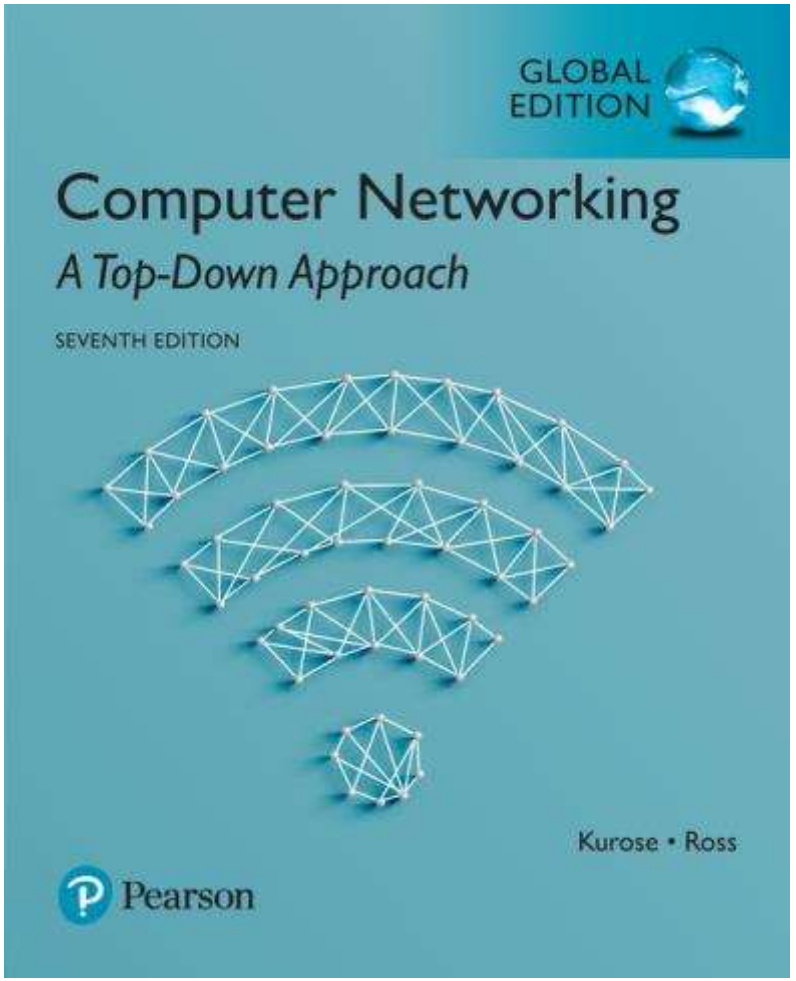
제29강
해시 함수, MAC, 디지털 서명

Computer Networking: A Top Down Approach

컴퓨터 네트워크
(2019년 1학기)

박승철교수

한국기술교육대학교
컴퓨터공학부



Pre-study Test :

1) 다음 중 해시 함수에 대한 설명 중 틀린 것은?
① 일반적으로 512비트 이하의 짧은 해시값을 생성한다.
② 문서의 무결성 확인에 주로 사용한다.
③ 일방향성을 보장한다.
④ 문서의 기밀성 확인에 주로 사용한다.

2) 다음 중 해시 함수의 일방향성(One-way Hash Function)을 설명한 것은?
① 주어진 해시값 h에 대해 H(x) = h인 메시지 x를 찾는 것은 계산상 불가능하다.
② H(x) ≠ H(y)인 서로 다른 메시지 쌍 (x, y)를 찾는 것은 계산상 불가능하다.
③ H(x) = H(y)인 서로 다른 메시지 쌍 (x, y)를 찾는 것은 계산상 불가능하다.
④ 주어진 메시지 x에 대해 H(x) = H(y)인 다른 메시지 y(x ≠ y)를 찾는 것은 계산상 불가능하다.

3) 다음 중 가장 안전한 해시 함수는?
① MD4
② SHA-1
③ SHA-256
④ MD5

4) 다음 중 메시지 인증 코드(Message Authentication Code)에 대한 설명 중 틀린 것은?
① 메시지 무결성을 보장한다.
② 메시지 인증성을 보장한다.
③ 메시지 기밀성을 보장한다.
④ IP 스푸핑 공격을 방어한다.

5) 다음 중 디지털 서명(Digital Signature)에 대한 설명 중 틀린 것은?
① 개인키(Private Key)가 서명 생성키가 된다.
② 공개키(Public Key)가 서명 검증키가 된다.
③ 공인인증서가 필요하다.
④ 공개키로 문서의 해시값을 암호화한다.

6) 다음 중 디지털 서명(Digital Signature)이 보장하는 보안 요소가 아닌 것은?
① 기밀성
② 무결성
③ 인증성
④ 책임성

7) 다음 중 X.509 공인인증서에 포함되는 내용이 아닌 것은?
① 공개키(Public Key)
② 인증기관 정보
③ 사용 주체 정보
④ 사용 주체 서명

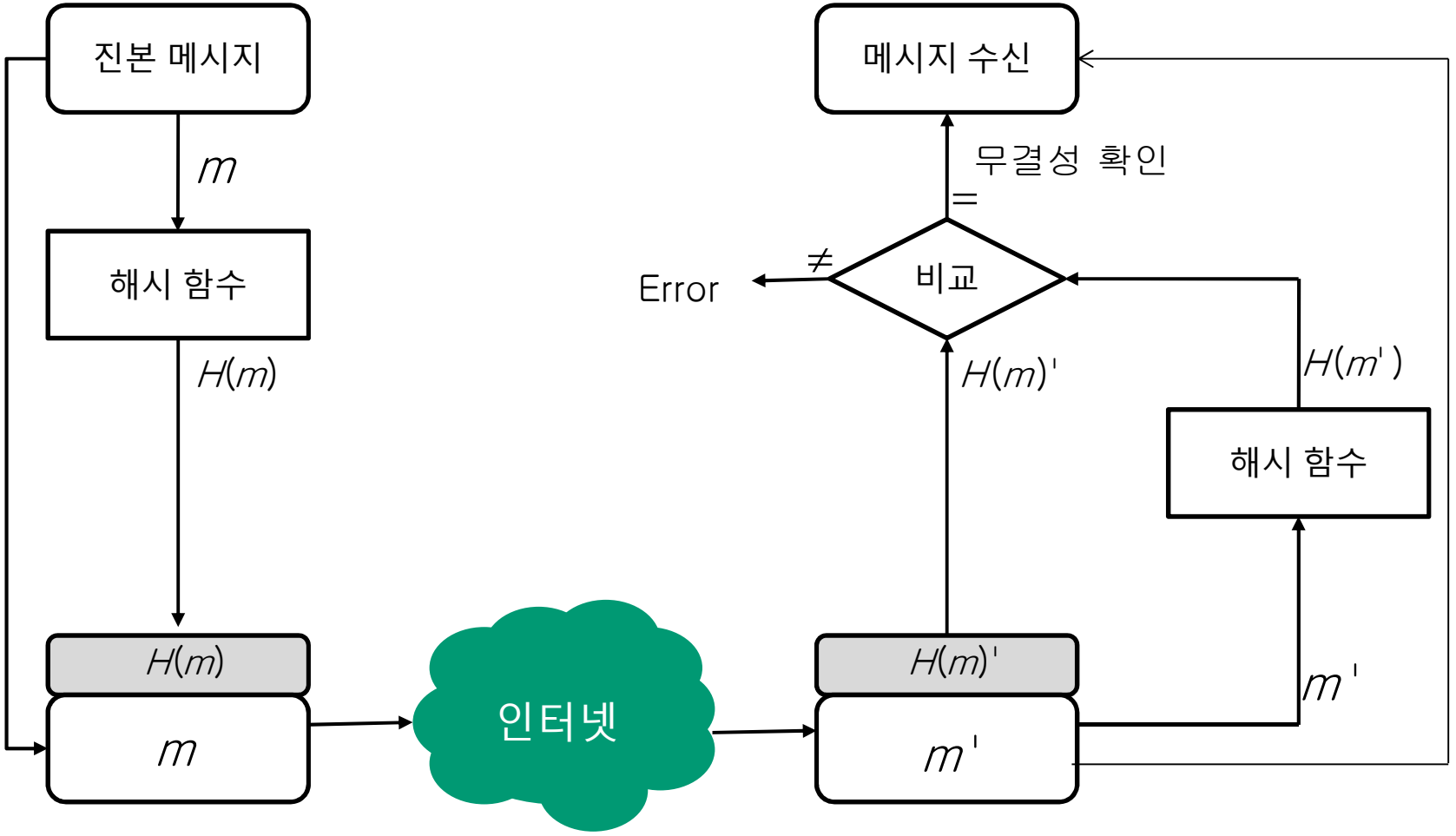
7) 암호에 사용된 키를 알아내기 위해 모든 경우의 수를 시도하는 공격을 무엇이라 하는가?

① 추측 공격(guessing attack)
② 사전 공격(dictionary attack)
③ 도청 공격(eavesdrop attack)
④ 전사 공격(brute force attack)

해시 함수와 메시지 무결성

- 해시 함수(Hash Function) :
  - 메시지에 대해 길이가 짧고 일정하며, 고유한 메시지 지문(해시값, 메시지 다이제스트) 생성
  - 메시지 지문의 길이는 해시 함수에 따라 128 ~ 512 비트
- 메시지 무결성(Message Integrity)
  - 메시지가 의도적으로 또는 비의도적으로 변경되지 않은 원본이 맞음을 나타내는 성질
  - 메시지 원본 대신 해시값을 사용하여 간단하게 무결성 확인

해시 함수와 메시지 무결성



해시 함의 성질

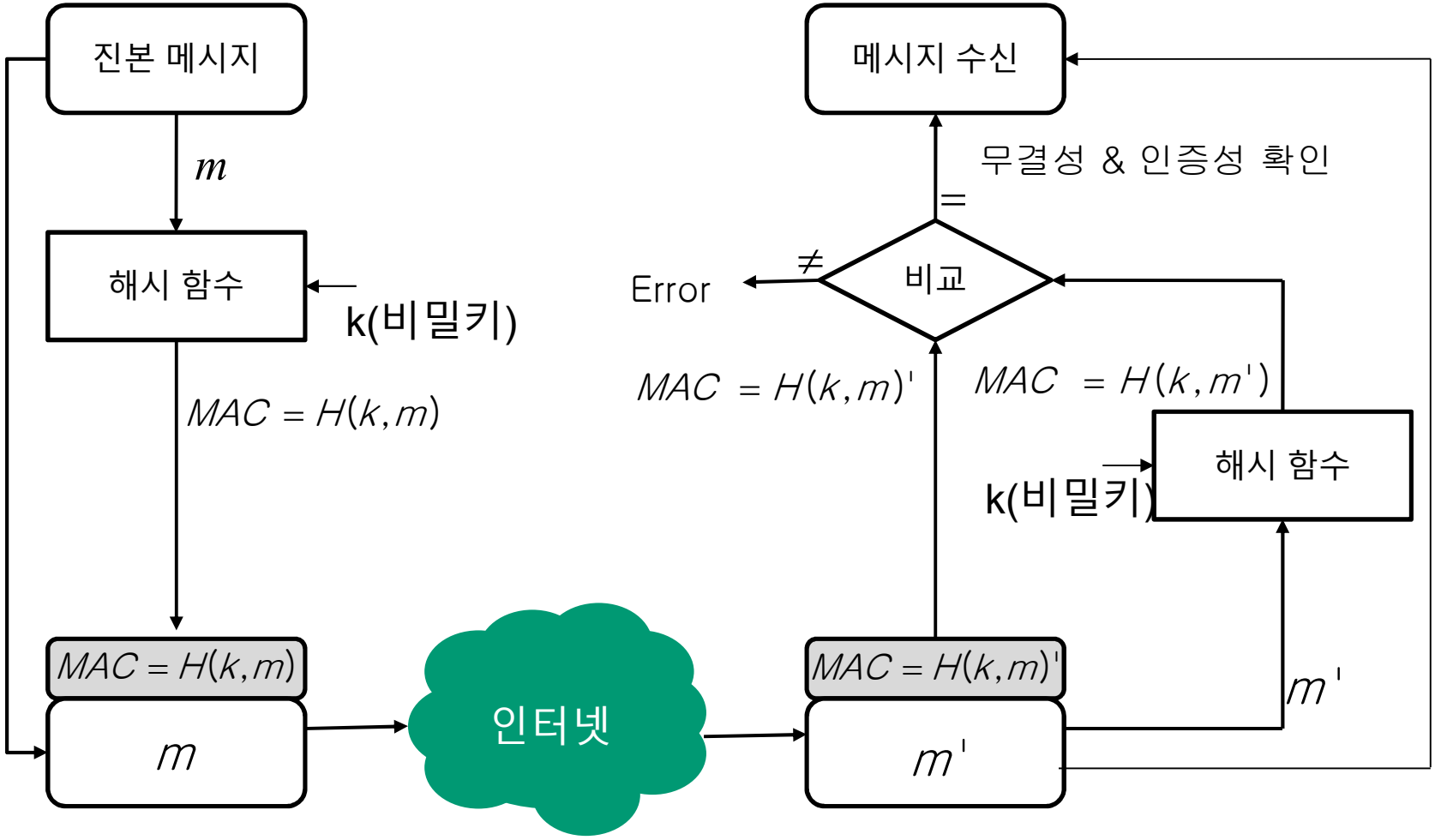
1. 주어진 해시값 h에 대해 h(H(x)=h)를 생성한 원래 메시지 x를 찾는 것은 계산상 불가능하다
   (일방향성=역상 저항성)

2. 약한 충돌 저항성, 제2 역상 저항성, 제2 프리이미지 내성
3. 강한 충돌 저항성

Message Authentication Code

- 메시지 인증 코드(MAC) :
  - 메시지와 송신자와 수신자가 공유하고 있는 키(key)를 입력으로 고정 길이의 짧은 코드(MAC)를 생성하는 함수.
  - 비밀키를 알 수 없는 제3의 공격자는 생성 불가 보장

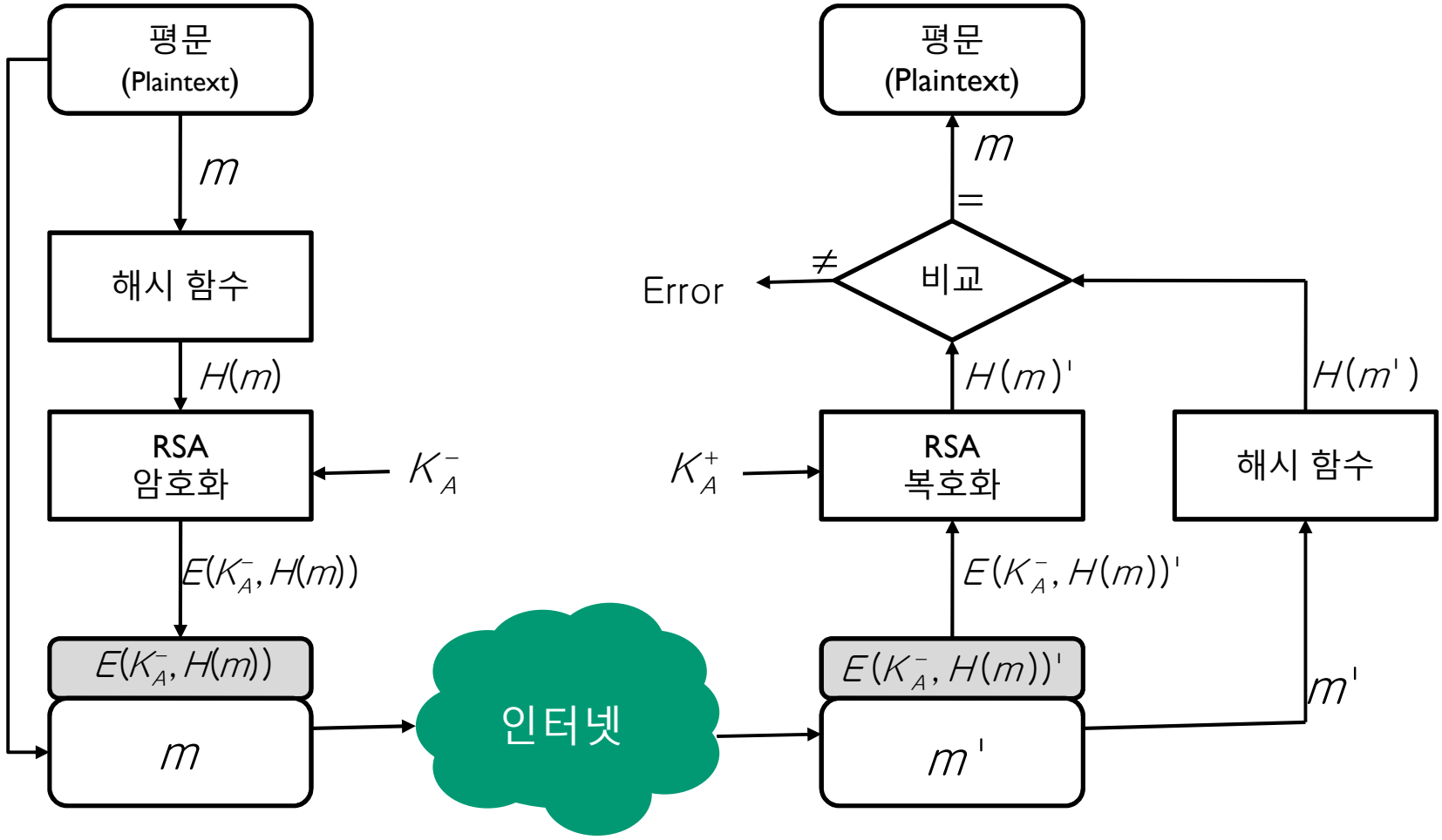
Message Authentication Code



Message Authentication Code

- 제3자에 대한 메시지 송신자 증명 불가
  - 비밀키를 공유하는 사용자 간에 메시지 송신자 인증 가능
  - 비밀키를 공유하지 않는 제3자에 대해 송신자를 증명하는 것은 불가능
- 부인 방지(non-repudiation) 불가
  - 비밀키를 공유하는 사용자 A가 사용자 B에게 메시지와 MAC을 송신한 후 메시지 전송 사실 부인
  - 사용자 B가 제3자에게 사용가 A가 송신한 메시지임을 증명 불가(사용자 B의 자작극 의심 가능)

Digital Signature



Public-key certification

필드	설명
버전(Version)	X.509의 버전
일련 번호(Serial Number)	발급 기관에 의해 인증서에 부여되는 유일한 순서 번호
디지털 서명 알고리즘 ID	인증서 서명 작성에 사용된 알고리즘 식별자
발급 기관(issuer) 이름	인증서 발급 기관의 이름
유효 기간	인정서가 유효한 기간
주체(subject) 이름	공개키의 소유자 이름
주체의 공개키	주체에 대한 공개키
확장 정보(extensions)	응용에 필요한 추가적인 정보
서명(signature)	발급 기관의 디지털 서명

After-study Test :

1) 다음 중 해시 함수에 대한 설명 중 틀린 것은?
① 일반적으로 512비트 이하의 짧은 해시값을 생성한다.
② 문서의 무결성 확인에 주로 사용한다.
③ 일방향성을 보장한다.
④ 문서의 기밀성 확인에 주로 사용한다.

2) 다음 중 해시 함수의 일방향성(One-way Hash Function)을 설명한 것은?
① 주어진 해시값 h에 대해 H(x) = h인 메시지 x를 찾는 것은 계산상 불가능하다.
② H(x) ≠ H(y)인 서로 다른 메시지 쌍 (x, y)를 찾는 것은 계산상 불가능하다.
③ H(x) = H(y)인 서로 다른 메시지 쌍 (x, y)를 찾는 것은 계산상 불가능하다.
④ 주어진 메시지 x에 대해 H(x) = H(y)인 다른 메시지 y(x ≠ y)를 찾는 것은 계산상 불가능하다.

3) 다음 중 가장 안전한 해시 함수는?
① MD4
② SHA-1
③ SHA-256
④ MD5

4) 다음 중 메시지 인증 코드(Message Authentication Code)에 대한 설명 중 틀린 것은?
① 메시지 무결성을 보장한다.
② 메시지 인증성을 보장한다.
③ 메시지 기밀성을 보장한다.
④ IP 스푸핑 공격을 방어한다.

5) 다음 중 디지털 서명(Digital Signature)에 대한 설명 중 틀린 것은?
① 개인키(Private Key)가 서명 생성키가 된다.
② 공개키(Public Key)가 서명 검증키가 된다.
③ 공인인증서가 필요하다.
④ 공개키로 문서의 해시값을 암호화한다.

6) 다음 중 디지털 서명(Digital Signature)이 보장하는 보안 요소가 아닌 것은?
① 기밀성
② 무결성
③ 인증성
④ 책임성

7) 다음 중 X.509 공인인증서에 포함되는 내용이 아닌 것은?
① 공개키(Public Key)
② 인증기관 정보
③ 사용 주체 정보
④ 사용 주체 서명