전자서명

■ 전자서명(Electronic Signature)

- 서명자를 확인하고 서명자가 해당 전자문서에 서명했다는 사실을 나타내는 데 이용하려고, 특정 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보
    * 종이 문서에 자필로 서명하거나 도장을 찍는 행위를 디지털 환경에서 구현한 것
        ⇒ 도장(개인키) 자체를 상대방에게 주는 것이 아니라, 도장을 찍은 흔적(전자서명)만 전달하는 것임

■ 전자서명의 주요 기능 및 특징

- 전자서명은 일반 서명과 동일한 법적 효력을 가집니다 (대한민국에서는「전자서명법」에 의해 효력이 부여됨).

    * 1) 서명자 인증 (신분 증명)
        - 서명을 한 사람이 누구인지 그 신원을 명확하게 확인할 수 있음
        - 공개키 암호화 방식(PKI) 등 기술을 사용하여 서명자의 신원을 보장함

    * 2) 무결성 보장 (위변조 방지)
        - 문서가 서명된 후 변경되지 않았음을 증명함
        - 문서의 고유한 해시값(Hash)을 생성하고 이를 서명자의 개인키로 암호화하여 서명에 포함시키는데, 문서 내용이 단 1비트라도 바뀌면 해시값도 완전히 달라져 서명이 무효가 됨

    * 3) 부인 방지
        - 서명자가 나중에 "나는 이 문서에 서명하지 않았다"라고 주장하는 것을 막아줌
        - 서명이 유효하다는 것은 개인키를 가진 당사자가 서명했다는 것을 기술적으로 증명하기 때문임

■ 전자서명과 디지털 서명의 관계

- 전자서명(Electronic Signature)이 디지털 서명(Digital Signature)을 포괄하는 상위 개념

  - 전자서명(Electronic Signature)
    * 포괄적인 개념으로, 디지털 문서에 동의나 승인을 나타내는 모든 전자적인 행위(예: 문서에 타이핑된 이름, 스캔된 서명 이미지, 클릭으로 동의)

  - 디지털 서명(Digital Signature)
    * 전자서명의 한 종류로, 공개키 암호화 기술(PKI)을 기반으로 하여 서명자 인증, 무결성, 부인 방지 등의 강력한 보안 기능을 제공하는 기술적인 방법

구분	전자서명 (Electronic Signature)	디지털 서명 (Digital Signature)
개념	넓은 의미의 전자적 동의 및 승인 행위 전체	공개키 암호화 기술(PKI)을 사용한 보안성이 강화된 특정 유형의 전자서명
범위	모든 형태의 전자적 서명 (상위 개념)	전자서명 중 기술적 표준을 따르는 형태 (하위 개념)
예시	마우스로 그린 서명 이미지, PDF에 타이핑된 이름, "동의" 버튼 클릭, 전화 PIN 입력 등	공인(또는 공동)인증서로 생성된 서명, 디지털 인증서를 기반으로 하는 서명
보안	비교적 낮거나 다양함 (변조 방지가 어려울 수 있음)	암호화를 통해 무결성과 부인 방지가 확실하게 보장됨 (고수준 보안)

일반적으로 비대칭 암호 방식(공개키 암호)의 기본적인 용도

● 데이터 기밀성(Confidentiality) 확보

⇒ 공개키로 암호화, 개인키로 복호화

● 데이터 무결성 및 인증(Integrity & Authentication) 확보 (전자 서명)

⇒ 개인키로 암호화, 공개키로 복호화(검증)

⇒ 공개키로 복호화하는 과정은 암호문 내용의 기밀성을 확보하는 것이 목적이 아니라, 암호문이 특정 개인키 소유자(발신자)에 의해 생성되었음을 공개적으로 확인(검증)하는 것이 목적임

전자서명의 원리 – 개인키를 사용해서 서명하는 것

□ 전자서명(DSA, Digital Signature Algorithm)의 핵심 원리 요약

- 메시지에 디지털 서명을 생성하고 검증하는 알고리즘
  * '이 메시지를 내가 보냈다는 증거'를 수학적으로 만들어내는 방식임
- 전자서명은 세 단계로 이루어지며, 개인키의 비밀 유지와 공개키를 통한 검증임
- 공개키로 암호화된 메시지를 복호화한다는 것은 메시지가 해당 공개키와 쌍을 이루는 개인키로 암호화되었다는 것을 증명하기 위함
  * 송신자 A가 자신의 개인키로 암호화하고, 수신자 B가 A의 공개키로 복호화하여 검증하는 과정

1. 서명 생성 (개인키의 역할)

- 주체 : 서명을 하는 사람 (사용자)
- 원리
  * 서명할 문서(예: 이체 내용)의 내용을 "요약(해시)"함
  * 요약된 정보(해시 값)를 나의 비밀 도장인 개인키(P_r)로 암호화함
  * 결과(전자서명 S) : 암호화된 요약 정보자(개인키(P_r) 자체는 절대 밖으로 나가지 않음)
- 예
  * 개인키 (x) : 서명을 만들 때 사용하는 비밀 숫자
  * 공개키 (y) : 서명을 검증할 때 사용하는 공개 숫자
  * 예시 : Alice는 개인키 x=7을 가지고 있고, 공개키 y=23을 공개

  * 서명 생성 (Alice가 메시지를 보낼 때)
    - 개인키와 랜덤값으로 서명(r, s)을 만듬
    - 메시지 해시 : 메시지 "Hello"를 SHA-1 같은 해시 함수로 처리
      → 해시값 H = 12345
    - 랜덤 수 k 선택 : Alice는 k=5 같은 임의의 수를 선택
      * 1) 서명 계산
        - r = (g^k mod p) mod q → r = 8
        - s = (k^{-1} × (H + x × r)) mod q → s = 12
      * 2) 서명 결과

2. 서명 첨부 및 전송

- 주체 : 서명을 하는 사람
- 원리
    * 원래의 문서와 전자서명(S)을 함께 상대방(은행)에게 보냄(이때, 공개키(P_u)가 담긴 인증서도 함께 보냄)

- 예
    * Alice는 메시지와 함께 (r=8, s=12)를 Bob에게 보냄

3. 서명 검증 (공개키의 역할)

- 주체 : 서명을 받는 사람 (은행)
- 원리 :
    * 은행은 내가 보낸 공개키(P_u)를 사용하여 전자서명(S)을 복호화함 → 원래의 요약 값(H_1)이 나옴
    * 은행은 받은 원래 문서를 똑같은 방식으로 자체적으로 요약 → 새로운 요약 값(H_2)이 나옴
    * 만약 H_1과 H_2가 일치하면
        * "이 서명은 이 공개키에 해당하는 개인키를 가진 사람만 만들 수 있다." (신원 보증)
        * "문서가 전송 중에 위변조되지 않았다." (무결성 보장)

- 예
    * 서명 검증 (Bob이 메시지를 받을 때)
        - 1) 메시지 해시 : Bob도 "Hello"를 해시 → H = 12345
        - 2) 계산
            * $w = s^{-1} \bmod q \rightarrow w = 3$
            * $u1 = H \times w \bmod q \rightarrow u1 = 2$
            * $u2 = r \times w \bmod q \rightarrow u2 = 4$
            * $v = ((g^{u1} \times y^{u2}) \bmod p) \bmod q \rightarrow v = 8$
        - 3) 검증
            * 공개키로 계산한 값이 r과 같으면, 서명이 진짜임을 확인
            * v == r → 8 == 8 → **서명 유효!!!!!**

* 공개키(Public Key)를 이용한 복호화는 주로 전자 서명(Digital Signature)의 검증 과정에서 사용