전자 서명을 위해 RSA와 SHA

● RSA와 SHA는 상호 보완적으로 작동

- 데이터 기밀성 확보를 위한 암호화는 주로 대칭키 암호화(AES)가 담당
- 비대칭키(RSA)는 대칭키를 안전하게 교환하는 데 사용되는 것이 일반적임

● 전자 서명에서 RSA와 SHA의 역할 분담

- 전자 서명은 메시지의 인증 및 무결성을 보장하는 기술
- 주로 해시 함수(SHA)와 비대칭 키 암호화(RSA)의 조합으로 구현됨

알고리즘	종류	목적	전자 서명에서의 역할
SHA (Secure Hash Algorithm)	해시 함수	메시지의 무결성	원본 메시지를 고정 길이의 다이제스트로 압축 (지문 생성)
RSA (Rivest-Shamir-Adleman)	비대칭 암호	인증 및 부인 방지	SHA 다이제스트를 개인키로 암호화하여 서명 생성 및 공개키로 복호화하여 검증

● 전자 서명 과정에서의 사용 예시 (RSA-SHA256)

- 서명 생성자 (개인키 소유자)
  * SHA 사용 : 원본 메시지 M을 SHA-256으로 해시하여 메시지 다이제스트 h를 생성
  * RSA 사용 : h를 자신의 RSA 개인키로 암호화하여 최종 디지털 서명 S를 만듬

- 검증자 (공개키 소유자)
  * RSA 사용 : 서명 S를 서명자의 RSA 공개키로 복호화하여 원래의 해시값 h'를 얻음
  * SHA 사용 : 받은 원본 메시지 M을 SHA-256으로 다시 해시하여 해시값 h''를 생성
  * 검증: h'와 h''가 일치하면 서명이 유효하다고 판단

● 데이터 기밀성 (암호화)에서의 사용

알고리즘	종류	역할
AES (Advanced Encryption Standard)	대칭키 암호	실제 대용량 데이터를 빠르게 암호화/복호화 (기밀성 확보의 주역)
RSA	비대칭 암호	AES에 사용된 대칭키를 수신자의 공개키로 암호화하여 안전하게 전달
SHA	해시 함수	데이터의 기밀성보다는 무결성이나 패스워드 저장에 사용됨