4장. 키분배와 사용자 인증

4.3 비대칭 암호를 이용한 키 분배

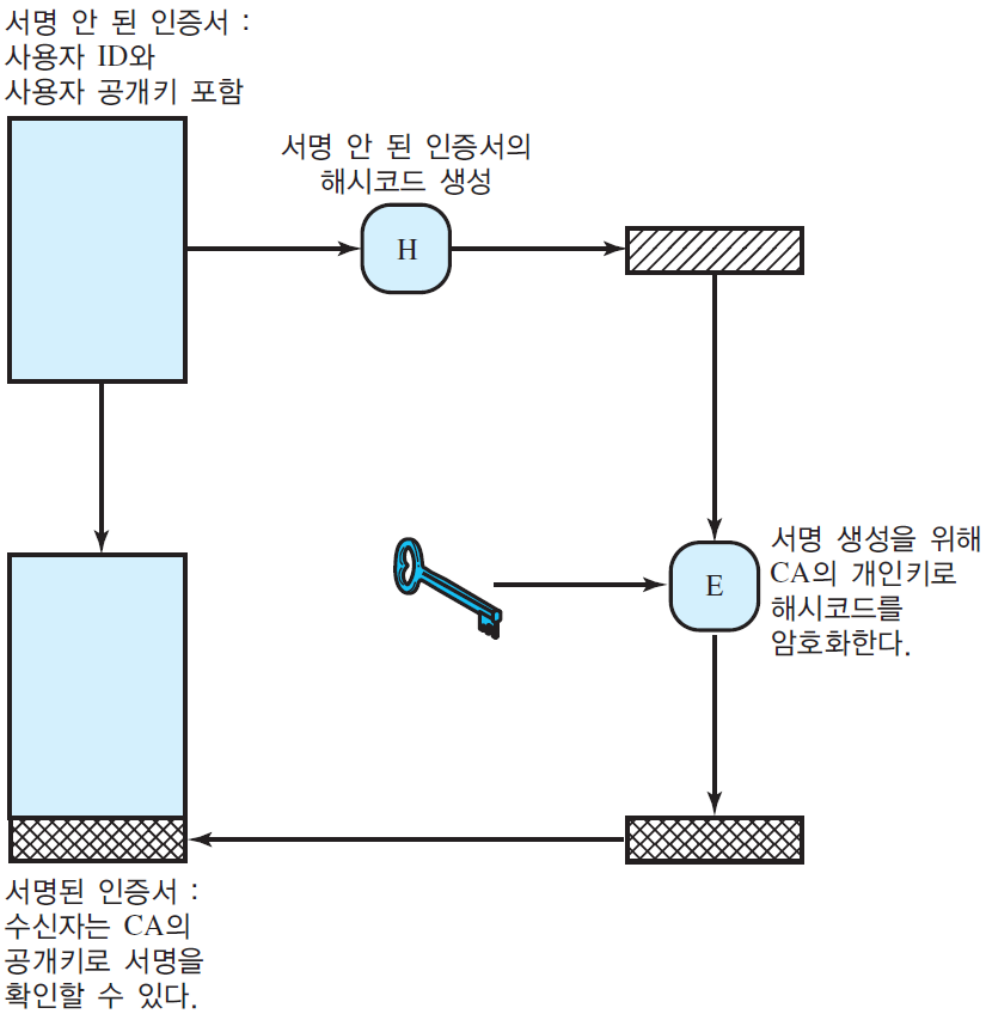
개요

- 공개키 암호의 용도
  - 공개키 분배
  - 대칭 비밀키 분배

공개키 인증서

- 공개키 암호화의 요점
  - 공개키 공개
- 공개키의 위장 문제
  - 공격자가 A의 공개키라고 위장하는 경우 그것을 어떻게 구별할 수 있나?
- 안전한 공개키 전달
  - 공개키 인증서(public-key certificate)
    - 공개키와 키 소유자의 사용자 ID로 구성
    - 이를 신뢰할 만한 제 3자가 서명
    - 제3자라 하면 정부기관이나 금융기관 같은 사용자 모두가 신뢰하는 인증기관(CA: certificate authority)

공개키 인증서 사용


서명 안 된 인증서 :
사용자 ID와
사용자 공개키 포함
서명 안 된 인증서의
해시코드 생성
H
서명 생성을 위해
CA의 개인키로
해시코드를
암호화한다.
E
서명된 인증서 :
수신자는 CA의
공개키로 서명을
확인할 수 있다.

공개키를 이용한 비밀키 분배

- Diffie-Hellman 키교환을 이용
  - 사실 이 방법은 널리 이용
  - 두 통신자 사이에 인증을 제공하지 못함
- 강력한 대안
  - 공개키 인증서 활용

방법

1. 메시지를 준비한다.
2. 일회용 세션키를 이용하는 관용암호 기법으로 메시지를 암호화한다.
3. 앨리스의 공개키를 이용해서 그 세션키를 암호화한다.
4. 암호화된 세션키를 메시지에 첨부해서 앨리스에게 보낸다.