해시와 공개키 암호화 목적(디지털 서명에서 함께 사용)

● 해시와 공개키의 기본 역할

▶ 해시 (Hash)

- 목적 : 데이터의 무결성(Integrity) 확인
- 특징
  * 임의의 길이의 데이터를 고정된 길이의 해시값으로 변환
  * 이 과정은 단방향(일방향 함수)이라서 해시값에서 원본 데이터를 복원하는 것은 불가능(예: SHA-256)
- 키 사용 : 키를 사용하지 않음

▶ 공개키 암호화 (Public Key Cryptography)

- 목적 : 데이터의 기밀성(Confidentiality) 또는 인증(Authentication) 및 부인 방지(Non-repudiation)
- 특징
  * 공개키와 개인키 쌍을 사용
  * 기밀성 : 공개키로 암호화, 개인키로 복호화
  * 인증/서명 : 개인키로 암호화(서명), 공개키로 복호화(검증)
- 키 사용 : 공개키와 개인키를 사용