Chap 8-1 참고자료
메시지 인증

박 종 혁

(jhpark1@snut.ac.kr)

❑ 목 차

인증에서의 요구 조건 (1/2)

❑ 인증에서의 요구 조건

- ❖ 1. 노출(Disclosure)
  - ➢ 정확한 암호키를 소유하지 않은 사람 **or** 프로세스에게 메시지의 내용이 노출되는 것을 말함.
- ❖ 2. 트래픽 분석(Traffic analysis)
  - ➢ 통신자들 사이에 트래픽 패턴을 알아내는 것.
  - ➢ 연결형 응용에서, 연결 주기와 사용 시간이 파악됨.
  - ➢ 연결형이든 비 연결형 환경이든 간에 사용자들 간의 메시지 개수 및 길이 등은 확인될 수 있음.
- ❖ 3. 위장(masquerade)
  - ➢ 부정한 소스로부터 나온 메시지를 네트워크 상에 삽입하는 것.
  - ➢ 이것은 인증된 실체로부터 온 것인 양, 적이 생성한 메시지를 포함.
  - ➢ 메시지 수신자가 아닌 다른 사람에 의한 메시지의 수신 및 비수신에 대한 거짓된 승인도 포함.
- ❖ 4. 내용 수정(Content Modification)
  - ➢ 삽입, 삭제, 전치 및 수정을 포함한 메시지 내용의 변경을 의미.

인증에서의 요구 조건 (2/2)

❑ 인증에서의 요구 조건

❖ 5. 순서 수정(Sequence Modification)

- ➢ 삽입, 삭제 및 전치를 통한 통신 쌍방간의 메시지 순서의 변경을 말함.

❖ 6. 시간 수정(timing modification)

- ➢ 메시지의 지연과 재전송.
- ➢ 연결형 응용에서는, 메시지들의 전체 세션이나 순서는 이전의 어떤 유효한 세션의 재전송일 수 있고, 또는 그 순서에서의 각각의 메시지들이 지연되거나 재 전송될 수도 있음.
- ➢ 비연결형 응용에서는, 각각의 메시지**(**예**: datagram)**들이 지연되거나 재 전송될 수 있음.

❖ 7. 발신처 부인(source repudiation): 발신자가 메시지의 전송 사실을 부인함.

❖ 8. 수신처 부인(destination repudiation): 수신자가 메시지의 수신 사실을 부인함.

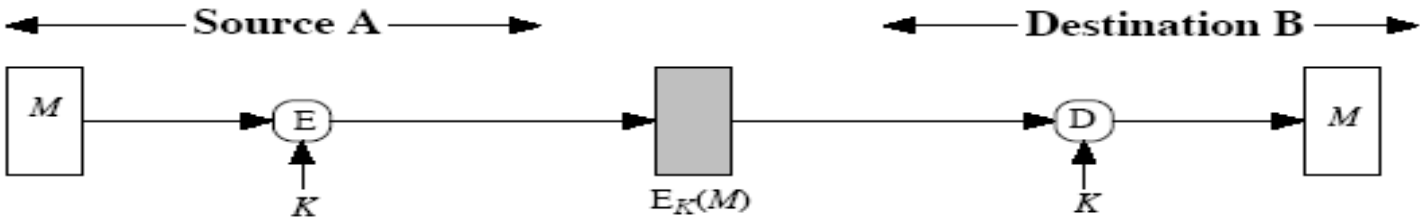
인증 함수 (1/15)

❑ 인증 함수

- ❖ 메시지 암호화(message encryption)
  - ➢ 메시지 전체의 암호문이 이것의 인증자로 제공.
- ❖ 메시지 인증 코드(MAC)
  - ➢ 인증자로서 적용되는 고정된 길이 값을 만드는 메시지 및 비밀키의 공개 함수.
- ❖ 해쉬 함수(hash function)
  - ➢ 임의 길이의 메시지를 고정된 길이의 해쉬 값으로 대응시키는 공개 함수로서 인증자로서 제공.

인증 함수 (2/15)

❑ 메시지 암호화의 기본 사용법 : 대칭암호



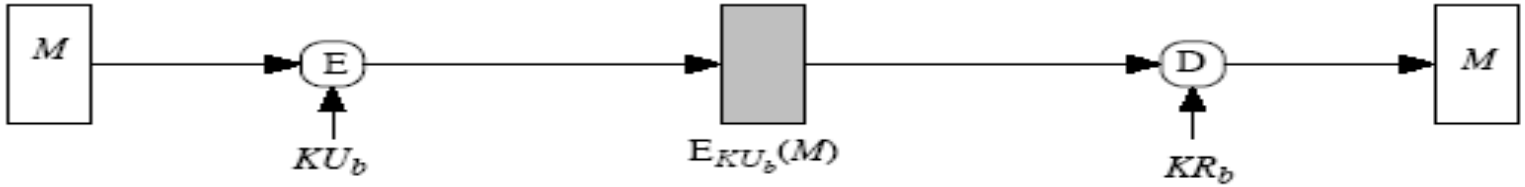
(a) Symmetric encryption: confidentiality and authentication

❖ A → B: $E_k[M]$

- ➢ 기밀성 제공
  - 오직 **A**와 **B**만이 **K**를 공유함.
- ➢ 부분적인 인증 제공
  - 오직 **A**로부터 전송 가능함.
  - 전송 중 변경은 불가능해야 함.
  - 특정 형식과 잉여 정보가 필요함.
  - 서명은 제공하지 않음
  - 송신자가 메시지를 위조할 수 있음.
  - 송신자가 메시지 전송에 대해 부인 가능함.

인증 함수 (3/15)

❑ 메시지 암호화의 기본 사용법 : 공개키(비대칭) 암호



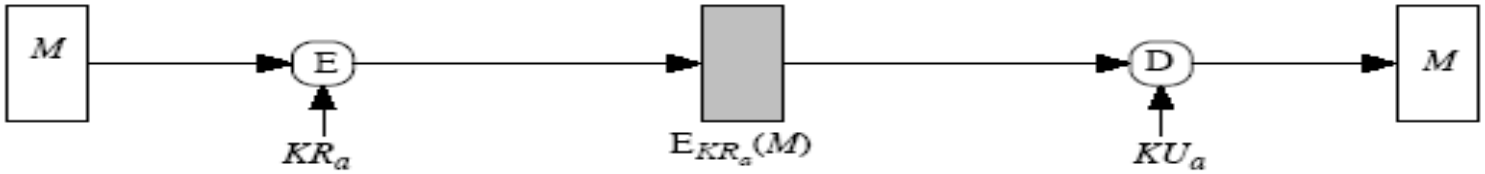
(b) Public-key encryption: confidentiality

❖ A → B: E_{kub}[M]

- ➢ 기밀성 제공
  - 오직 **B**만이 복호 가능한 $\mathbf{KR_B}$를 가지고 있음.
- ➢ 인증은 제공하지 않음
  - 메시지 암호를 위해 누군가 $\mathbf{KU_B}$를 이용할 수 있으며, 자신이 **A**라고 주장할 수 있음.

인증 함수 (4/15)

❑ 메시지 암호화의 기본 사용법 : 공개키 암호 – 인증과 서명



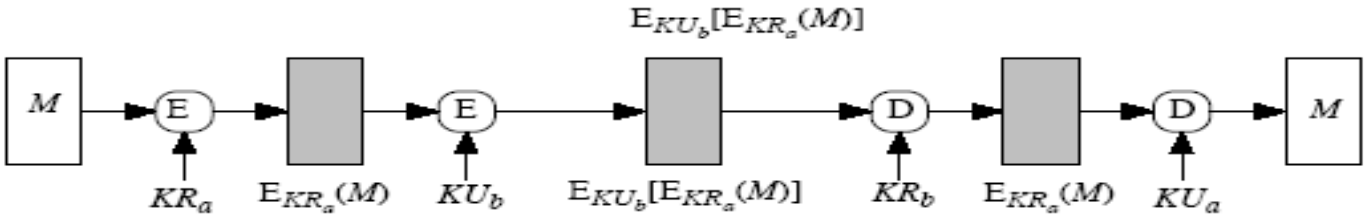
(c) Public-key encryption: authentication and signature

❖ A → B: $E_{kRa}[M]$

- 인증과 서명을 제공
  - 오직 **A**만이 암호화를 위해 $\mathbf{KR}_a$를 갖는다.
  - 전송상에 변경되어서는 안됨.
  - 특정 형식과 잉여 정보가 필요함.
  - 누구라도 서명 검증을 위해 $\mathbf{KU}_a$를 사용할 수 있음.

인증 함수 (5/15)

❑ 메시지 암호화의 기본 사용법 : 공개 키암호 – 기밀성, 인증과 서명



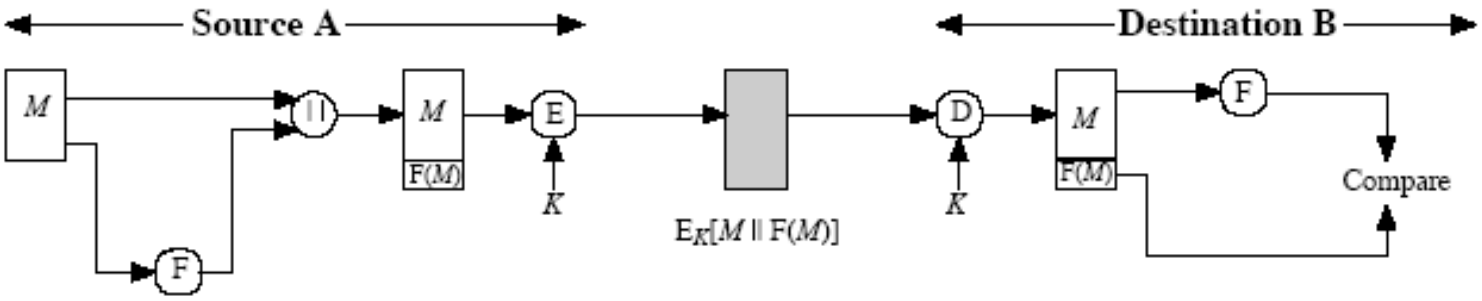
(d) Public-key encryption: confidentiality, authentication, and signature

❖ A → B: $E_{kUb}[E_{kRa}(M)]$

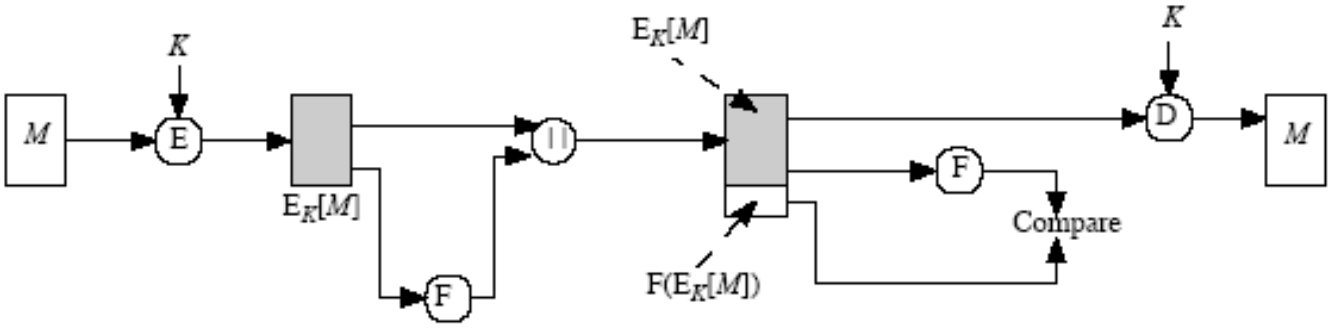
- **KU_b**가 있기 때문에 기밀성을 제공
- **KR_a**가 있기 때문에 인증과 서명을 제공

인증 함수 (6/15)

❑ 내부 및 외부 에러 제어



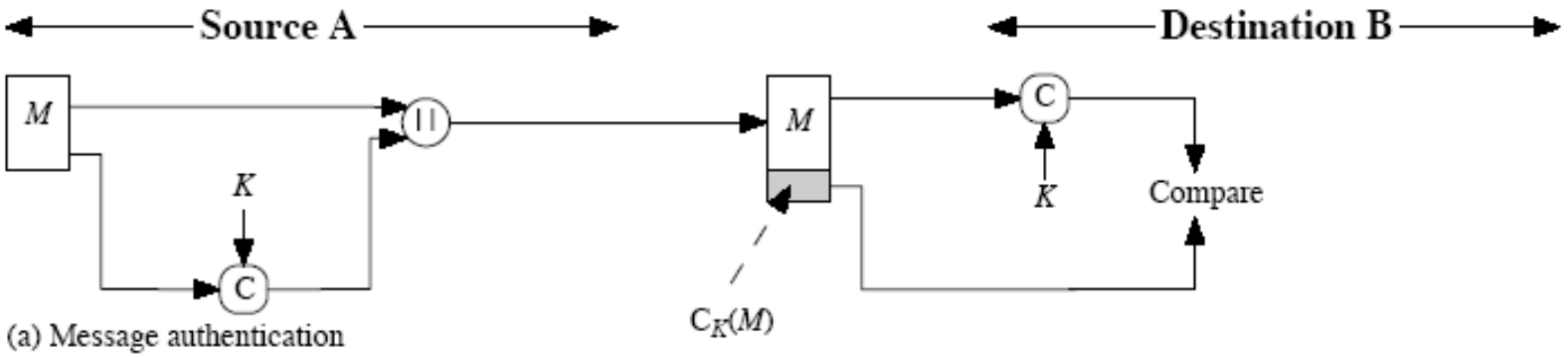
(a) Internal error control



(b) External error control

인증 함수 (7/15)

❑ MAC의 기본 사용법 : 메시지 인증



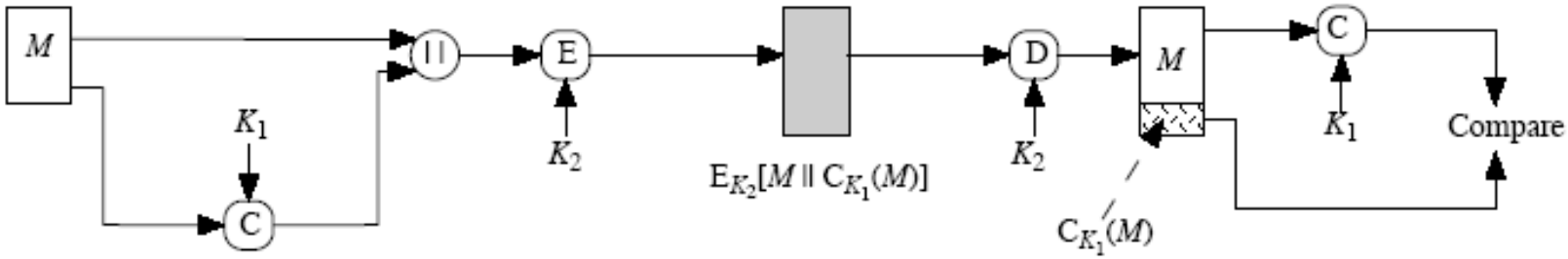
❖ A → B: M || C_k[M]

➢ 인증 제공

- 오직 **A**와 **B**만이 **K**를 공유

인증 함수 (8/15)

❑ MAC의 기본 사용법 : 메시지 인증과 기밀성(평문에 인증을 연결)



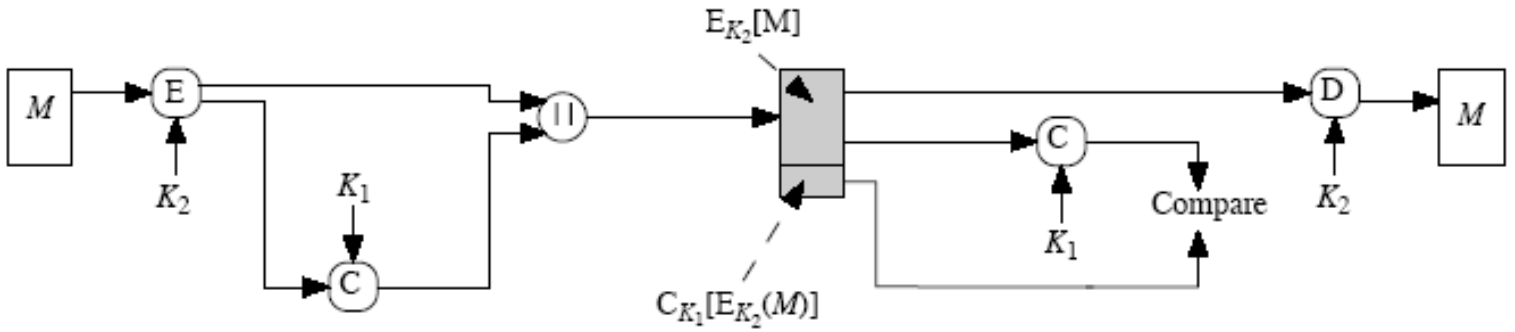
(b) Message authentication and confidentiality; authentication tied to plaintext

❖ A → B: $E_{k2}[M \| C_{k1}(M)]$

- 인증 제공
  - 오직 **A**와 **B**만이 $\mathbf{K_1}$를 공유
- 기밀성 제공
  - 오직 **A**와 **B**만이 $\mathbf{K_2}$를 공유

인증 함수 (9/15)

❑ MAC의 기본 사용법 : 메시지 인증과 기밀성(암호문에 인증을 연결)

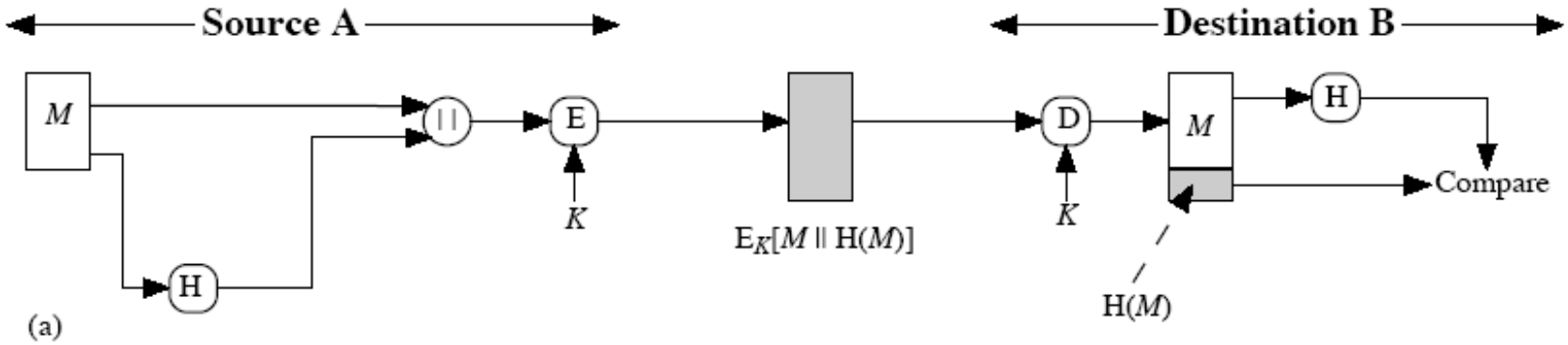


(c) Message authentication and confidentiality; authentication tied to ciphertext

- A → B: $E_{k2}[M] || C_{k1}(E_{k2}[M])$
  - 인증 제공
    - $\mathbf{K_1}$를 사용
  - 기밀성 제공
    - $\mathbf{K_2}$를 사용

인증 함수 (10/15)

❑ 해쉬함수 H의 기본 사용법 : 메시지와 해쉬 코드를 암호화

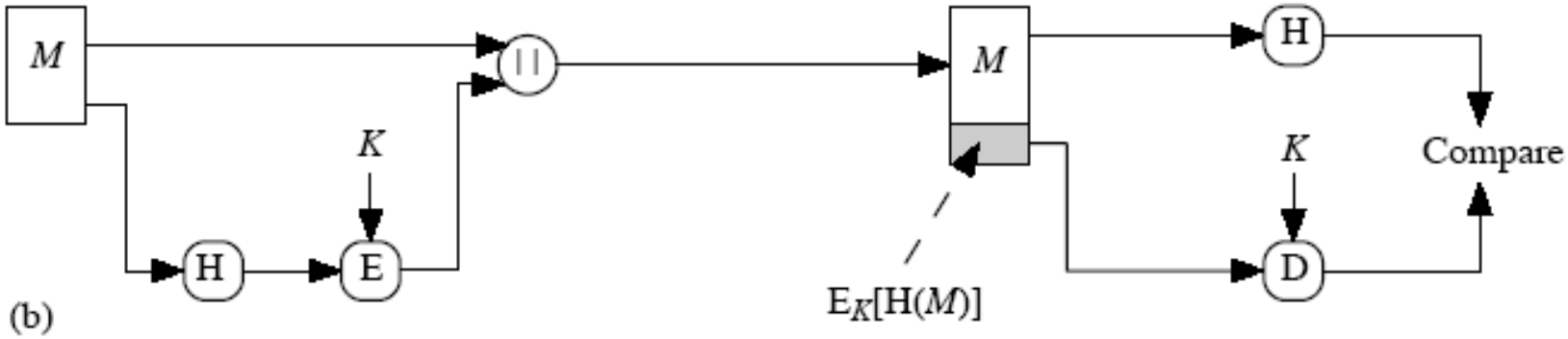


❖ A → B: E_k [M || H[M])

- 기밀성 제공
  - 오직 **A**와 **B**만이 **K**를 공유
- 인증 제공
  - **H(M)**은 암호학적으로 보호됨.

인증 함수 (11/15)

❑ 해쉬함수 H의 기본 사용법 : 공유된 비밀키를 갖고 해쉬 코드 암호화

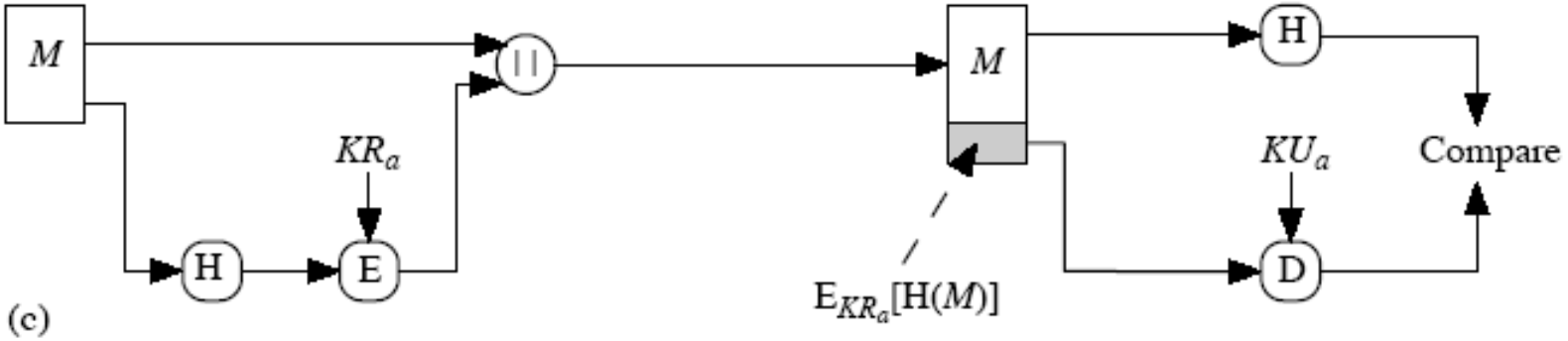


❖ A → B: $E_k[M \,||\, E_{kRa}[H(M)]]$

- 인증 및 디지털 서명 제공
- 기밀성 제공
  - 오직 **A**와 **B**만이 **K**를 공유

인증 함수 (12/15)

❑ 해쉬함수 H의 기본 사용법 : 송신의 개인키로 해쉬 코드를 암호화



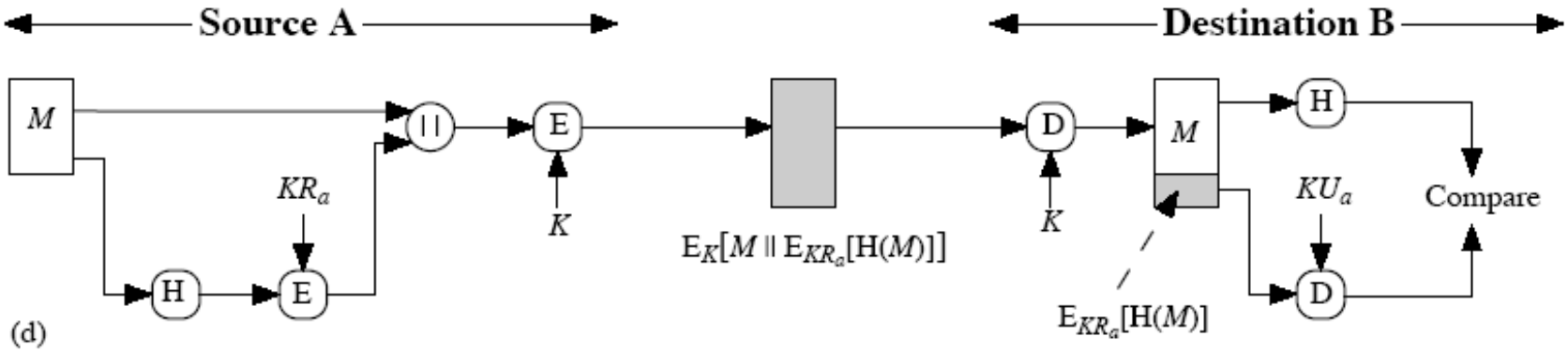
❖ A → B: M || E_{kRa}[H(M)]

➢ 인증 및 디지털 서명 제공

- **H(M)**은 암호학적으로 보호됨.
- 오직 **A**만이 $\mathbf{E_{kRa}[H(M)]}$를 생성할 수 있음.

인증 함수 (13/15)

❑ 해쉬함수 H의 기본 사용법 : 공유된 비밀키로 (c)의 결과를 암호화

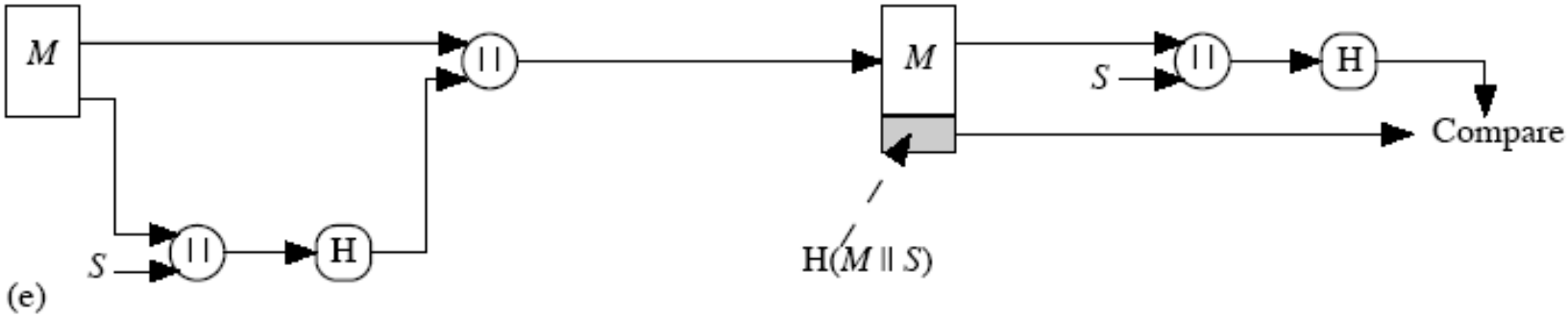


❖ A → B: $E_k[M \| E_{kRa}[H(M)]$

- 인증 및 디지털 서명 제공
- 기밀성 제공
  - 오직 **A**와 **B**만이 **K**를 공유

인증 함수 (14/15)

❑ 해쉬함수 H의 기본 사용법 : 메시지와 해쉬 코드를 암호화



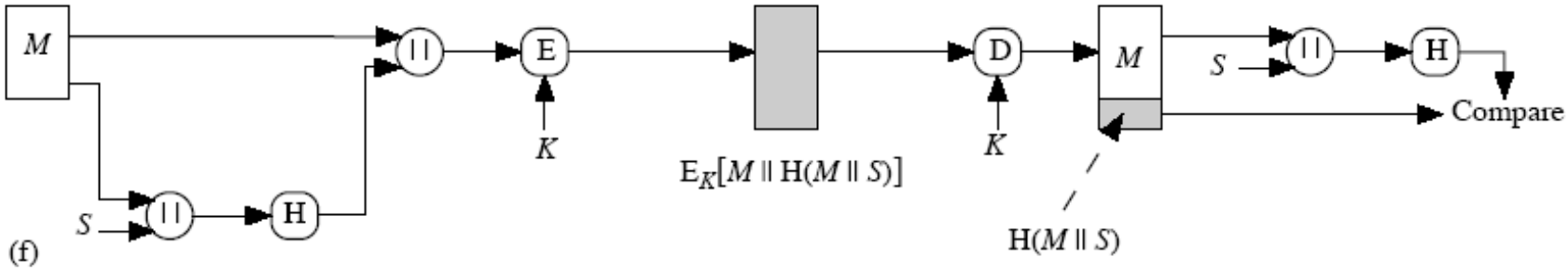
❖ A → B: M || H(M || S)

➢ 인증 제공

▪ 오직 **A**와 **B**만이 **S**를 공유

인증 함수 (15/15)

❑ 해쉬함수 H의 기본 사용법 : (e)의 결과를 암호화



- A → B: E_k[M || H(M) || S]
  - 인증 제공
    - 오직 **A**와 **B**만이 **S**를 공유
  - 기밀성 제공
    - 오직 **A**와 **B**만이 **K**를 공유

참고문헌

- 컴퓨터 통신보안, 최용락 외3 공역, 그린 출판사, 2006
- 암호이론과 보안, 박창섭 저, 대영사, 1999

Thanks

Q & A