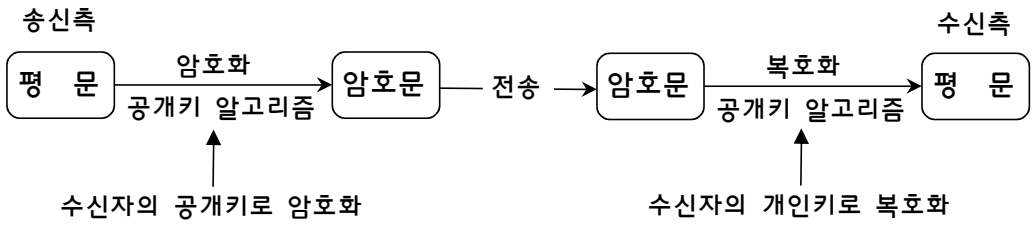
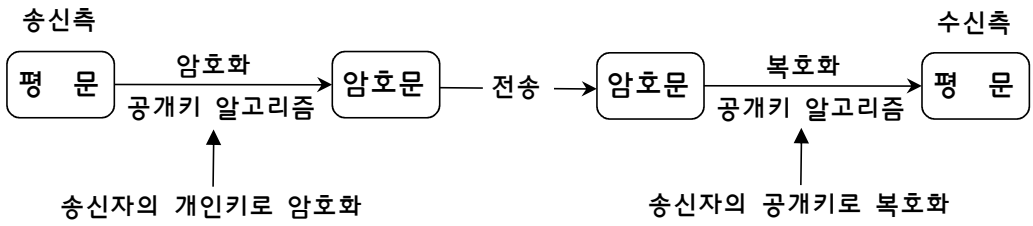
2. 공개키 암호 응용

공개키 암호는 다음 2가지 분야에 활용할 수 있다. 즉, 2가지 기능을 가진다.

◈ 공개키를 이용한 문서 암호화(기밀성)



◈ 개인키를 이용한 문서에 대한 전자서명(인증, 무결성, 부인방지)



◈ 공개키 암호 정리

암호화한 키	설 명	활용 분야
공개키로 암호화한 경우	• 암호화된 문서는 개인키 소유자만이 복호화할 수 있다. • 해서, 문서에 대한 암호화 기능을 가진다.(기밀성 제공)	비밀통신
개인키로 암호화한 경우	• 문서는 공개된 공개키로 누구나 복호화할 수 있다. • 누구나 복호화가 가능하므로 기밀성 역할은 불가능 • 하지만, 개인키로 문서를 암호화한 사람은 오직 1명이다. • 전자서명 기능을 가진다.(인증, 무결성, 부인방지 제공)	전자서명

• 공개키 암호에서 메시지를 “공개키로 암호화하느냐? 개인키로 암호화하느냐?”에 따라서 활용되는 분야는 전혀 다르다.

◈ **공개키 기반구조에서 메시지 송수신(중요!)**

다음은 '놀부와 흥부' 사이의 메시지 송수신 과정에서 사용되는 키를 보여준다.

놀부(송신자)

흥부야!
형 놀부다.
잘 익은 사과 80상자 보내라.
돈은 나중에 줄께!

메시지 암호 : 흥부의 공개키(수신측 공개키)
전자서명 : 놀부의 개인키(송신측 개인키)

▼

흥부(수신자)

흥부야!
형 놀부다.
잘 익은 사과 80상자 보내라.
돈은 나중에 줄께!

메시지 해독 : 흥부의 개인키(수신측 개인키)
사용자 인증 : 놀부의 공개키(송신측 공개키)

• 흥부가 놀부의 메시지를 받았을 때, 궁금한 것이 뭘까?
• 메시지 무결성과 메시지를 보낸 사람이 정말로 놀부인가? 이다.

• 메시지 무결성(integrity) : "메시지가 전송 도중에 변경되지 않았다"는 뜻이다.
• 메시지 인증(authentication) : "메시지가 올바른 송신자(놀부)로부터 온 것이다"는 뜻이다.

// **표로 정리하면**

하는 일	사용되는 키
암호화된 메시지 송신	수신자(흥부)의 공개키
암호화된 전자서명 송신	송신자(놀부)의 개인키
암호화된 메시지 수신 후 해독(복호화)	수신자(흥부)의 개인키
암호화된 전자서명 해독 및 송신자 인증	송신자(놀부)의 공개키

• 주어진 내용은 시험에 계속 출제되고 있다.

기출문제 분석

1. 다음은 공개키 암호시스템을 이용하여 Alice가 Bob에게 암호문을 전달하고, 이를 복호화하는 과정에 대한 설명이다. ㉠~㉢에 들어갈 내용으로 옳은 것은? [2014년 국가 7급]

ㄱ. Bob은 개인키와 공개키로 이루어진 한 쌍의 키를 생성한다.
ㄴ. Bob은 (㉠)를 Alice에게 전송한다.
ㄷ. Alice는 (㉡)를 사용하여 메시지를 암호화한다.
ㄹ. Alice는 생성된 암호문을 Bob에게 전송한다.
ㅁ. Bob은 (㉢)를 사용하여 암호문을 복호화한다.

---

① ㉠ Bob의 공개키 ㉡ Alice의 공개키 ㉢ Alice의 개인키
② ㉠ Bob의 개인키 ㉡ Bob의 공개키 ㉢ Bob의 개인키
③ ㉠ Bob의 개인키 ㉡ Alice의 공개키 ㉢ Alice의 개인키
④ ㉠ Bob의 공개키 ㉡ Bob의 공개키 ㉢ Bob의 개인키

♤ **공개키 암호시스템**

ㄱ. Bob은 개인키와 공개키로 이루어진 한 쌍의 키를 생성한다.
ㄴ. Bob은 (㉠ Bob의 공개키)를 Alice에게 전송한다.
ㄷ. Alice는 (㉡ Bob의 공개키)를 사용하여 메시지를 암호화한다.
ㄹ. Alice는 생성된 암호문을 Bob에게 전송한다.
ㅁ. Bob은 (㉢ Bob의 개인키)를 사용하여 암호문을 복호화한다.

정답 : ④

2. 공개키 기반 구조(PKI)에 대한 설명으로 옳지 않은 것은? [2014년 계리직]

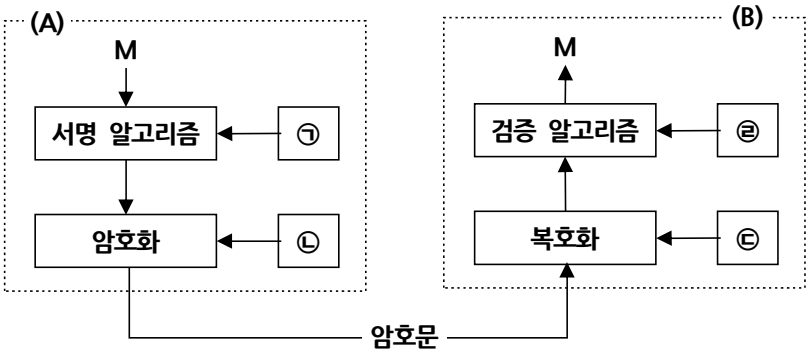
① 인증기관은 공개키 인증서의 발급을 담당한다.
② 공개키 기반 구조는 부인방지 서비스 제공이 가능하다.
③ 공개키로 암호화 한 데이터는 암호화에 사용된 공개키로 해독한다.
④ 공개키 기반 구조는 공개키 알고리즘을 통한 암호화와 전자서명을 제공하는 복합적인 보안 시스템 환경이다.

♤ **공개키 기반 구조**

• 공개키로 암호화 한 데이터는 암호화에 사용된 공개키의 짝인 **개인키로 해독**한다.

정답 : ③

3. A가 B에게 공개키 알고리즘을 사용하여 서명과 기밀성을 적용한 메시지(M)를 전송하는 그림이다 . ㉠~㉣에 들어갈 용어로 옳은 것은? [2017년 지방 9급]



	㉠	㉡	㉢	㉣
①	A의 공개키	B의 공개키	A의 개인키	B의 개인키
②	A의 개인키	B의 개인키	A의 공개키	B의 공개키
③	A의 개인키	B의 공개키	B의 개인키	A의 공개키
④	A의 공개키	A의 개인키	B의 공개키	B의 개인키

♤ **공개키 알고리즘 기능**

- 문서 전자서명 : 송신자의 (개인키, 공개키)
- 문서 암복호화 : 수신자의 (공개키, 개인키)

정답 : ③