전자서명

목차

- 전자서명 개요
- 학문적 RSA 전자서명
- 큰 메시지 전자서명과 해쉬함수
- 전자서명: 서명과 검증
- 공개키 인증서

전자서명 개요

Reference: (Paar & Pelzl, 2010)

- 전자서명
  - 특정 객체가 메시지를 생성했음에 대한 전자적 증명 방법
  - 대칭키 암호 기술은 부인불가(non-repudiation) 기능 제공 불가
  - 공개키 암호 기술이 사용됨
  - 전자서명은 메시지 무결성, 메시지 인증, 부인불가를 제공함
- 학문적 RSA 전자서명
  - 서명자는 자신의 개인키 (d, n)으로 메시지 m을 암호화하여 서명 s 생성
    - $s \equiv m^d \ mod \ n$
    - 서명자는 서명 s를 메시지 m에 부착하여 전송
  - 검증자는 서명자의 공개키 (e, n)으로 서명 s를 복호화 후 메시지 m′ 생성
    - m과 m′이 같다면 서명자가 해당 메시지를 서명했음을 확인
    - $s^e \equiv \left(m^d\right)^e \equiv m^{de} \equiv m \ \ (mod \ n)$
  - 문제점
    - 큰 메시지 서명을 어떻게 할 것인가?
      - 예) RSA-1024에서 1024비트(128바이트)보다 큰 메시지 서명은 어떻게 하는가?

학문적 RSA 전자서명 예

Reference: (Paar & Pelzl, 2010)

Alice

- Alice가 Bob의 서명된 메시지를 검증하려 함
- Bob의 공개키 $(3, 33)$으로 서명 $s = 16$을 복호화

$$m' \equiv s^e \equiv 16^3 \equiv 4 \ (mod\ 33)$$

- $m' = m = 4$이므로 유효한 서명임을 확인

$(e, n) = (3,33)$ ←----------

$(m, s) = (4,16)$ ←----------

Bob

- 두 소수 $p = 3,\ q = 11$ 선택
- $n = p \times q = 3 \times 11 = 33$ 계산
- $\phi(n) = (p - 1) \times (q - 1) = 20$ 계산
- 다음 조건을 만족하는 $e = 3,\ d = 7$ 선택

$$\gcd(\phi(n), e) = 1, \qquad 1 < e < \phi(n)$$
$$ed\ mod\ \phi(n) = 1$$

- 공개키 $(e, n) = (3,33)$ → 공개
- 개인키 $(d, n) = (7,33)$ → 안전하게 보관
- 평문 $m = 4$에 대한 서명 s 계산

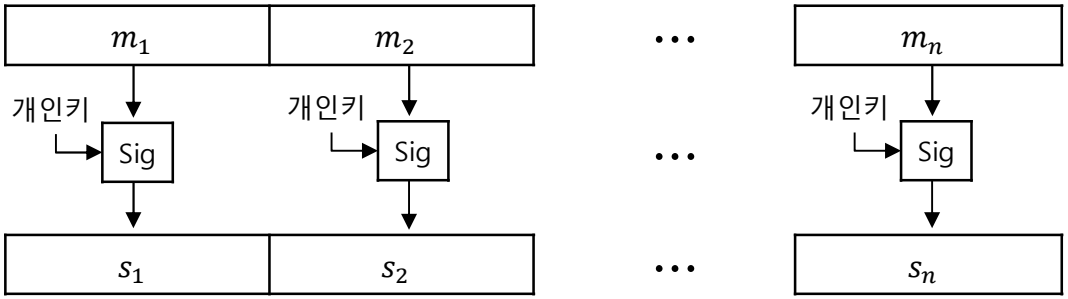
$$s = m^d\ mod\ n = \ 4^7\ mod\ 33 = 16$$

- 평문과 서명을 전송
- 개인키 $(d, n) = (7,33)$으로 암호문 복호화
- Alice가 보낸 평문 4 수신

큰 메시지 전자서명과 해쉬함수

Reference: (Paar & Pelzl, 2010)

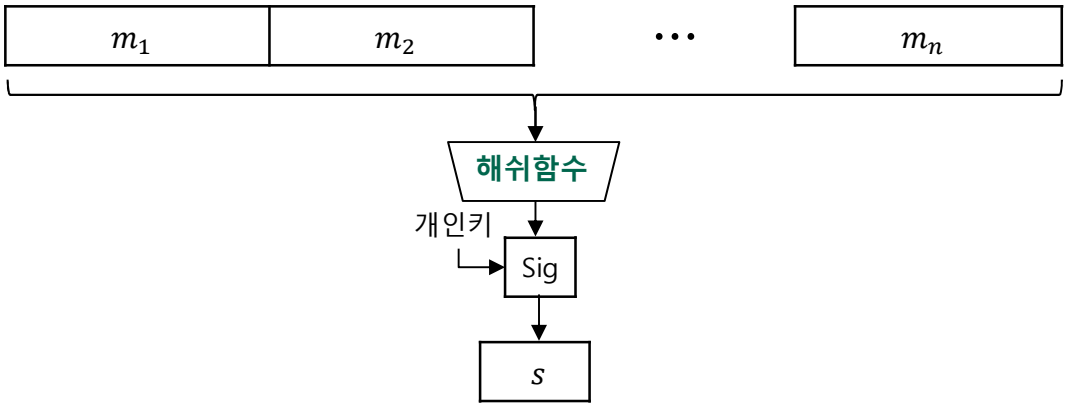
전자서명 방법 1



전자서명 방법 1

- 서명 모듈의 입력 크기로 큰 메시지를 분할하여 각 메시지 블록에 대해 서명 생성
- 많은 계산량

전자서명 방법 2

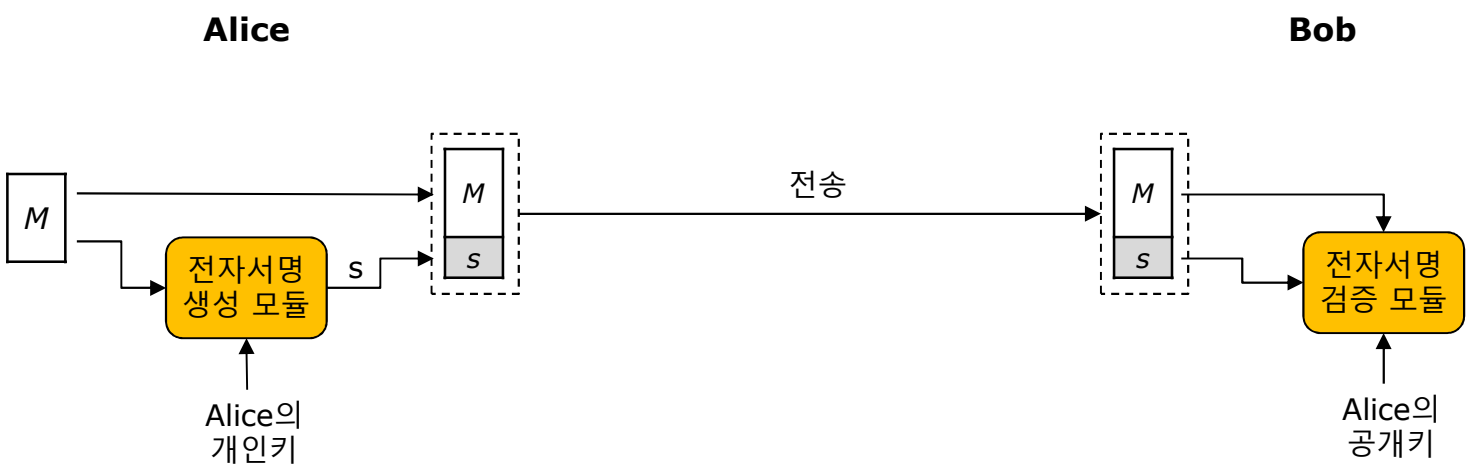


전자서명 방법 2

- Bob은 자신의 개인키 K_{pr}와 해쉬 함수 H를 이용하여 큰 메시지 m에 대한 메시지 다이제스트 $h = H(m)$ 생성 후 메시지 다이제스트에 대해 서명 s 생성
- $s = Sig_{K_{pr}}(h)$
- Alice는 (m, s) 수신
- Alice는 수신한 메시지 m의 해쉬값 h'을 계산하고, Bob의 공개키 K_{pub}를 이용하여 s로부터 h를 복호화한 후, h와 h'이 일치하는 검증

전자 서명: 서명과 검증

Reference: (Stallings, 2014)

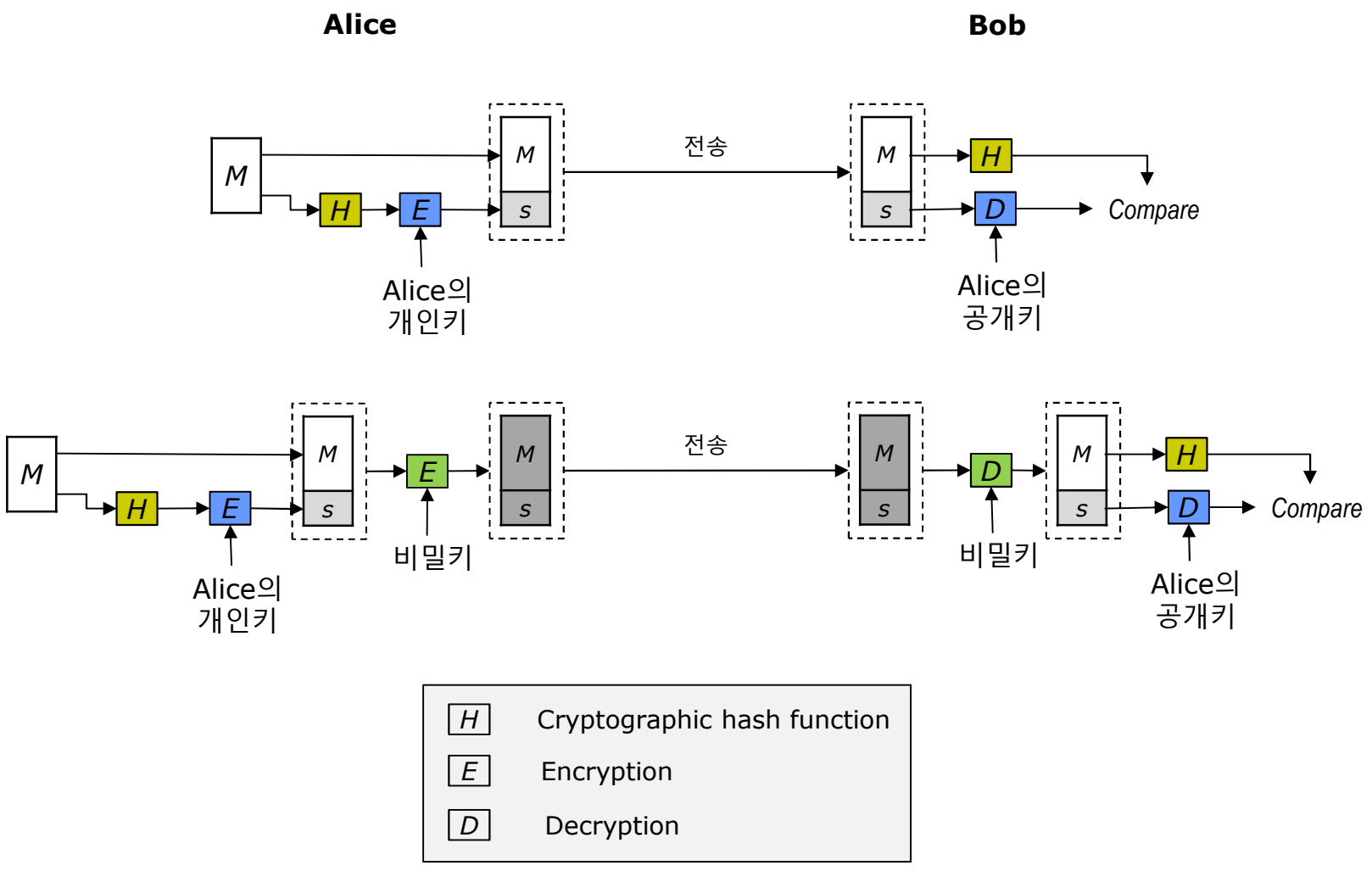


전자서명(Digital signature)

- Alice는 Bob에게 전송할 메시지 M에 대해 자신의 개인키를 이용하여 전자서명 s를 생성한 후 메시지와 함께 송신
- Bob은 수신한 메시지와 전자서명이 Alice가 작성한 것이 맞는지 Alice의 공개키를 이용하여 검증

전자 서명: 서명과 검증

Reference: (Stallings, 2014)



공개키 인증서

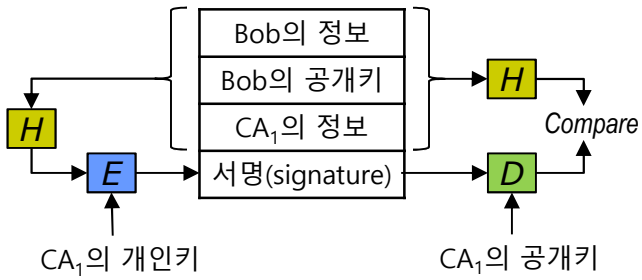
Reference: (Stallings, 2014)

- 공개키 인증서 → Public-key Certificate
- 인증기관 → Certification Authority, CA
- 중간 인증기관 → Intermediate CA
- 루트 인증기관 → Root CA

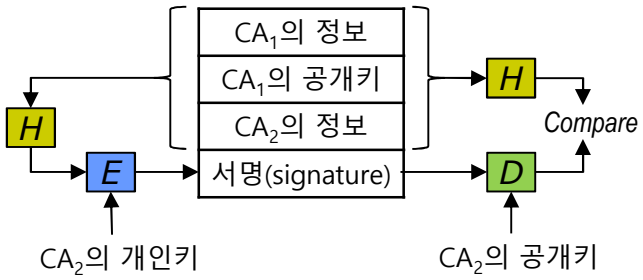
- 암호기술
  - 대칭키 암호 기술
    - 송수신 양측이 대칭키를 확보하고 있다고 가정
      - 대칭키는 비대칭키 암호 기술을 통해 획득 가능
        - Alice가 생성한 대칭키를 Bob의 공개키로 암호화하여 Bob에게 안전하게 전송
          - 이 경우 Alice는 Bob의 공개키를 신뢰한다는 전제 필요
  - 비대칭키 암호 기술
    - Alice는 Bob의 공개키를 어떻게 신뢰할 수 있는가?
      - Bob은 자신의 공개키가 신뢰할 수 있는 인증기관(CA_1)으로부터 인증 받았다는 인증서를 제시할 필요 있음
        - CA_1은, CA_1의 개인키로 Bob의 공개키를 서명하여 **Bob의 공개키 인증서**를 발급
        - Alice는 **Bob의 공개키 인증서**를 CA_1의 공개키로 검증 후 Bob의 공개키 신뢰
          - Alice가 CA_1의 공개키로 검증한다는 것은 CA_1의 공개키를 신뢰한다는 전제가 있어야 함
    - Alice는 CA_1의 공개키를 어떻게 신뢰할 수 있는가?
      - CA_1은 자신의 공개키가 신뢰할 수 있는 인증기관(CA_2)로부터 인증 받았다는 인증서를 제시할 필요 있음
        - CA_2는, CA_2의 개인키로 CA_1의 공개키를 서명하여 **CA_1의 공개키 인증서**를 발급
        - Alice는 **CA_1의 공개키 인증서**를 CA_2의 공개키로 검증 후 CA_1의 공개키를 신뢰
          - Alice가 CA_2의 공개키로 검증한다는 것은 CA_2의 공개키를 신뢰한다는 전제가 있어야 함
    - Alice는 CA_2의 공개키를 어떻게 신뢰할 수 있는가?
      - 이 신뢰의 고리를 어떻게 끊을 것인가?
      - CA_2는 자신의 공개키가 자신(CA_2)으로부터 인증 받았다는 인증서를 제시함 (self-signature)

공개키 인증서 포맷은 **X.509** 표준으로 명시됨

Bob의 공개키 인증서



CA_1의 공개키 인증서



References

- Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill, 2008
- William Stallings, Cryptography and Network Security: Principles and Practice, Sixth Edition, Prentice Hall, 2014
- Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010
- 김명환, 수리암호학개론, 2019
- 정민석, 암호수학, 경문사, 2017
- 최은미, 정수와 암호론, 북스힐, 2019
- 이민섭, 정수론과 암호론, 교우사, 2008