3.6 디지털 서명

제3장. 공개키 암호와 메시지 인증

디지털 서명 (1)

- 메시지의 출처와 메시지 내용에 대한 확신을 위해 메시지 전체를 암호화하면 된다
  - 단점 : 메모리가 많이 소요
- 전체가 아닌, 문서의 기능을 대신하는 작은 비트블록을 암호화하는 방법이 필요
  - 인증자(authenticator) : MAC(Hash)을 암호화

디지털 서명 (2)

- 인증자 변경 없이 문서만 변경하는 것이 불가능
  - MAC의 기능
- 인증자를 송신자의 개인키로 암호화했다면, 무결성 외에도 출처 확인 가능
- SHA-1 같은 안전 해시코드가 이런 역할
- 메시지의 무결성은 보장하지만 기밀성은 보장 못한다