2. 전자서명 방식

1. 중재 서명

① 대칭키 암호 알고리즘과 중재자를 이용하는 서명이다.
- 대칭키 암호는 하나의 키를 여러 사람이 공유한다.
- 항상, 정보가 노출될 수 있다.

② 대칭키 암호를 이용한 전자서명은 서명자가 자신이 서명한 것이 아니라고 부인할 수 있다.
- 대칭키 노출 등의 이유로 서명자는 항상 서명 사실을 부인할 수 있다.
- 즉, 분쟁이 발생될 수 있다.
- 중재자가 서명 절차에 관여한 경우는 부인을 봉쇄할 수 있다.(증인)

2. 위임(대리) 전자서명
- 본인이 부재 시 자신을 대신하여 다른 사람이 서명한다.
- 제3자가 서명할 수 있어야 하고 검증자는 서명자의 위임 사실을 확인할 수 있어야 한다.
- 완전위임, 부분위임, 보증위임

3. 다중 전자서명
- 상황에 따라서, 하나의 문서에 여러 명이 서명하는 경우가 있다.
- 예를 들면, 전자 결재 시스템에서 하나의 문서에 여러 명이 서명해야 한다.
- 하나의 문서에 여러 명이 서명할 수 있도록 고안된 서명이다.

4. 부인방지 전자서명
- 공개키 암호 알고리즘을 이용한 전자서명이다.
- 서명검증과정에 서명자의 신뢰성 있는 공개키가 있어야 검증 가능하다.
- 서명을 검증할 때 반드시 서명자의 도움이 있어야 검증이 가능한 방식이다.
- 서명자의 도움이 있어야 하는 이유는 공개키에 대응하는 개인키가 필요하므로
- 개인키는 서명자만 가지고 있다.

5. 메시지 복원형 전자서명

① 원래의 메시지가 필요 없는 전자서명이다.

- 서명검증과정에서 원래의 메시지가 복원된다.
- 서명 검증을 위해 원래의 메시지가 필요 없다.

② **RSA 암호** 알고리즘은 메시지 복원형 전자서명 방식으로 구현할 수 있다.

- 해시함수를 사용하지 않고, 메시지에 **직접 서명**한다.(번잡함 회피) → $c = m^d \bmod n$
- 매우 큰 메시지에는 적용하기 어렵다.
- 전자서명에서 개인키는 서명키가 되고, 공개키는 확인키가 된다.
- 전자서명에서 공개키의 인증이 매우 중요하다.
- 공개키의 인증이 불확실하면 누구의 서명인지 확신할 수 없다.
- 따라서, 인증기관에서 보증하는 인증서를 이용한다.
- 인증서는 공개키가 누구의 공개키인지 확인해주는 역할을 담당한다.

6. 부가형 전자서명

① 원래의 메시지가 필요한 전자서명이다.

- 서명검증과정에서 메시지를 추출할 수 없다.
- 서명검증을 위해서는 원래의 메시지가 반드시 필요하다.
- 예를 들면, **해시함수를 이용한 전자서명**이다.

② 메시지에 서명함수를 적용하지 않고, 메시지의 해시값에 서명함수를 적용한다.

- 긴 메시지에 서명하지 않고, 짧은 해시값에 서명함으로 효율적이다.
- 해시함수를 이용한 전자서명은 변조/위조가 어렵다.(해시함수의 일방향성 성질)

③ 전자서명에 사용할 해시함수는 "일방향성과 충돌회피"를 만족해야 한다.

7. 은닉 전자서명(blind digital signature)

- 서명하고자 하는 문서의 **내용은 공개하지 않고**, 문서에 대한 서명을 받는다.
- 개인정보 보호 및 익명성을 보장할 수 있다.
- 서명자는 자신이 누구에게 서명했는지 알 수 없다.
- 서명자는 은닉 전자서명 발행 프로토콜을 통해 생성한 (문서, 서명) 쌍에 대해 그 유효성을 검증할 수는 있다. 하지만, 자신이 누구에게 발행했는지 알 수 없다.
- 예 : 금융거래에서 입출금, 과학자들이 발견한 중요한 이론 특허, 전자화폐, 전자선거 등
- David Chaum이 고안한 서명기법이다.
- RSA 디지털 서명 구조를 변형하여 은닉 전자서명을 구현하였다.

◈ 공증기관의 블라인드 디지털 서명

소유주는 메시지를 작성하고, 은닉(blind) 시킨다.
⇓
은닉(blind)된 메시지를 공증기관에 보낸다.
⇓
공증기관은 은닉(blind)된 메시지에 서명한다.
⇓
공증기관은 서명된 메시지를 소유주에게 되돌려준다.
⇓
원래의 메시지 서명을 얻기 위해 은닉(blind)을 제거한다.

기출문제 분석

1. 전자서명 방식에 대한 설명으로 옳지 않은 것은? [2016년 지방 9급]

① 은닉 서명(blind signature)은 서명자가 특정 검증자를 지정하여 서명하고, 이 검증자만이 서명을 확인할 수 있는 방식이다.
② 부인방지 서명(undeniable signature)은 서명을 검증할 때 반드시 서명자의 도움이 있어야 검증이 가능한 방식이다.
③ 위임 서명(proxy signature)은 위임 서명자로 하여금 서명자를 대신해서 대리로 서명할 수 있도록 한 방식이다.
④ 다중 서명(multi_signature)은 동일한 전자문서에 여러 사람이 서명하는 방식이다.

♤ **은닉 서명(blind signature)**

• **은닉 서명**(blind signature)은 서명자가 특정 검증자를 지정하여 서명하고, 이 검증자만이 서명을 확인할 수 있는 방식이다.**(×)**
→ **은닉 서명**은 서명하고자 하는 문서 내용은 **공개하지 않고**, 문서에 대한 서명을 받는다.

정답 : ①