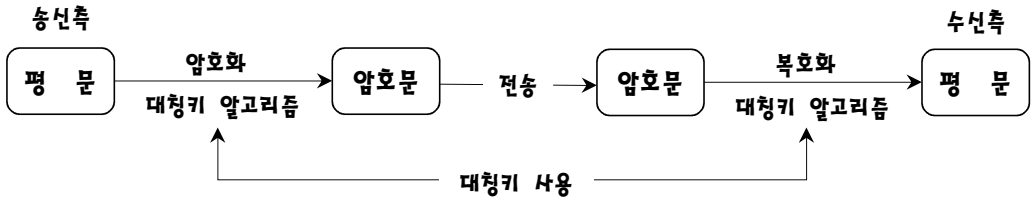
1. 대칭키 암호 개요

대칭키 암호 알고리즘은 암호화와 복호화에 **동일한 비밀키**를 사용한다.



① 대칭키 암호에 사용되는 키를 **'대칭키, 비밀키, 관용키, 공용키, 단일키'**라 한다.
② 송수신자는 적절한 방법으로 안전하게 대칭키를 미리 서로 공유해야 한다.
→ 교환 과정에서 제3자에게 키가 누설될 가능성이 항상 존재한다.(문제점)
③ 대칭키로 암호화된 문서는 동일한 대칭키를 가지고 있는 사람만 복호화 할 수 있다.
④ 대칭키 암호는 내부구조가 간단하여, 속도가 빠르고, 경제적이다.
→ 비대칭키(공개키) 암호는 대칭키 암호에 비해 속도가 매우 느리다.

// 대칭키 암호 알고리즘 구분

대칭키 암호는 "스트림 암호와 블록 암호" 알고리즘으로 구분한다.

스트림 암호	• 스트림 암호는 암복호화에 한 번에 한 개의 기호가 적용된다.**(bit, 문자)** • 스트림 암호는 블록 암호에 비해 암호 단위가 상대적으로 작다. • 그런데, 스트림 암호도 평문을 한 번에 32bit씩 연속 암호화 할 수 있다. ◇ **예를 들면** 01011001 → **평문** XOR) 11110000 → **키 스트림** 10101001 → **암호문**
블록 암호	• 블록 암호는 고정길이의 블록**(64bit, 128bit 등)**을 암복호화 한다. • 블록 암호는 임의의 평문을 일정 길이의 블록으로 나누어 암호화 한다. • 각 입력 블록에 블록 암호 알고리즘을 반복 적용하여 암호문을 생성한다. • 블록 암호는 스트림 암호에 비해 암호 단위가 상대적으로 크다.

기출문제 분석

1. 대칭키 암호에 대한 설명으로 옳지 않은 것은? [2020년 국회 9급]

① 부인방지 기능을 제공한다.
② 비대칭키 암호에 비해 속도가 빠르다.
③ 송신자와 수신자가 동일한 비밀키를 사용한다.
④ IDEA는 대칭키 암호 알고리즘이다.
⑤ RC4는 스트림 암호 알고리즘이다.

♤ **대칭키 암호**

· 부인방지 기능을 제공한다.(×)
→ 대칭키 암호는 부인방지 기능을 제공하지 못한다.(취약)
→ 대칭키 암호는 송수신자가 동일한 키를 사용하므로

정답 : ①

2. 〈보기〉에서 설명하는 암호화 알고리즘으로 옳은 것은? [2016년 서울 9급]

---<보기>---

- **Ron Rivest가 1987년에 RSA Security에 있으면서 설계한 스트림 암호이다.**
- **바이트 단위로 작동되도록 만들어진 다양한 크기의 키를 사용한다.**
- **사용되는 알고리즘은 랜덤 치환에 기초해서 만들어진다.**
- **하나의 바이트를 출력하기 위해서 8번에서 16번의 기계연산이 필요하다.**

---

① RC5 ② SEED ③ SKIPJACK ④ RC4

♤ **RC4(Rivest Cipher 4)**

- Ronald Rivest에 의해 설계된 바이트 단위의 **스트림 암호**화 방식
- 평문 1byte와 암호키 1byte가 XOR 연산처리 되어 암호문 1byte를 생성한다.
  → 유사난수를 연속적으로 생성하여 암호화하려는 평문과 XOR 연산
- 암호문을 생성하는 기본 구성 키는 1~256byte 중 어떤 값이라도 된다.
  → **다양한 키 길이**를 갖도록 설계된 바이트 기반의 알고리즘이다.
- 사용되는 알고리즘은 랜덤 치환에 기초해서 만들어진다.
- 하나의 바이트를 출력하기 위해서 8번에서 16번의 기계연산이 필요하다.

정답 : ④

3. 스트림 암호에 대한 설명으로 옳은 것은? [2018년 국가 7급]

① 대표적인 스트림 암호 방식인 RC4는 다양한 키 길이를 갖도록 설계된 바이트 기반의 알고리즘이다.
② 안전성은 키열(key stream)을 생성하는 의사 난수 생성기의 안전성에 반비례한다.
③ 블록 암호와 달리 구현이 어렵고 속도가 느린 단점이 있다.
④ 키열의 반복 주기가 짧을수록 암호문을 해독하기가 더 어려워진다.

♤ **스트림 암호**

---

② 안전성은 키열(key stream)을 생성하는 의사 난수 생성기의 안전성에 반비례한다.**(×)**
→ 의사 난수 생성기의 안전성에 비례한다.
③ 블록 암호와 달리 구현이 어렵고 속도가 느린 단점이 있다.**(×)**
→ 구현이 쉽고 속도가 빠르다.
④ 키열의 반복 주기가 짧을수록 암호문을 해독하기가 더 어려워진다.**(×)**
→ 키열의 반복 주기가 짧을수록 암호문을 해독하기가 더 쉬워진다.

정답 : ①

4. 스트림 암호에 대한 설명으로 옳지 않은 것은? [2021년 지방 9급]

① 데이터의 흐름을 순차적으로 처리해 가는 암호 알고리즘이다.
② 이진화된 평문 스트림과 이진 키스트림 수열의 XOR 연산으로 암호문을 생성하는 방식이다.
③ 스트림 암호 알고리즘으로 RC5가 널리 사용된다.
④ 구현이 용이하고 속도가 빠르다는 장점이 있다.

♤ **스트림 암호**

• **스트림 암호** 알고리즘으로 RC5가 널리 사용된다.**(×)** → RC5는 **블록암호** 알고리즘이다.

// 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.
④ RC5는 가변적 라운드 수를 적용한다.
⑤ RC5는 워드 크기가 다른 프로세서에 적용할 수 있다.
⑥ RC5는 제한된 메모리를 사용하는 시스템에도 적합하다.

정답 : ③

5. 대칭키 암호에 대한 설명으로 옳지 않은 것은? [2014년 국회 9급]

① 공개키 암호 방식보다 암호화 속도가 빠르다.
② 비밀키 길이가 길어질수록 암호화 속도는 빨라진다.
③ 대표적인 대칭키 암호 알고리즘으로 AES, SEED 등이 있다.
④ 송신자와 수신자가 동일한 비밀키를 공유해야 된다.
⑤ 비밀키 공유를 위해 공개키 암호 방식이 사용될 수 있다.

♤ **대칭키 암호**

• 비밀키 길이가 길어질수록 암호화 속도는 빨라진다.**(×)**
→ 비밀키 길이가 길어질수록 암호화 속도는 느리게 된다.(○)

정답 : ②

6. 공개키 암호와 대칭키 암호에 대한 설명으로 옳은 것은? [2016년 국회 9급]

① 공개키를 교환하기 위해 대칭키 암호를 이용한다.
② 128비트 RSA 공개키와 2048비트 대칭키는 안전도가 비슷하다.
③ 두 암호 모두 기밀성과 무결성을 동시에 보장한다.
④ 긴 메시지 암호에는 하이브리드 방식의 암호가 효율적이다.
⑤ 공개키 암호는 대칭키 암호에 비해 처리속도가 빠르다.

♤ **공개키 암호와 대칭키 암호**

---

① 공개키를 교환하기 위해 대칭키 암호를 이용한다.**(×)**
→ 대칭키를 교환하기 위해 공개키 암호를 이용한다.
② 128비트 RSA 공개키와 2048비트 대칭키는 안전도가 비슷하다.**(×)**
→ 공개키와 대칭키 안전도를 직접 비교하는 것은 큰 의미가 없다.
③ 두 암호 모두 기밀성과 무결성을 동시에 보장한다.**(×)**
→ 대칭키 암호는 무결성을 보장하는 것은 아니다.
⑤ 공개키 암호는 대칭키 암호에 비해 처리속도가 빠르다.**(×)**
→ 대칭키 암호는 공개키 암호에 비해 처리속도가 빠르다.

정답 : ④