency)**

- 아리아(ARIA)는 우리나라 국가보안기술연구소에서 개발한 블록암호 알고리즘이다.
- 아리아 구조는 Involution SPN 구조(암호화와 복호화 과정이 같은 구조)

◉ **CAST**

- CAST는 캐나다에서 설계된 블록 암호의 한 종류이다.(Feistel 구조)
- CAST-128은 128비트 키와 64비트 블록을 가진다.
- CAST-256은 CAST-128의 확장으로 256비트 키와 128비트 블록을 가진다.

◉ **LOKI**

- LOKI는 1990년 호주에서 설계된 블록 암호의 한 종류이다.(Feistel 구조)
- LOKI는 DES와 유사한 암호 알고리즘이다.

정답 : ①

3. 대칭키 암호 알고리즘에 대한 설명으로 옳은 것만을 모두 고르면? [2018년 지방 9급]

ㄱ. AES는 128/192/256 비트 키 길이를 지원한다.
ㄴ. DES는 16라운드 Feistel 구조를 가진다.
ㄷ. ARIA는 128/192/256 비트 키 길이를 지원한다.
ㄹ. SEED는 16라운드 SPN(Substitution Permutation Network) 구조를 가진다.

---

① ㄱ, ㄹ ② ㄴ, ㄷ
③ ㄱ, ㄴ, ㄷ ④ ㄱ, ㄴ, ㄹ

♤ **대칭키 암호 알고리즘**

ㄹ. SEED는 16라운드 SPN(Substitution Permutation Network) 구조를 가진다.**(×)**
→ SEED-128은 16라운드 Feistel 구조를 가진다.

정답 : ③