전자 서명

https://www.youtube.com/watch?v=o6jrjjar4vo

Contents

CryptoCraft LAB

전자서명과 보안서비스

- 보안 서비스

1. 기밀성(confidentiality): 정보를 비밀로 하는 것을 보장
2. 무결성(integrity): 메시지가 전송 중 변경되지 않았음을 보장
3. 메시지 인증(message authentication): 메시지의 송신자 신원을 보장
4. 부인불가(nonrepudiation): 메시지 송신자는 메시지 생성을 부인할 수 없음을 보장

전자 서명:
무결성, 메시지 인증, 부인 불가 제공

RSA

- 정수환 $Z_n = \{0,1,2,\ldots.n-1\}$ 에서 실행
  - 공개키: (N,e) => k_{pub}
  - 개인키:(N,d) => k_{pr}

  - 암호화: $y = e_{k_{pub}}(x) \equiv x^e \ mod \ n$
  - 복호화: $x = d_{k_{pr}}(y) \equiv y^d \ mod \ n$

RSA

$K_{pub} = (N, e)$ $K_{pr} = d$

$$\Phi(N) = \Pi_{i=1}^{n}\left(p_i^{e_i} - p_i^{e_i-1}\right)$$

Ex) $240 = 2^4 \times 3 \times 5$
$= p_1^{e_1} \times p_2^{e_2} \times p_3^{e_3}$

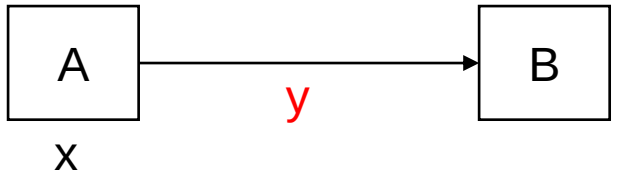
$\Phi(240)$
$= (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0)$

- 키 생성

① 두개의 소수 p & q 선택
② $N = p \times q$
③ $\Phi(N) = (p-1) \times (q-1)$
④ gcd(e, $\Phi(N)$) =1 => $\Phi(N)$와 서로소 관계인 e 선택
⑤ $d = e^{-1} \, mod \, \Phi(N) \Rightarrow \; d \times e \equiv 1 \, mod \, \Phi(N)$
=> d는 e의 역원

RSA

Ex)



$y = x^{e_B} \bmod N_B$

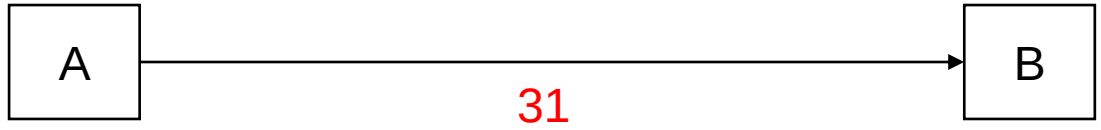
$y^{d_B} = (x^{e_B})^{d_B} \bmod N_B$
$= x^{e_B * d_B} \bmod N_B$

Bob

1. p =3 q=11
2. N= $p \times q = 33$
3. $\Phi(N) = (3-1) \times (11-1) = 20$
4. e = 3
5. d = $e^{-1} \equiv 7 \; mod \; 20$

$k_{pub_B} = (N_B, e_B) = (33, 3)$

$k_{pr_B} = d = 7$



전달할 메시지 x = 4

암호화: $y = 4^3 \equiv 31 \; mod \; 33$

복호화: $31^7 \equiv 4 \bmod 33$

RSA 전자서명

- 보내는 사람의 개인키로 서명(암호화) 한다.

Alice 가 Bob 한테 메시지를 보내려고함

d $= k_{pr_A}$ e$= k_{pub_A}$

$sig\ x \Rightarrow x^d mod\ n \Rightarrow s$

(x,s)

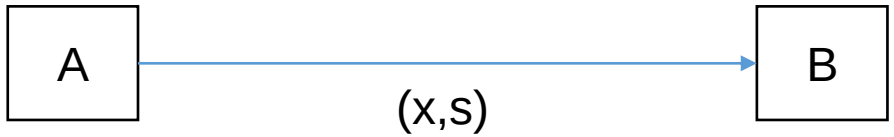
$s^e = \left(x^d\right)^e \equiv x'\ mod\ n$

$x' = x \Rightarrow true$

1. p =3 q=11
2. N= $p \times q = 33$
3. $\Phi(N) = (3-1) \times (11-1) = 20$
4. e = 3
5. d = $e^{-1} \equiv 7\ mod\ 20$

$k_{pub_A} = (N_A, e_A) = (33, 3)$

$k_{pr_A} = d = 7$



보낼 메시지 x=4

$s = x^d = 4^7 \equiv 16\ mod\ 33$

(x,s)=(4,16)

$16^3 \equiv 4\ mod\ 33$

(x')

x' =x 확인

DSA 전자서명

- Elgamal 전자서명 개량한 방식

키 생성
① 소수 p 선택
② p-1 의 약수 중 소수인 q 선택
③ $ord(\alpha) = q$인 원소 α 선택
④ 0<d<q 인 임의의 정수 d 선택
⑤ $\beta \equiv \alpha^d \ mod \ p$ 계산

$k_{pub} = (p, q, \alpha, B)$
$k_{pr} = (d)$

DSA 서명 생성
① $0<K_E<$ q 임시키 K_E 정수 선택
② $r \equiv (\alpha^{k_E} \ mod \ p) \ mod \ q$ 계산
③ $s \equiv (SHA(x) + d \times r)K_E^{-1} \ mod \ q$ 계산

DSA 서명 검증
1. $\omega \equiv s^{-1} \ mod \ q$ 계산
2. $u_1 \equiv \omega \times SHA(x) \ mod \ q$ 계산
3. $u_2 \equiv \omega \times r \ \ mod \ q$ 계산
4. $v \equiv (\alpha^{u_1} \times \beta^{u_2} \ mod \ p) \ \ mod \ q$ 계산

$v \equiv$ r mod q => 유효한 서명

DSA 전자서명

Alice

① p = 59 선택
② q = 29 선택
③ α = 3 선택
④ 개인키 d=7 선택
⑤ $\beta = \alpha^d = 3^7 \equiv 4 \mod 59$

(p,q, α, β) =(59,29,3,4)

서명
h(x) =26
1. 임시키 K_E = 10
2. $r = (3^{10} \bmod 59)$
   $\equiv 20 \ mod \ 29$
3. $s = (26 + 7 \times 20) \times 3$
   $\equiv 5 \ mod \ 29$

(x,(r,s)) = (x,(20,5))

Bob

검증
1. $\omega = 5^{-1} \equiv 6 \ mod \ 29$ 계산
2. $u_1 = 6 \times 26 \equiv 11 \ mod \ 29$ 계산
3. $u_2 = 6 \times 20 \equiv 4 \ mod \ 29$ 계산
4. $v \equiv (3^{11} \times 4^4 \ mod \ 59) \ mod \ 29$
   = 20
5. $v \equiv$ r mod 29 => 유효한 서명

전자서명 보안수준

- RSA : N은 1024bit~ 3072 bit
- DSA

p	q	해시 결과	보안 수준
1024	160	160	80
2048	224	224	112
3072	256	256	128

- 그 외 전자서명

  Elgamal algorithm , ECDSA algorithm
- 메시지 인증 코드 (Message Authentication Code,MAC)

  “부인불가” 제공 x

Q & A