

전자서명(Digital Signature)

컴퓨터공학부 김상원

<https://youtu.be/KL5oo3PSn7g>

전자서명(Digital Signature)이란

RSA키 생성

전자서명의 생성과 검증

Q&A

전자서명이란

정의: 네트워크에서 송신자의 신원을 증명하는 방법으로, 송신자가 자신의 비밀키로 암호화한 메시지를 수신자가 송신자의 공용 키로 해독하는 과정이다.

요구조건

1. **인증**(Authentication) : 정당한 서명자(서명자 개인 비밀키)만이 서명을 생성한다.
2. 위조 불가능성(**무결성**) : 위조할 수 없도록 한다.
3. 거부의 불가능성(**부인방지**) : 서명한 자가 서명 후에 서명 사실을 부인 못 하게 한다.
4. 재사용 불가능성(**유일성**) : 다른 문서의 서명으로 대치하는 행위를 못 하게 한다.
5. **진위확인**의 용이성 : 서명의 진위를 누구든 쉽게 확인한다.

이점

1. **무결성 보장** : 이론적으로 보았을 때, 전송되는 데이터를 해커가 보지 않아도 변경을 할 수 있지만 디지털 서명이 있는 데이터의 경우 이러한 상황이 발생이 된다면 서명이 무효가 되어 암호화가 된 디지털 서명 데이터는 위, 변조가 되었는지 확인을 할 수 있어 안전하다.
2. **개인의 신원 보호** : 디지털 서명의 소유권은 특정 사용자에게 구속력을 가지고 있어 원하는 사람과 의사소통을 하고 있는지 확인이 가능하다.
3. **개인 키가 개별 사용자와 연결** : 디지털 서명에 부인 방지의 품질을 부여한다. 이것은 데이터에 서명한 개인 키가 그 소유자가 아닌 다른 사람에 의해 손상되거나, 사용될 일이 없다는 것이다.

RSA키 생성

1. 서로 다른 큰 소수 p, q 를 선택한다. ($p \times q$)
2. $N = p \times q$ 를 계산한다.
3. $\varphi(N) = (p - 1) \times (q - 1)$ 을 계산한다.
4. $\varphi(N)$ 보다 작고, $\varphi(N)$ 와 서로소인 자연수 e 를 선택한다.
($\gcd(e, \varphi(N))=1, 1 < e < \varphi(N)$ 인 e 선택)
5. $d \times e$ 를 $\varphi(N)$ 로 나누었을 때 나머지가 1인 정수 d 를 구한다.
($de = 1 \bmod \varphi(N)$), 유클리드 호제법 이용
6. 공개 키 = $\langle e, N \rangle$, 개인 키 = $\langle d, N \rangle$ 이 된다.

RSA키 생성 예시

1. 두 개의 소수 p, q 를 정한다.
2. 두 소수의 곱을 N 으로 한다. ($N = pq$)
3. N 의 오일러 피 함수 값을 계산한다.

$\varphi(N)$: N 이하의 자연수 중에서
 N 과 서로소인 수의 갯수

$$N=pq \text{ (} p, q \text{는 소수)}$$
$$\varphi(N) = (p-1)(q-1)$$

4. 다음을 만족하는 수를 e 로 한다.
 $\varphi(N)$ 보다 작고, $\varphi(N)$ 과 서로소인 자연수
5. 다음을 만족하는 수를 d 로 한다.
 ed 를 $\varphi(N)$ 으로 나누었을 때,
나머지가 1이 된다.

1. $p=3, q=11$
 2. $N = 33$
 3. $\varphi(N)=(3-1) \times (11-1)=20$
 4. $e = 3$
 5. $ed/\varphi(N) \cdots 1 = 3d/20 \cdots 1$
즉, $3d = 20k + 1$
 6. $d = 7$
- 공개키 $\langle 33, 3 \rangle$
개인키 $\langle 33, 7 \rangle$

RSA키 암호·복호화

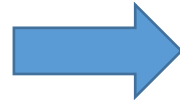
공개키 <33, 3>

개인키 <33, 7>

원문 7

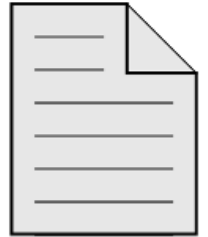


7



암호화

$$7^3 = 343 \text{ mod } 33 = 13$$



Data



복호화

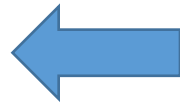
$$13^7 = 62\,748\,517 \text{ mod } 33 = 7$$

1. 발신자 원문 공개 키로 암호화
2. 암호 문 송신
3. 수신자 원문 개인 키로 복호화

1. $7^3 \text{ mod } 33 = X$ ($X = 13$)
2. X 송신
3. $X^7 \text{ mod } 33 = Y$ ($Y = 7$)




7



전자서명의 생성과 검증

공개키 <33, 3>

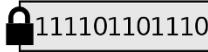
개인키 <33, 7>

원문 7 



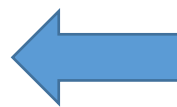
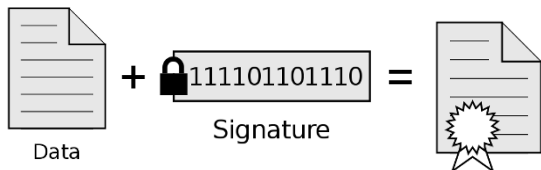
101100110101
Hash



서명 생성 
Signature
 $7^7 = 823\,543 \text{ mod } 33 =$
823543 28

1. 발신자 : 원문을 해시 함수로 해시화
2. 해시를 발신자 개인 키로 암호화하여 서명 생성
3. 수신자에게 원문 + 서명 전송
4. 수신자 : 서명 공개 키로 복호화
5. 원문을 해시 함수로 해시화 후 복호화 된 서명과 비교

1. $7^7 \text{ mod } 33 = X \text{ (} X = 13 \text{)}$
2. X 송신
3. $X^3 \text{ mod } 33 = Y \text{ (} Y = 7 \text{)}$



101100110101
Hash

Hash

=


101100110101
Hash

Hash

서명 검증

$21\,952 \text{ mod } 33 =$ $28^3 =$
7 21952



 111101101110
Signature



Data

Q & A