2010-1학기 현대암호학

제 9장 디지털 서명

박 종 혁

Tel: 970-6702
Email: jhpark1@snut.ac.kr

9.1 주요 내용

- 디지털 서명
  - 문서에 하는 인감 날인이나 사인에 해당하는 기능을 컴퓨터의 세계에서 실현하기 위한 기술
  -
- 디지털 서명을 사용하면
  - 변경이나 거짓 행세를 검출
  - 부인을 방지

9.2 디지털 서명

- 서명을 할 경우에 요구되는 조건
  - 문서가 읽을 수 있는 평문으로 저장되어 있어야 한다
  - 분쟁 발생시 증명에 사용될 해당 문서의 암호문도 저장하고 있어야 한다

- 메시지 전문을 암호화 하는 방법을 통해 서명을 할 경우에는 분명히 이 두 조건을 만족한다.
- 하지만 위와 똑 같은 효과를 가지면서 더 효율적인 방법이 있다.

인증자

- **인증자**(authenticator) : 문서의 기능을 대신하는 작은 비트블록을 암호화 하는 방법을 사용

- 인증자가 갖춰야 할 성질
  - 인증자는 변경하지 않으면서 문서만 변경하는 것이 불가능해야 한다함

인증자

- 이 인증자가 송신자의 개인키를 이용하여 암호화되었다면 메시지의 출처, 내용, 그리고 순서까지 확인해주는 서명이 되는 것이다.

- 예
  - SHA-1 같은 안전한 해시코드

9.2.1 앨리스의 차용서

- 이메일로 차용서
「**밥님께, 귀하로부터 일금 100만원을 차용합니다. 앨리스**」를 보낸다고 할 경우

- 이메일로 보낸 차용서는 간단히 위조를 할 수 있고 법적인 효력도 갖지 못한다.

- 앨리스가 쓴 메일을 누군가가 **변경**했을지도 모르고,
- 처음부터 앨리스인 것처럼 **거짓 행세**를 한 누군가가 보낸 것인지도 모르고,
- 나중에 앨리스가 「그런 차용서 난 몰라」라고 부인할 수도 있다.

9.2.2 메시지 인증 코드에서 디지털 서명으로

메시지 인증 코드의 한계

- 메시지 인증 코드를 사용하면 메시지의 변경과 거짓 행세를 검출할 수 있음
- 메시지의 무결성을 확인하여 인증을 행할 수 있음
- 차용서를 만드는 데 메시지 인증 코드를 사용할 수는 없다.
  - 메시지 인증 코드는 부인 방지에는 도움이 되지 않기 때문

디지털 서명을 이용한 해결

- 앨리스가 사용하는 키는 앨리스만이 알고 있는 개인적인 것
- 앨리스는 메시지 송신 시에 그 개인적인 키를 써서 「서명」을 작성
- 수신자 밥은 앨리스의 키와는 다른 키를 써서 「서명」을 검증

=> 디지털 서명(digital signature)

9.2.3 서명 작성과 서명 검증

- 메시지의 서명을 작성하는 행위
  - 메시지의 송신자 앨리스가 수행
  - 간단히 「메시지에 서명한다」라고도 함
  - 서명 작성은 「나는 이 메시지의 내용을 인정한다」라는 표시로 메시지를 기초로 디지털 서명 값을 계산하는 행위
- 메시지의 서명을 검증하는 행위
  - 서명의 검증은 「이 메시지 서명은 분명히 앨리스의 것인지 어떤지」를 조사하는 행위
  - 서명의 검증 결과: 성공 or 실패

전용 키

- 앨리스는 「서명용 키」를 사용해서 메시지 서명을 작성
- 밥이나 빅터는 「검증용 키」를 사용해서 메시지 서명을 검증.
- 디지털 서명에서는 「서명용 키」와 「검증용 키」가 나누어져 있어서 검증용 키로 서명을 작성할 수는 없음
  - 「서명용 키」: 서명을 하는 사람만이 가지고 있음
  - 「검증용 키」: 서명을 검증하는 사람이라면 누구라도 가질 수 있음

디지털 서명과 공개 키

- 디지털 서명은 공개 키 암호와 밀접한 관계가 있음

  ➔ 디지털 서명은 공개 키 암호를 「역으로 사용」함으로써 실현

공개 키 암호와 디지털 서명의 키 사용 방법

표 9-1 공개 키 암호와 디지털 서명의 키 사용 방법

	개인 키	공개 키
공개 키 암호	수신자가 복호화에 사용	송신자가 암호화에 사용
디지털 서명	서명자가 서명 작성에 사용	검증자가 서명 검증에 사용
키는 누가 갖는가?	개인이 갖는다.	필요한 사람은 아무나 가지고 있어도 된다.

9.2.4 공개 키 암호와 디지털 서명

- 디지털 서명에서도 마찬가지로 공개 키와 개인 키의 키 쌍을 사용
- 그러나 두 키의 사용 방법은 공개 키 암호 시스템을 사용할 때와는 반대

- 메시지를 **개인 키로 암호화하는 것이 서명 작성**
- 그 암호문을 **공개 키로 복호화하는 것이 서명 검증**

공개 키에 의한 암호화(공개 키 암호)

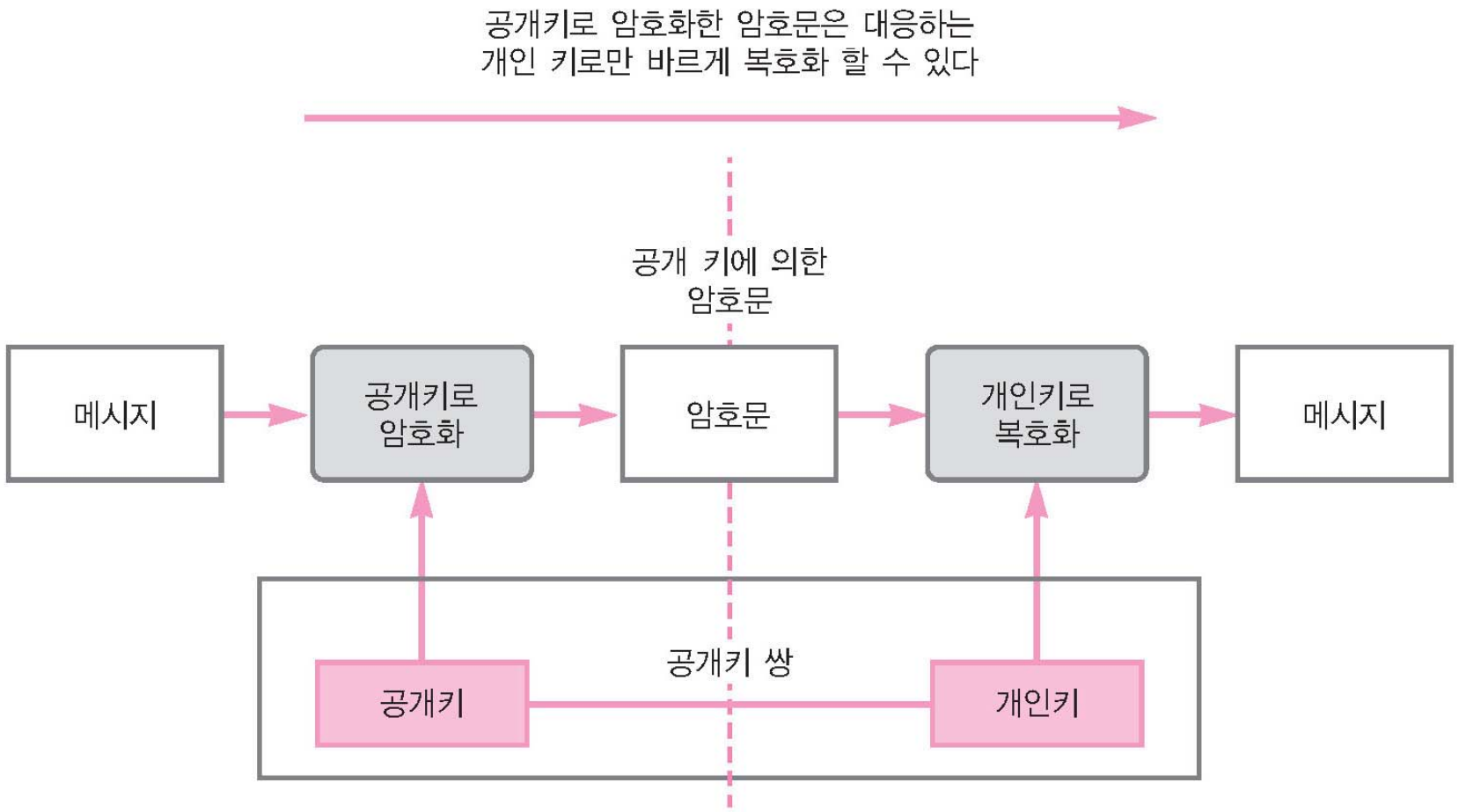

그림 9-1 공개 키에 의한 암호화(공개 키 암호)

개인 키에 의한 암호화(디지털 서명)

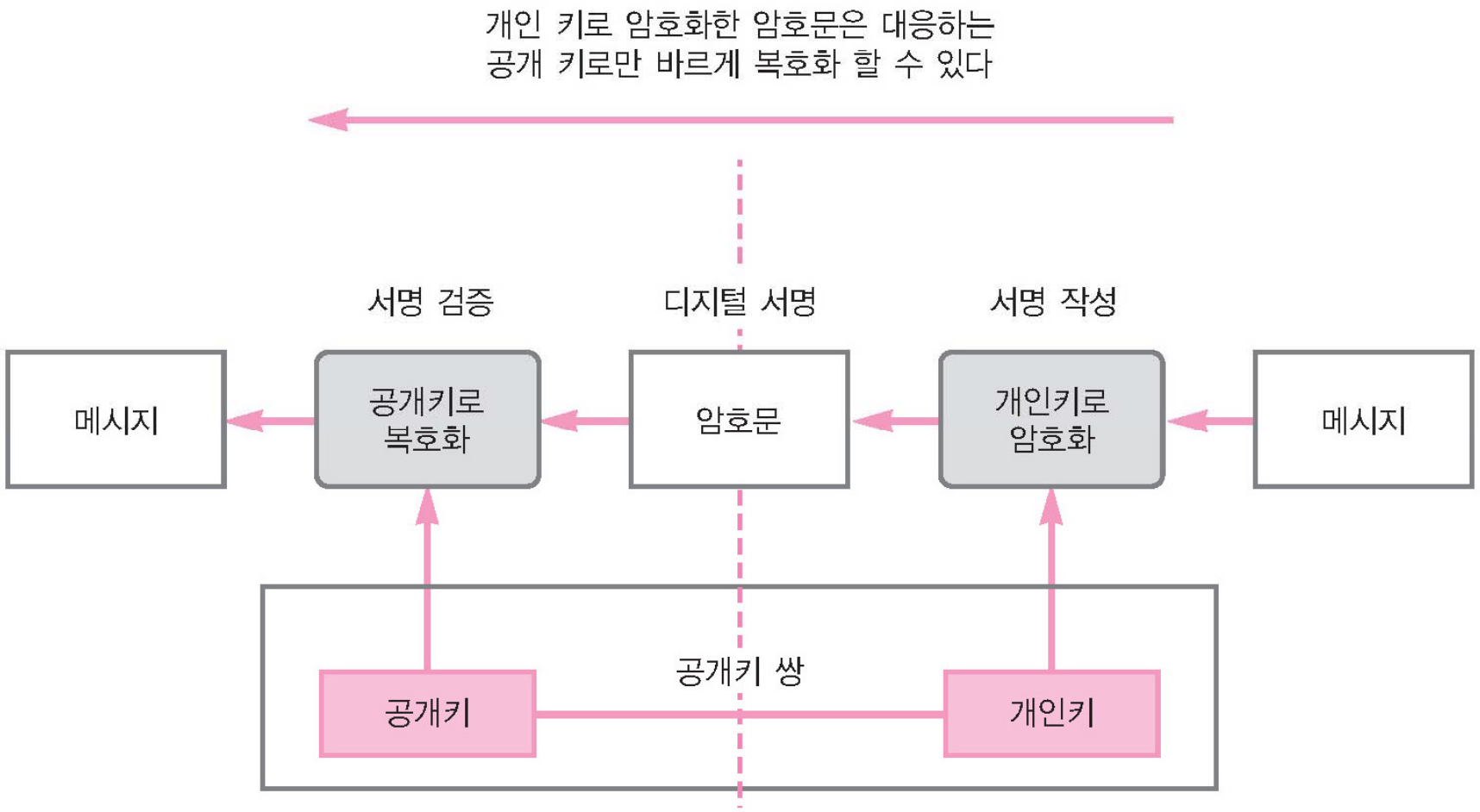

그림 9-2 개인 키에 의한 암호화(디지털 서명)

공개 키 암호는 누구라도 암호화할 수 있다(공개 키 암호)

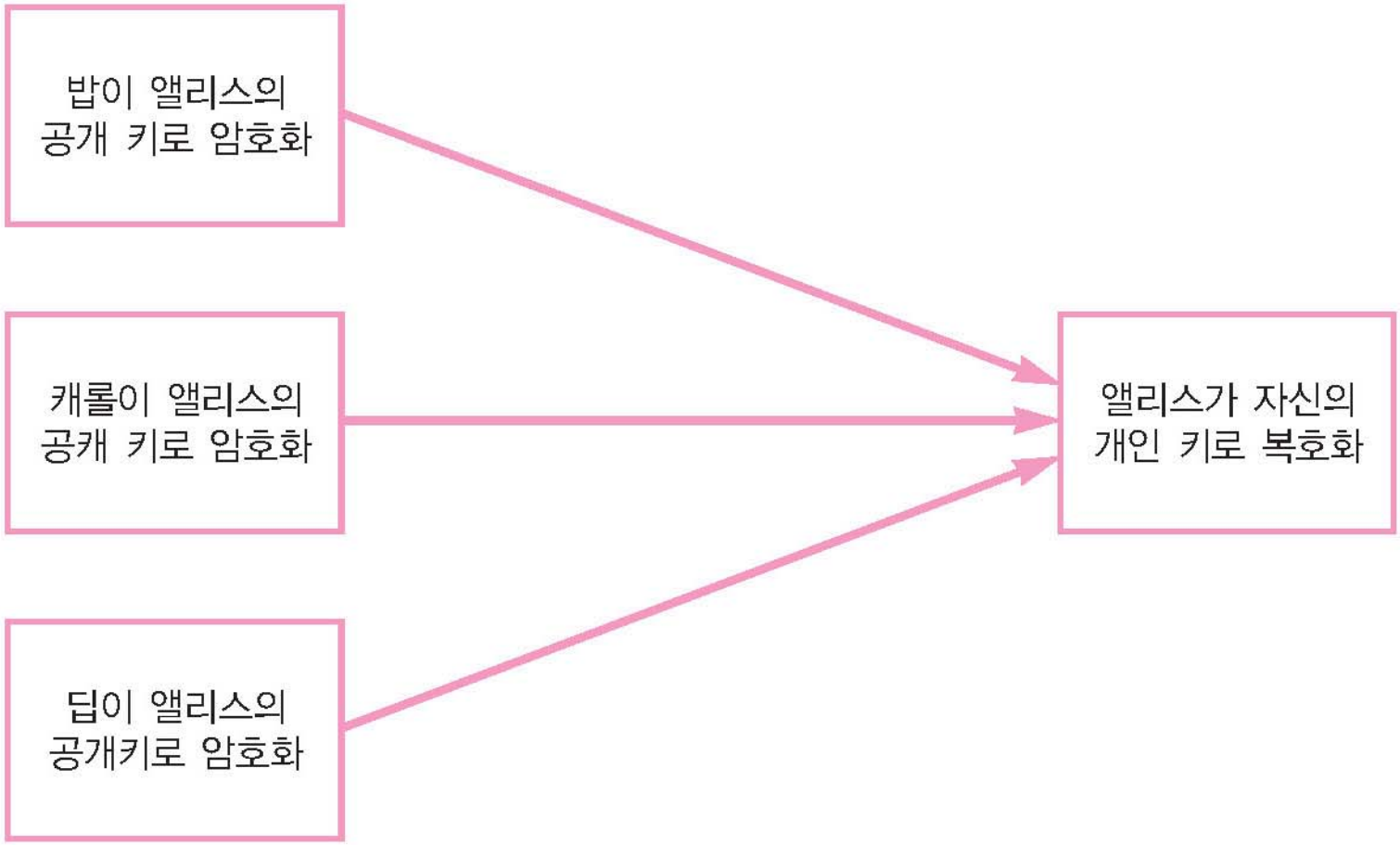

그림 9-3 공개 키 암호는 누구라도 암호화할 수 있다(공개 키 암호).

디지털 서명은 누구라도 서명의 검증을 할 수 있다(디지털 서명)

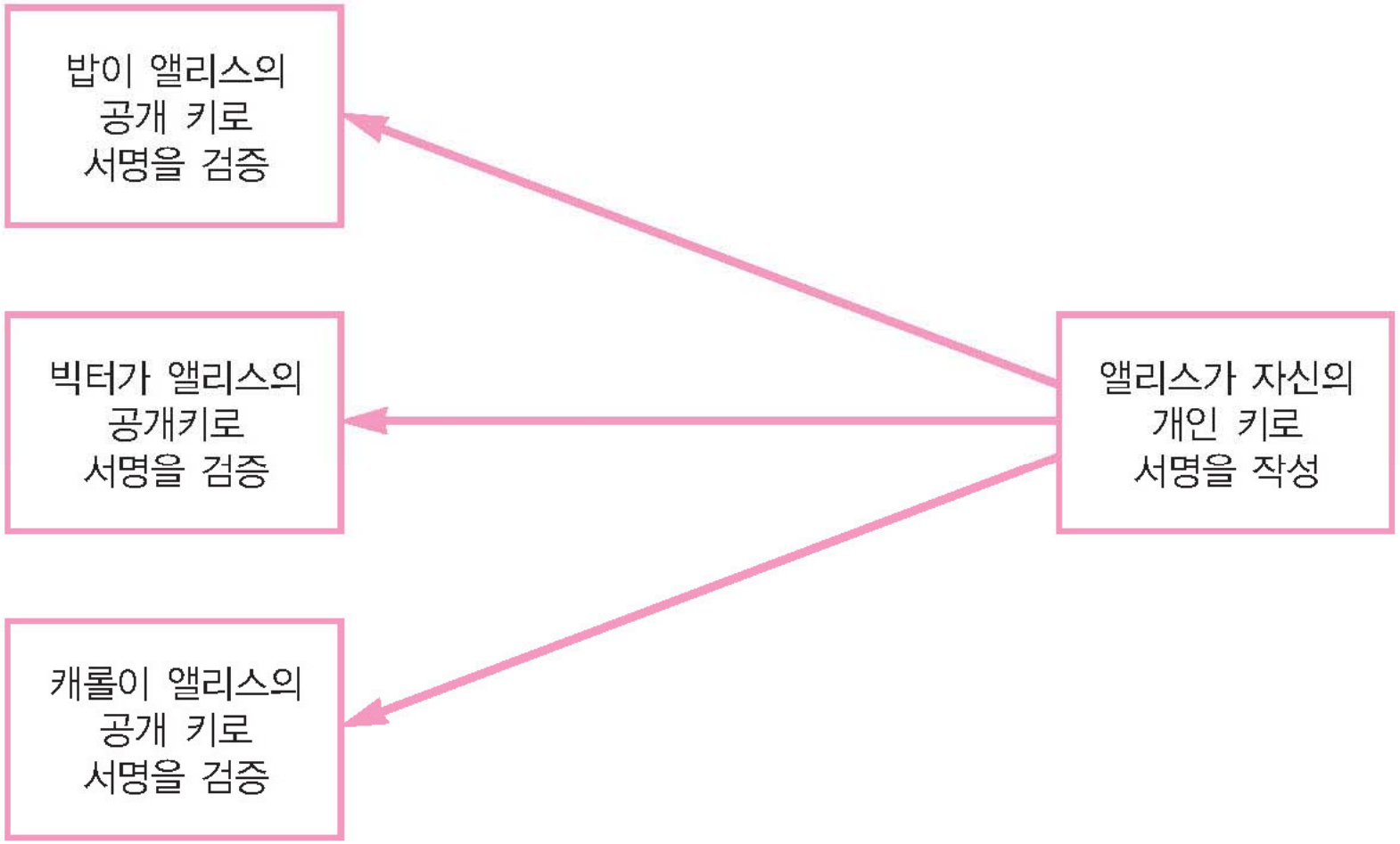

그림 9-4 디지털 서명은 누구라도 서명의 검증을 할 수 있다(디지털 서명).

9.3 디지털 서명 방법

- 메시지에 직접 서명하는 방법
- 메시지의 해시 값에 서명하는 방법

9.3.1 메시지에 직접 서명하는 방법

앨리스가 메시지에 서명하고, 밥이 서명을 검증한다

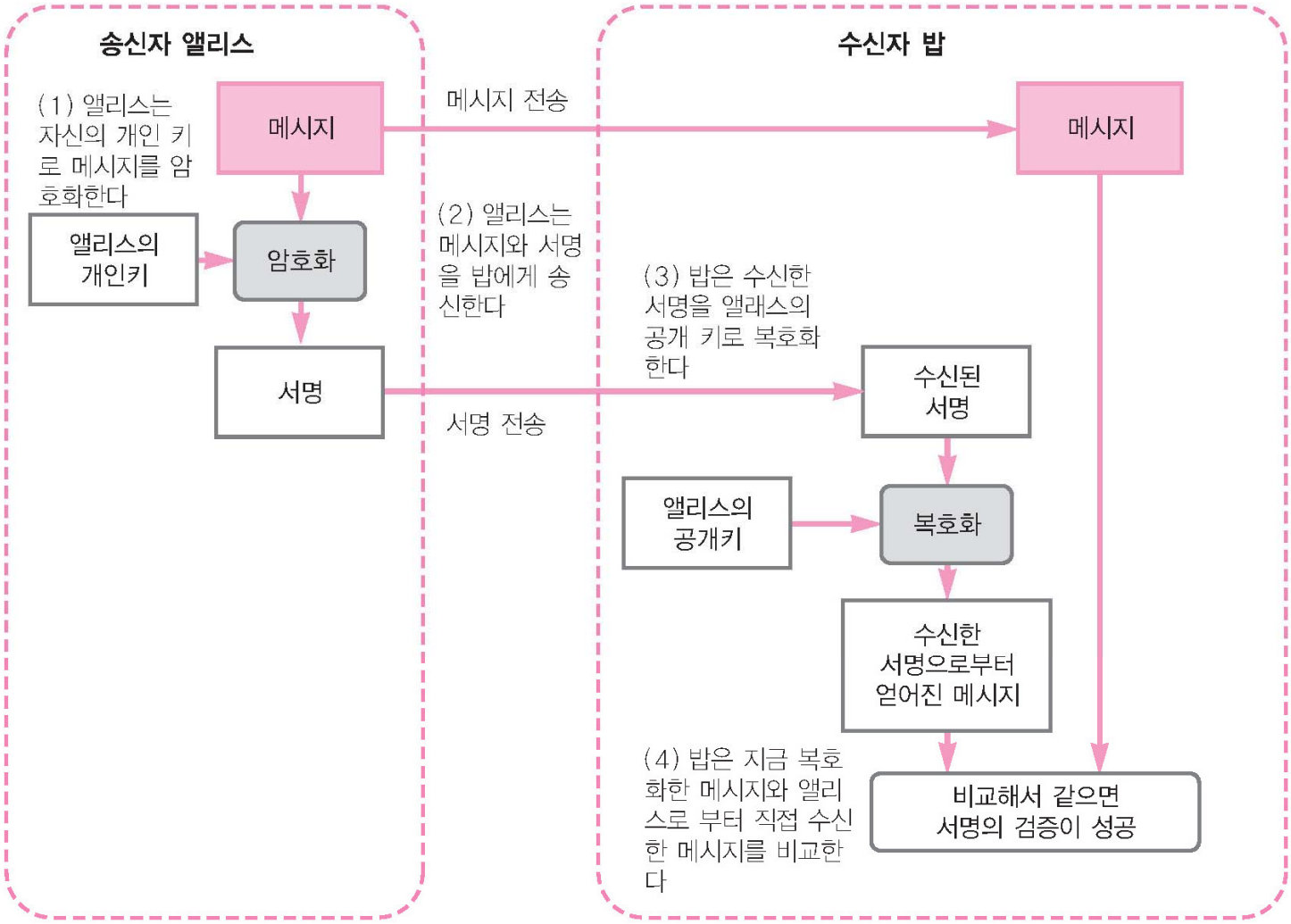

그림 9-5 앨리스가 메시지에 서명하고, 밥이 서명을 검증한다

9.3.2 메시지의 해시 값에 서명하는 방법

- 메시지 전체를 암호화(메시지에 서명)하는 대신
  - 일방향 해시 함수를 사용해서 메시지의 해시 값을 구함
  - 그 해시 값을 암호화(해시 값에 서명)하도록 함
- 메시지가 아무리 길어도 해시 값은 짧기 때문에 암호화(서명)하는 것이 훨씬 수월해짐

절차

(1) 앨리스는 일방향 해시 함수로 메시지의 해시 값을 계산한다.

(2) 앨리스는 자신의 개인 키로 해시 값을 암호화한다.

(3) 앨리스는 메시지와 서명을 밥에게 송신한다.

(4) 밥은 수신한 서명을 앨리스의 공개 키로 복호화한다.

(5) 밥은 수신한 서명으로부터 얻어진 해시 값과 앨리스로부터 직접 수신한 메시지의 해시 값을 비교한다.

앨리스가 메시지의 해시 값에 서명하고 밥이 서명을 검증한다

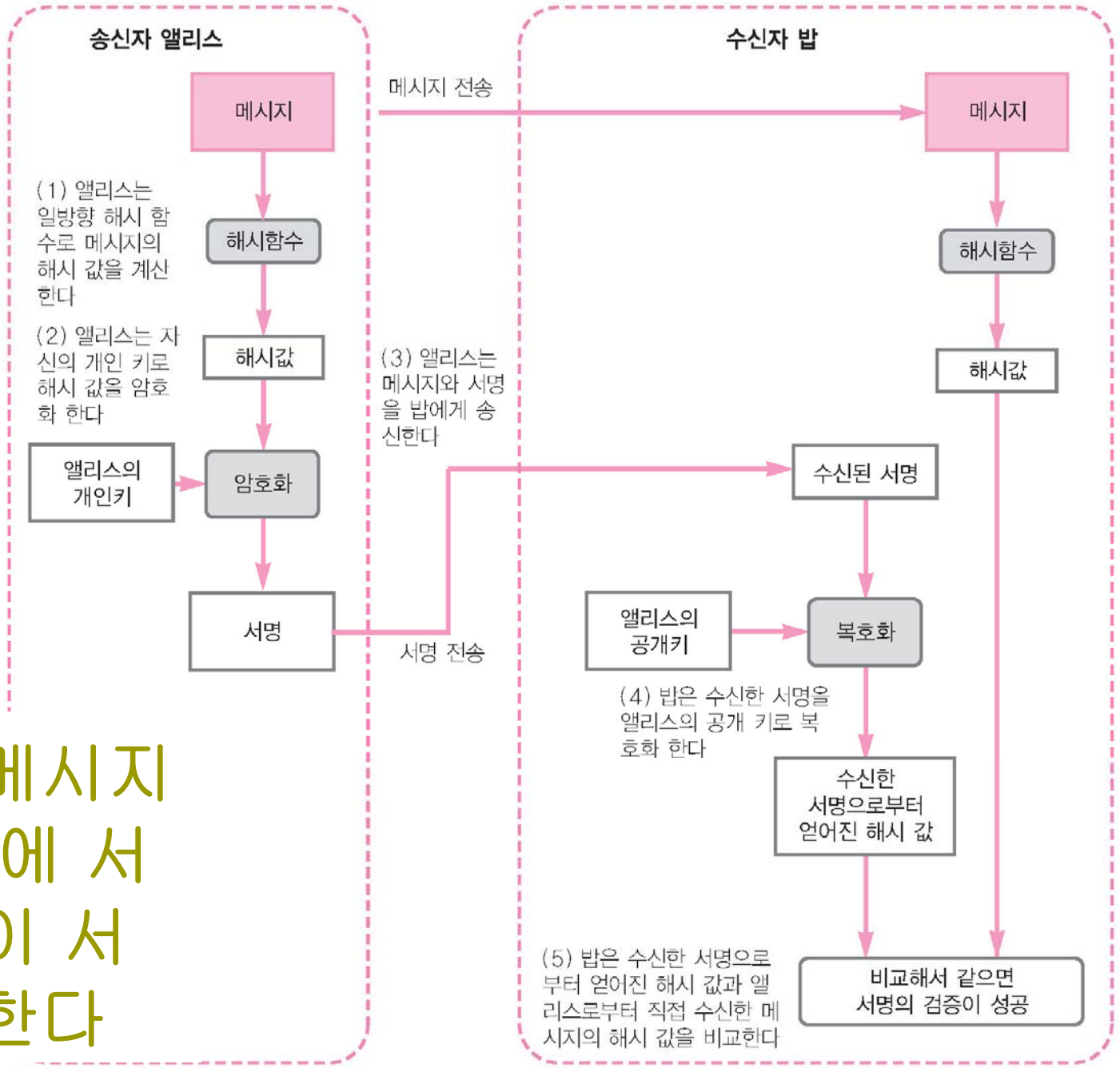

그림 9-6 앨리스가 메시지의 해시 값에 서명하고 밥이 서명을 검증한다

앨리스가 메시지의 해시 값에 서명하고 밥이 서명을 검증한다(시간적인 흐름)

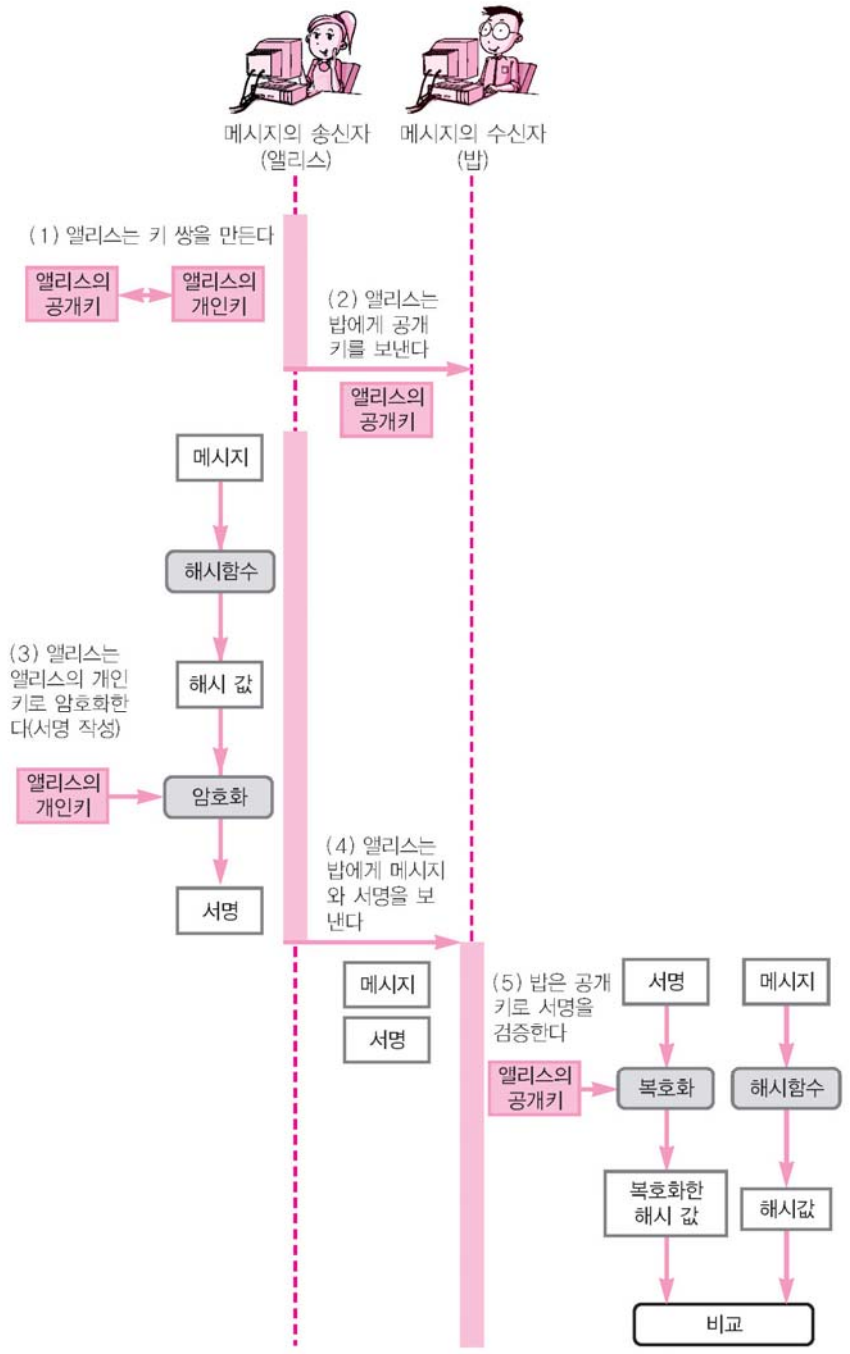

그림 9-7 앨리스가 메시지의 해시 값에 서명하고 밥이 서명을 검증한다(시간적인 흐름)

9.4 디지털 서명에 대한 의문

9.4.1 암호문의 서명사용

- 의문
  - 메시지를 개인 키로 암호화하는 것이 서명의 작성이 되고, 공개 키로 복호화해서 비교하는 것이 서명에 대한 검증이 된다는 흐름은 이해했다.
  - 그러나 암호문이 어떻게 서명으로서의 의미를 갖는 것일까?

- 답
  - 개인 키로 암호화한다는 것은, 행하고 있는 처리의 내용을 설명한 것임

  ➔기밀성을 실현하기 위해 암호화하고 있는 것은 아님

9.4.2 기밀성의 유지

- 의문
  - 그림 9-5와 그림 9-6을 보면 메시지가 암호화되지 않은 채 보내지고 있다.
  - 이래서는 메시지의 기밀성을 유지할 수 없는 것은 아닐까?

9.4.2 기밀성의 유지

- 답
  - 맞다.
  - 디지털 서명은 기밀성을 지키기 위한 것은 아니다.
  - 만약 기밀성이 필요하다면 메시지를 그대로 보내는 것이 아니고, 암호화를 별도로 행해서 보내야 된다.

9.4.3 복사된 서명

- 의문
  - 디지털 서명이라고 해도 단지 컴퓨터상의 데이터에 지나지 않으므로, 간단하게 복사본을 만들 수 있을 것 같은 느낌이 든다.
  - 만약 같은 내용의 복사본을 간단히 만들 수 있다면 서명이라고 말할 수 없지 않을까?

복사된 서명

- 답
  - 사실 서명이라고 해도 단지 컴퓨터상의 데이터에 지나지 않는다.
  - 메시지의 마지막에 이름이 첨부되어 있는 경우도 있고, 메시지와는 분리되어 서명이 별도의 파일로 되어 있는 경우도 있다.
  - 어느 경우라도 통상의 파일 복사처럼 같은 내용에 대한 복사를 몇 개라도 간단히 만들 수 있다.

복사된 서명

- 답
  - 서명은 그것이 원본이냐 사본이냐 하는 오리지널리티의 진위가 중요한 것이 아니고, **특정 서명자와 특정 메시지가 결부되어 있다**는 사실이 중요한 것이다.
  - 아무리 많이 복사를 해도 「그 메시지에 누가 서명했는가」하는 사실에는 조금도 변화가 없다. 복사는 할 수 있다. 그러나 그것에 의해 서명이 무의미해지는 것은 아니다.

9.4.4 서명 변경

- 의문
  - 디지털 서명이라고 해도 단지 데이터이므로 메시지와 서명 양쪽을 원하는 만큼 변경할 수 있을 것이다.
  - 그렇다면 서명이라고는 말할 수 없는 것이 아닐까?

9.4.4 서명 변경

- 답
  - 확실히 서명한 후에 메시지와 서명의 내용을 수정할 수는 있다.
  - 그러나 수정해 버리면 서명의 검증에 실패하기 때문에, 검증하는 사람은 수정이 되었다는 것을 검출할 수 있다.

  - 디지털 서명이 실현하고자 하는 것은
    - 변경하지 못하도록 막는 **방지**가 아니라
    - 문서에 변경 행위가 있었는지 아닌지를 **검출**하는 것

- 의문
  - 서명 대상의 메시지와 서명 양쪽을 수정해서 서명의 검증에 성공할 수 있도록 앞뒤를 잘 맞출 수 있지는 않을까?

- 답
  - 아니다. 그것은 사실상 불가능하다.
  - 해시 값에 서명하는 경우를 예로 들겠다.
  - 메시지를 1비트라도 수정하면 새로 계산한 해시 값은 변화한다.
  - 앞뒤를 맞추고자 하는 사람은 개인 키를 모르는 상태에서 그 새로운 해시 값을 암호화하지 않으면 안 되는데, 그것은 사실상 불가능하다.
  - 개인 키를 알지 못하면 개인 키를 사용한 암호문을 새롭게 만들 수는 없기 때문이다.

9.4.5 서명 부분의 재이용

- 의문
  - 구체적인 누군가의 디지털 서명을 손에 넣었다면 그 서명 부분만 잘라내서 다른 메시지에 첨부할 수 있다고 생각한다.
  - 그렇다면 서명이 되는 것이 아닐까?

9.4.5 서명 부분의 재이용

- 답
  - 확실히 서명 부분만을 잘라내서 다른 메시지에 첨부하는 것은 가능하다. 그러나 서명의 검증에는 실패한다.
  - 서명 부분을 잘라낸다는 행위는
    - 현실 세계의 종이로 된 계약서에서 서명을 베끼는 행위와 같은 공격
    - 그러나 디지털 서명의 경우에는 메시지와 서명 사이에는 수학적인 이론에 기초한 대응 관계가 있다.
  - **메시지가 다르면 서명도 다르기 때문에 서명만 잘라내서 재이용하는 것은 사실상 불가능하다.**

9.4.6 서명의 파기

- 의문
  - 종이로 된 차용서는 찢어서 버리면 파기할 수 있다.
  - 하지만 디지털 서명이 붙은 차용서는 단지 컴퓨터의 파일이므로 아무리 삭제해도 파기할 수 없다.
  - 삭제해도 어딘가에 복사본이 남아 있을지 모르기 때문이다. 파기할 수 없는 서명은 불편하지 않을까?

답

- 분명히 디지털 서명이 붙은 차용서는 삭제해도 파기할 수 없다.
- 디지털 서명이 붙은 차용서를 파기하는 경우에는 「영수증」에 상당하는 문서를 새로 만들고, 그것에 대해 상대에게 디지털 서명을 부탁하게 된다.
- 즉, 돈을 갚는 사람은 채권자로부터 차용금액을 받았다는 사실을 기록한 영수증을 작성하도록 하고 채권자로 하여금 서명을 하게 하여 그것을 보관하는 것이다.
- 이 행위는 차용서 자체를 없애는 것이 아니고 차용서의 본질적인 내용을 다른 행위(돈을 지불했다는 새로운 사실)로 무효화 시키는 것이다.

9.4.7 부인 방지

- 의문
  - 메시지 인증 코드로는 부인 방지를 할 수 없는데, 디지털 서명으로는 부인 방지를 할 수 있는 것은 왜인가?

- 답
  - 부인 방지는 「키를 가지고 있는 것은 누구인가?」라는 물음과 깊은 관계가 있다.
  - 메시지 인증 코드의 경우
    - MAC 값을 계산할 수 있는 키(공유 키)는 송신자와 수신자 양쪽이 가지고 있었다. 그러므로 송신자와 수신자의 어느 쪽이라도 MAC 값을 계산할 수 있었다.
    - 「그 MAC 값을 계산한 것은 내가 아니라 수신자 쪽이다」라고 주장하는 것이 가능했다.
  - 디지털 서명의 경우
    - 서명을 작성할 수 있는 키(개인 키)는 송신자만 가지고 있다. 서명을 작성할 수 있는 것은 송신자뿐

    ➔ 송신자는 「그 서명을 작성한 것은 내가 아니다」라고 주장할 수가 없다.

9.4.8 종이 서명의 대응

- 의문
  - 종이로 된 차용서에 도장이 찍혀져 있지 않으면 왠지 불안하다. 디지털 서명은 정말로 현실 세계의 서명이나 날인의 대용으로서 유효한 것일까?

- 답
  - 그 의문은 정당하다.
  - 디지털 서명 기술은 물리적으로 계약서를 이동시키지 않아도 계약할 수 있다는 점과 컴퓨터상의 임의의 데이터에 서명할 수 있다는 등의 장점이 있다.
  - 그러나 「실제로 서명의 대용이 되는 것인가?」라는 불안은 남는다.
  - 그 큰 이유는 계약을 하거나 뭔가를 인증하거나 하는 행위는 다분히 인간적이고 사회적인 행위이기 때문이다.

9.5 디지털 서명 활용 예

9.5.1 보안 공지

- 보안에 관련된 단체가 보안위협에 관한 경고문을 웹 사이트에서 공개
- 그 경고문은 정말로 그 단체가 쓴 것일까?
- 악의 있는 제삼자가 웹 페이지를 변경한 것이 아니라는 것은 어떻게 하면 확인할 수 있을까?
- 이과 같은 때에 디지털 서명이 사용

클리어서명(clearsign)

- 메시지는 암호화하지 않고 디지털 서명만 해서 공포할 필요도 있음

- 메시지를 암호화하지 않고 서명만 할 경우

  ➔ **클리어서명**(clearsign)

경고 메시지에 대한 디지털 서명 활용

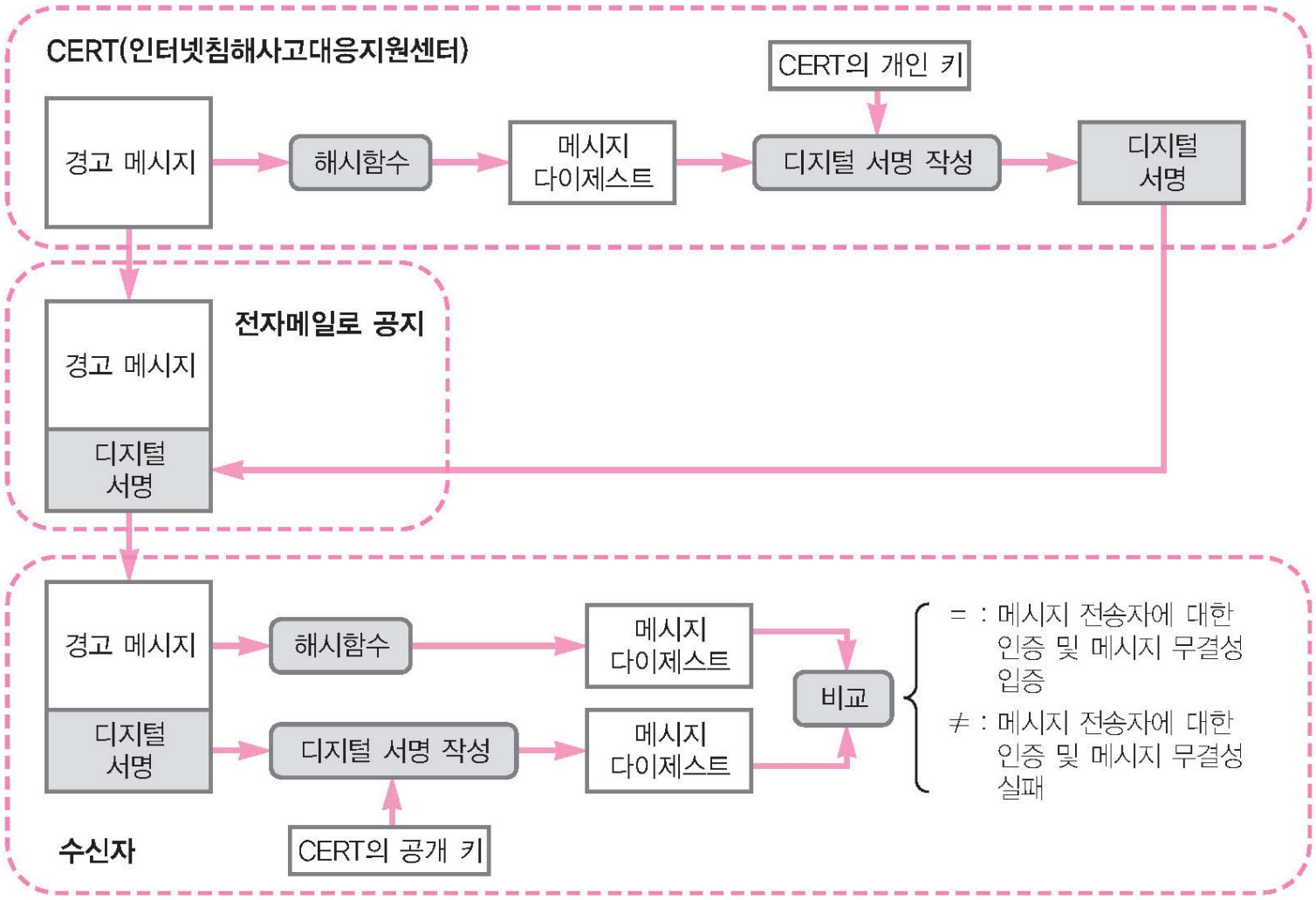

그림 9-8 경고 메시지에 대한 디지털 서명 활용

9.5.2 소프트웨어의 다운로드

- 이와 같은 경우에 소프트웨어의 작성자가 소프트웨어에 디지털 서명을 작성
- 사용자가 다운로드한 후, 서명을 검증하면
  - 적극적 공격자 맬로리에 의한 내용 변경을 검출하는 것이 가능

서명이 딸린 애플릿

- **서명이 딸린 애플릿**이라 불리는 소프트웨어

- 자바로 작성된 애플릿(Web 브라우저가 다운로드해서 실행하는 소프트웨어의 일종)에 작성자가 서명을 한 것
  - 사용자가 자신의 컴퓨터로 다운로드하면 사용자 컴퓨터의 Web 브라우저가 그 서명을 검증

9.5.3 공개 키 인증서

- 디지털 서명을 검증하려면 서명자의 개인 키와 쌍을 이루는 바른 공개 키가 필요

- 자신이 입수한 공개 키가 바른 공개 키인지 어떤지를 검증하기 위해서 공개 키를 메시지로 간주하고 그것에 제 3자가 디지털 서명을 하는 경우가 있음.
  - 제 3자는 메시지의 송신자와 수신자로부터 동시에 신뢰를 받고 있다는 가정

- **공개 키 인증서:** 공개 키에 디지털 서명을 붙인 것

9.5.4 SSL/TLS

- 서버와 클라이언트의 관계를 생각해보자.
  - 한 클라이언트가 서버에 접속요청을 한다고 했을 때 클라이언트 입장에서 자신이 접속하고자 하는 서버가 진짜 서버인지 아니면 위장된 서버인지를 확실히 알고 싶을 것이다.

- 이 경우에 SSL/TLS에서는 서버가 올바른 것이라는 것을 인증하기 위해서 서버 인증서를 이용
- 서버 인증서: 신뢰받는 제 3자가 서버의 공개키에 제 3자의 개인키로 서명을 한 것
- 서버의 입장을 생각해보면
  - 서버에 접속을 요청하는 클라이언트가 진정한 클라이언트인지를 검증하기 위해서 클라이언트에게 인증서를 요청

9.6 RSA에 의한 디지털 서명

- RSA에 의한 디지털 서명 알고리즘을 사용해서 실제로 서명을 해 보자.
- 서명의 작성과 검증에 대해서만 설명하기로 한다.
- 번잡함을 피하기 위해 일방향 해시 함수는 사용하지 않고 메시지에 직접 서명하기로 한다.

9.6.1 RSA에 의한 서명의 작성

- RSA에서는 서명 대상이 되는 메시지도 키도 작성된 서명도 모두 수로 표현
- 문장에 서명하고 싶을 경우에는 부호화를 행해서 문장을 수로 변환야 함
- RSA에 의한 서명 작성은 다음 식으로 표현할 수 있다(D와 N은 서명자의 개인 키).

$$\text{서명} = \text{메시지}^{D} \bmod N$$

9.6.2 RSA에 의한 서명의 검증

서명으로부터
얻어진 메시지 = 서명^{E} mod N

- E와 N은 서명자의 공개 키

RSA 서명의 작성과 서명의 검증

표 9-2 RSA 서명의 작성과 서명의 검증

키 쌍	**공개 키**	수 E와 수 N
	개인 키	수 D와 수 N
서명의 작성		서명 = 메시지^{D} mod N(메시지를 D 제곱해서 N으로 나눈 나머지)
서명의 검증		서명으로부터 얻어진 메시지 = 서명^{E} mod N(서명을 E제곱해서 N으로 나눈 나머지) 「서명으로부터 얻어진 메시지」와 「메시지」를 비교한다

9.6.3 자세한 RSA 서명

- 구체적인 수를 써서, RSA를 사용한 서명의 작성과 서명의 검증을 해 보자. 키 쌍으로는 RSA 공개키 암호에서 사용했던 다음의 수들을 이용한다.
  - 공개 키:
    E = 5
    N = 323
  - 개인 키:
    D = 29
    N = 323
- 여기서는 123이라는 메시지에 서명을 해 보자.

서명의 작성

- 메시지^{D} mod N = 123^{29} mod 323 = 157
- 서명은 157이 된다. 당신은 수신자에 대해서

(메시지, 서명) = (123, 157)

이라는 수의 짝을 송신한다.

서명의 검증

- 수신자는

  (메시지, 서명) = (123, 157)

  을 받았다.
- 공개 키(E, N) = (5, 323)을 사용해서 서명으로부터 얻어진 메시지를 계산한다.

  $서명^{E} \bmod N = 157^{5} \bmod 323 = 123$

9.7 다른 디지털 서명

- ElGamal 방식,
- DSA,
- Rabin 방식

에 대해서만 간단히 소개

9.7.1 ElGamal 방식

- ElGamal 방식
  - Taher ElGamal에 의한 공개 키 알고리즘
  - mod N으로 이산대수를 구하는 것이 곤란하다는 것을 이용
    ➔ 이산대수 문제가 효과적으로 풀린다면 ElGamal 방식도 깨진다는 것을 의미

- ElGamal 방법의 안전성은
  - 실제로 소위 말하는 결정적 Diffie-Hellman(Decisional Diffie-Hellman: DDH) 가정에 있음
  - 이 가정은 이산대수 문제보다도 더 강력함

- ElGamal 방식은 공개 키 암호와 디지털 서명에 이용할 수 있고, 암호 소프트웨어 GnuPG에서도 알고리즘의 하나로 사용하고 있음

9.7.2 DSA

- DSA(Digital Signature Algorithm)
  - 디지털 서명 알고리즘의 일종
  - NIST(National Institute of Standards and Technology)가 1991년에 제정한 디지털 서명 규격(DSS)용으로 만들어진 것
- DSA는 Schnorr의 알고리즘과 ElGamal 방식의 변종으로 디지털 서명에만 이용할 수 있음

9.7.3 Rabin 방식

- M. O. Rabin에 의한 공개 키 알고리즘
- mod N으로 제곱근을 구하는 것이 곤란하다는 것을 이용
- 공개 키 암호와 디지털 서명에 이용할 수 있음

9.8 디지털 서명에 대한 공격

9.8.1 중간자(man-in-the-middle) 공격

- 공개 키 암호에 대한 **중간자 공격**은 디지털 서명에도 위협이 되는 공격임

- 디지털 서명의 중간자 공격은 적극적 공격자 맬로리가 송신자와 수신자의 사이에 들어가 송신자에 대해서는 수신자처럼, 수신자에 대해서는 송신자처럼 거짓 행세를 하는 공격

- 이것은 디지털 서명의 알고리즘 자체를 깨지 않아도 가능하다.

방어 방법

- 앨리스와 밥이 각각 일방향 해시 함수로 해시 값을 계산해서 그 해시 값을 전화로 서로 확인하는 것이 좋은 방법

- 공개 키를 취급하는 소프트웨어는 공개 키의 해시 값을 표시하는 수단을 준비해 놓고 있음

  ➔ 이 해시 값을 **핑거프린트(fingerprint)**라 부름

9.8.2 일방향 해시 함수에 대한 공격

- 디지털 서명에서 사용하는 일방향 해시 함수는 충돌내성을 갖아야 함

- 만약 충돌내성을 없으면 디지털 서명을 한 해시 값과 같은 해시 값을 갖는, 다른 메시지를 만들 수 있게 됨

9.8.3 디지털 서명을 사용한 공개 키 암호 공격

- 「서명을 해 주세요」라는 의뢰는 「복호화를 해 주세요」라는 의뢰라고 생각할 수 있음
- 이것을 이용하면 「디지털 서명을 사용해서 암호문을 해독한다」는 교묘한 공격이 가능
- 이런 공격에 대한 대책은 **의미를 모르는 메시지에는 절대로 디지털 서명을 하지 않는** 것이다.
  - 특히 랜덤하게 보이는 메시지에는 디지털 서명을 해서는 안됨

9.8.4 기타 공격

- 공개 키 암호에 대한 공격의 대부분은 디지털 서명에 대한 공격으로서도 사용할 수 있음

- 예)
  - 개인 키를 전사공격으로 찾거나
  - RSA의 N을 소인수분해하려고 시도하거나 하는 것 등

9.9 기타 기술과의 비교

9.9.1 메시지 인증 코드와 디지털 서명

대칭 암호와 공개 키 암호의 비교 및 메시지 인증 코드와 디지털 서명의 비교

표 9-3 대칭 암호와 공개 키 암호의 비교 및 메시지 인증 코드와 디지털 서명의 비교

	대칭 암호	공개 키 암호
송신자	공유 키로 암호화	공개 키로 암호화
수신자	공유 키로 복호화	개인 키로 복호화
키 배송 문제	일어난다	일어나지만, 공개 키의 인증이 별도로 필요
기밀성	○	○

	메시지 인증 코드	디지털 서명
송신자	공유 키로 MAC 값을 계산	개인 키로 서명을 작성
수신자	공유 키로 MAC 값을 계산	공개 키로 서명을 검증
키 배송 문제	일어난다	일어나지만, 공개 키의 인증이 별도로 필요
무결성	○	○
인증	○(통신 상대에 대해서만)	○(제 3자에 대해서도)
부인 방지	×	○

9.9.2 하이브리드 암호 시스템과 해시 값에 대한 디지털 서명

- 하이브리드 암호 시스템
  - 메시지 전체를 대칭 암호로 암호화
  - 대칭 암호 키만을 공개 키 암호로 암호화
  - 대칭 암호 키를 메시지로 간주하고 이것을 공개 키로 암호화한 것
- 디지털 서명에서도 똑같은 기법을 이용
  - 메시지 전체를 일방향 해시 함수에 입력해서 해시 값을 구함
  - 해시 값에 대해 서명한
  - 해시 값을 메시지로 간주하고 이것을 개인 키로 암호화

- 정리하면,
  - 대칭 암호의 키는 **기밀성의 엣센스**이고,
  - 일방향 해시 함수의 **해시 값은 무결성의 엣센스**라고 할 수 음

9.10 디지털 서명으로 해결할 수 없는 문제

- 디지털 서명으로 메시지 내용 변경이나 거짓 행세를 검출하여 부인을 방지한다.
- 변경되 않은 공개 키를 「거짓 행세」하고 있지 않은 송신자로부터 받을 필요가 있다.

기술적인 방법만으로는 해결되지 않는 문제

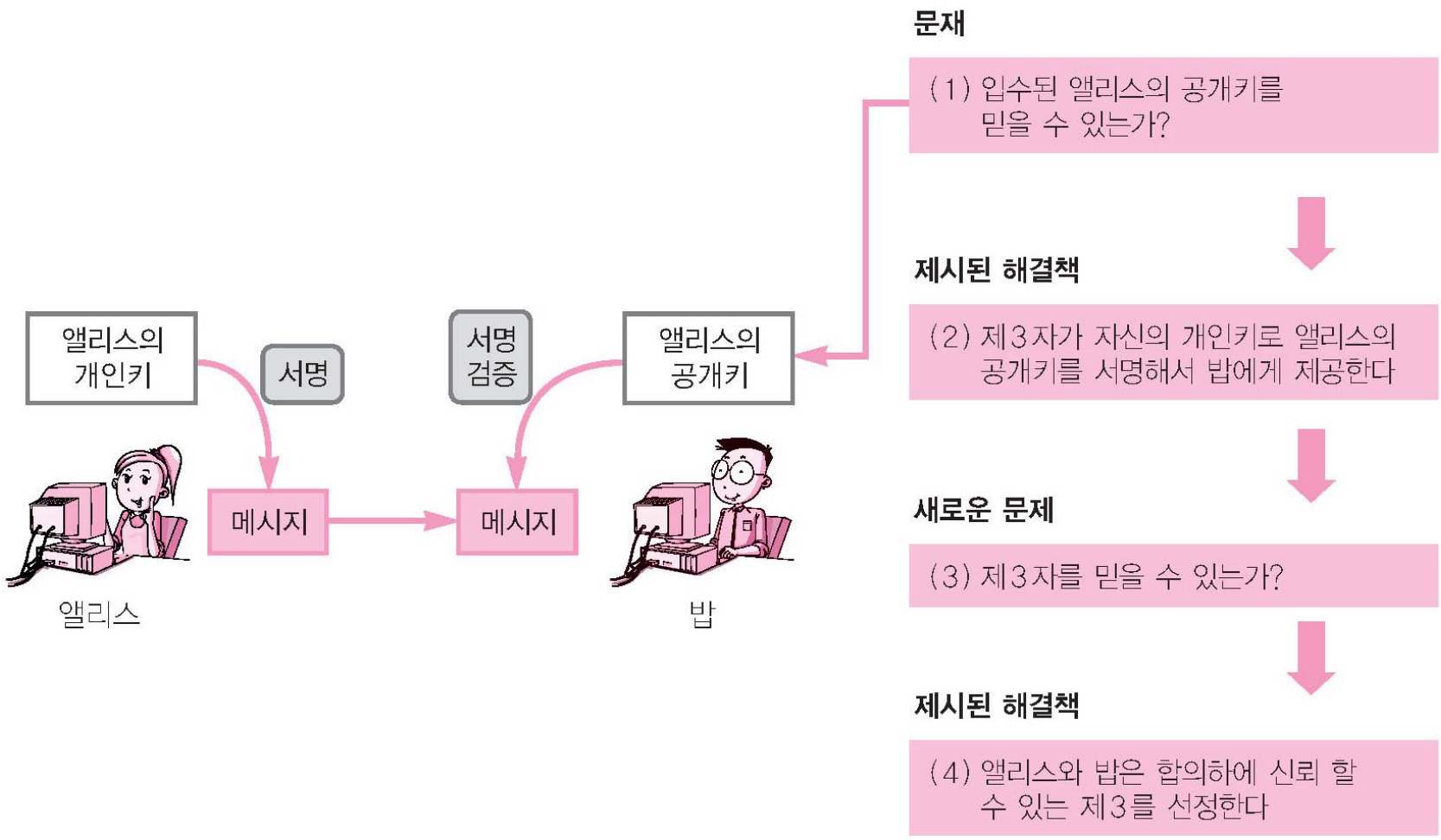

그림 9-9 기술적인 방법만으로는 해결되지 않는 문제

- 바른 공개 키를 입수하기 위해 고안된 것이 **인증서**임

- 인증서
  - 공개 키를 메시지로 간주하고, 신뢰할 수 있는 다른 사람이 자신의 개인 키로 디지털 서명을 한 공개 키

- 인증서에 포함된 공개 키를 제 3자의 개인 키로 암호화한 디지털 서명을 검증하기 위해서는
  - 제 3자의 바른 공개 키가 필요해지기 때문

- 어떻게 하면 신뢰할 수 있는 디지털 서명 연쇄를 구축할 수 있을까?
- 원래 누가 신뢰할 수 있는 인증서를 발행하는 것일까?

- 공개 키 암호 및 디지털 서명의 기술을 사회적인 기반(기반구조)으로 만들어 가는 것

➔ **공개 키 기반**(Public Key Infrastructure): **PKI**

질의 및 응답

– 끝–