Digital Signatures(전자서명)

https://youtu.be/ReQjuExafB8

전자서명의 원리

RSA 전자서명 기법

RSA 전자서명의 안정성

전자서명

전자서명

서명자를 확인하고 서명자가 전자문서에 서명하였음을 나타내는 데 이용.

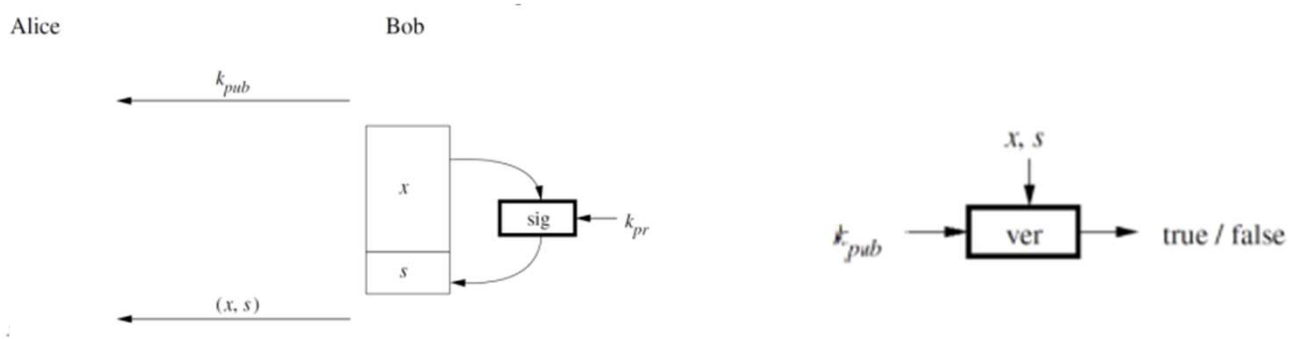
사이버 공간에서의 정보들을 쉽게 위변조 할 수 있기 때문에 제공자를 확인하고 증명하기 위함.

```
* 인감 : 종이문서 + 인감도장 날인
* 서명된 전자문서 : 전자문서 + 전자서명(전자문서 해시 + 개인키의 암호화)
```

→대부분 **공개키 암호 알고리**즘을 이용하여 구현하며, **무결성**을 확인하고 **인증**과 **부인 방지** 기능 제공

전자서명

전자서명의 기본 원리



기존의 수기 서명과 마찬가지로 전자서명 s가 메시지 x에 추가됨.

개인키 k_{pr} 을 가지고 있는 사람만이 서명을 생성할 수 있어야 함.

단, 서명은 문서마다 변경되어야 함.

→ 서명은 메시지 x와 개인키 k_{pr}을 입력으로 갖는 함수에 의해 구현됨.

→ 메시지 x와 공개키 k_{pub} 을 이용하여 검증됨(Verification)

전자서명

전자서명이 제공하는 보안 서비스

위조 불가 (Unforgettable) : 합법적인 서명자만이 전자 문서에 대한 전자서명을 생성할 수 있어야 한다.
서명자 인증 (User Authentication) : 전자서명의 서명자를 누구든지 검증할 수 있어야 한다.
부인 불가 (Non repudiation) : 서명자는 서명 후에 자신의 서명 사실을 부인할 수 없어야 한다.
변경 불가 (Unalterable) : 서명한 문서의 내용은 변경될 수 없어야 한다.
재사용 불가 (Not Reusable) : 전자문서의 서명은 다른 전자문서의 서명으로 사용될 수 없어야 한다.

전자서명 알고리즘 종류

RSA 전자서명 : 소인수분해하는 문제의 어려움에 근거.
엘가말 전자서명 : 이산대수 문제에 근거. (슈노어, DSS 전자서명)
타원곡선 전자서명 : 타원곡선상에서 군을 정의하고 이에 대한 이산대수 계산의 어려움에 근거.

RSA 전자서명 기법(Schoolbook RSA Signature Scheme)

RSA 전자서명 기법

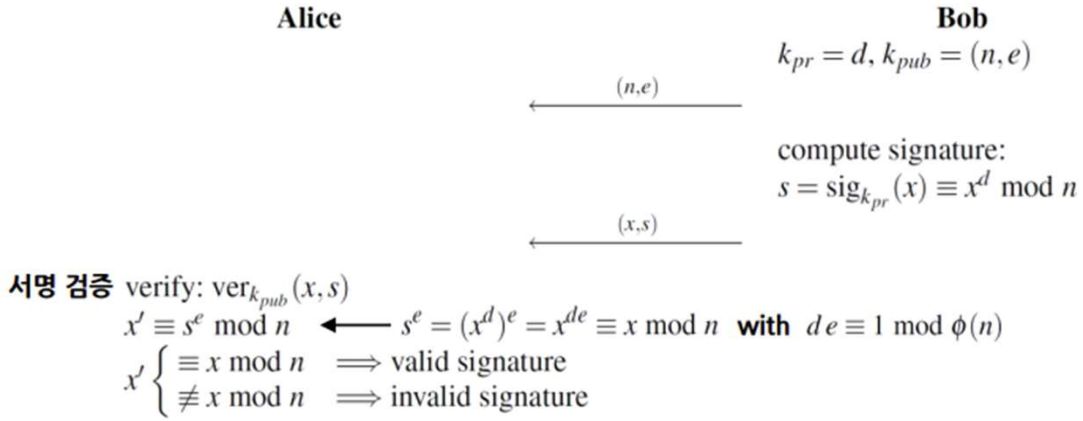
RSA 암호화 기법에 기반을 두고 있으며,

두 개의 큰 소수의 곱을 인수분해 하기 어렵다는 사실을 이용함.

Bob이 Alice에게 서명된 메시지를 보내고자 할 때, RSA 암호화와 동일한 RSA 키를 생성함

→Bob's 개인키 : $k_{pr} = d$

→Bob's 공개키 : $k_{pub} = (n, e)$

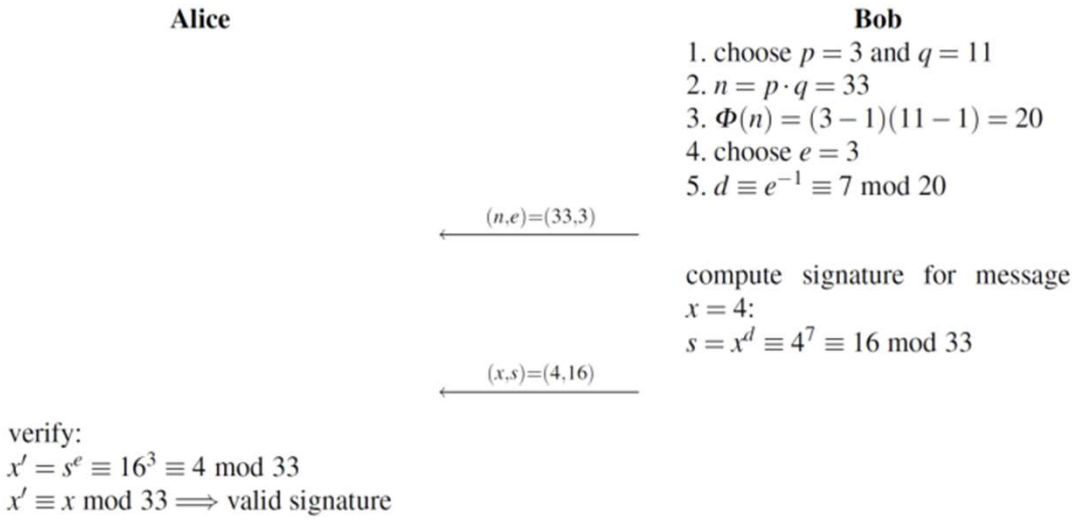


RSA 전자서명 기법(Schoolbook RSA Signature Scheme)

Example

Bob이 서명된 메시지 x = 4를 보내고자 함.

RSA 암호화 기법과 달리, 개인키가 전자서명에 사용되고 공개키는 이를 검증할 때 사용됨.



Alice는 위의 검증을 통해 메시지 인증(Authentication) 및 무결성(Integrity)을 확인할 수 있음.

RSA 전자서명의 안정성

RSA 암호화와 동일한 제한 사항

전자서명의 길이: 대략적으로$\lceil \log_2 n \rceil$ bit.

서명의 길이가 일반적인 인터넷 응용분야에서는 문제x

모바일 폰과 같이 제한되는 시스템에서는 바람직하지 않다.

공개키의 진정성(Authenticity) 필요

공개키의 진정성이 반드시 보장되어야 함.

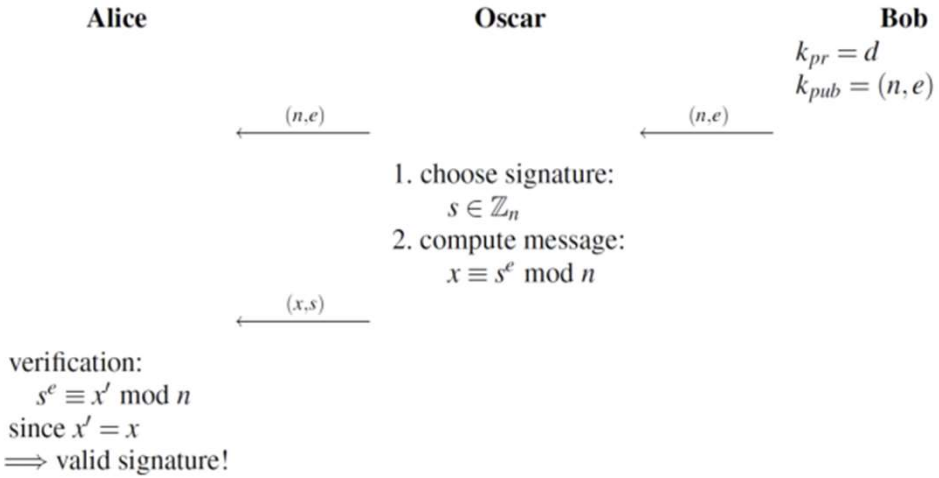
공격자가 서명자의 키인 것처럼 올바르지 않은 공개키를 사용하는 것을 막기 위해, 인증서가 사용됨

서명 위조 공격(Existential Forgery Attacks)

기본적인 RSA 전자서명 기법에서 공격자가 임의의 메시지 x에 대해

유효한 서명을 생성하여 공격하는 것을 말함.

RSA 전자서명의 안정성



공격자 Oscar는 중간에서 Alice에게 본인이 Bob이라고 주장하여 메시지-서명(x,s)을 생성할 수 있으며, Alice는 Oscar와 동일한 계산을 수행하게 되어 서명이 올바르다고 검증하게 됨.

공격자는 서명 s만 선택할 수 있고 메시지 x의 의미를 임의로 수정할 수는 없음.

그럼에도 위조를 제대러 인지하지 못하는 자동화된 검증 프로세서는 올바르게 작동한다고 할 수 있음. → 이러한 형태의 공격을 막기 위해 패딩 기법이 적용됨.

Q & A