Tutorial 7 ENG

27 October 2021 13:18

DIGITAL SIGNATURES

→ RSA Signatures

→ ElGamal Signatures

→ Subliminal channels

Digital signatures

Sign a message w

$Sig(w)$

$(w, Sig(w)) \xrightarrow{\text{impossible}} (w_1, Sig(w_1))$ hard to calculate

1.) Everyone is able to verify that the message was signed by the correct user → doable with public keys

2.) Only the correct user can sign messages → doable with private keys

RSA Signatures

Elements: p, q - large primes, $n = p \cdot q$, e, d

$e = d^{-1} \mod (p-1)(q-1)$

Private: d

Public: e, n

Signature of message w: $\mathrm{Sig}(w) = w^d \mod n$

Verification: $(w, \mathrm{sig}(w))$ check if $w = [\mathrm{sig}(w)]^e \mod n$

$= (w^d)^e \mod n$

$= w^{1 \mod \varphi(n)} \mod n$

$= w \mod n$

How to fake a signature?

1.) Factorize n $\updownarrow$
2.) Calculate $\varphi(n)$
3.) Invert e (RSA problem)
4.) From w, $w^d \mod n$
calculate d $\to$ discrete log problem

all computationally hard

How to break a signature scheme

Existential forgery: There exists a message w for which calculating $\mathrm{Sig}(w)$ is easy. In RSA what is $\mathrm{Sig}(1)$?

Universal forgery: All messages can be efficiently signed by the adversary.

RSA existential forgeries

Given pair (w, s) of a message and it's signature, can you find another (w', s') pair?

(w^2, s^2) is a valid signature of w^3

Given pair (w, s) of a message and it's signature, can you find another (w', s') pair?

(w^2, s^2) is a valid signature of w^3

(w_1, s_1) and (w_2, s_2) are valid $\Rightarrow$ $(w_1 w_2, s_1 s_2)$

Hash functions

$h: I \to K$ $\quad |I| >> |k| \approx 320$-bit number

1.) It is computationally hard to invert h: $k \in K$ it is hard to find $i \in I$ s.t. $h(i) \to k$

2.) It is computationally hard to find collisions: it is computationally hard to find $i_1, i_2 \in I$ s.t. $h(i_1) = h(i_2)$.

$$\boxed{w,\ h(w),\ sig(h(w))}$$

1.) Advantage 1: signatures are always calculated for small messages (320-bits)

2.) $\boxed{w,\ h(w),\ sig(h(w))}$

$\boxed{w',\ h(w)^2,\ sig(h(w))^2}$ $\to$ it is computationally difficult to calculate w', s.t. $h(w') = h(w)^2$

ElGamal signatures

Elements: p - a large prime

q - a primitive element of $\mathbb{Z}_p^*$ $\quad \mathbb{Z}_p^* = (1, \dots, p-1) = (q, q^2, q^3, \dots, q^{p-1})$

x - $0 < x < p-1$

$y = q^x \bmod p$

Public: g, q, p

Private: x

To sign w: 1.) choose randomly $r \in \mathbb{Z}_{p-1}^{*}$

All numbers invertible mod $p-1$
$\Updownarrow$
all numbers r smaller than $p-1$ with
$\gcd(r, p-1) = 1$

2.) $a = q^{r} \mod p$

3.) $b = r^{-1} \cdot (w - a \cdot x) \; \boxed{\mod p-1}$

inverse of r mod $(p-1)$

Verification of $(w, (a,b))$

$$q^{w} \overset{?}{\equiv} g^{a} \cdot a^{b} \mod p$$

$$\equiv (q^{x})^{a} \cdot (q^{r})^{b} \mod p$$

$$\equiv q^{xa} \cdot q^{\overbrace{r \cdot (r^{-1}}^{=1 \mod (p-1)} (w - a \cdot x))}$$

$$\equiv \cancel{q^{xa}} \cdot q^{w} \cdot \cancel{q^{-xa}} \mod p$$

$$\equiv q^{w} \mod p$$

Elgamal Existential Forgeries

1.) There is an existential forgery which doesn't require a message-signature pair.

Two parameter family $\alpha, \beta \in \mathbb{Z}_{p-1}^{*}$

$a = q^{\alpha} \cdot g^{\beta}$, $b = -a \cdot \beta^{-1} \mod p-1$, $\boxed{w = \alpha \cdot b}$

$$g^{a} \cdot a^{b} \equiv \quad q^{\alpha} \cdot g^{\beta} \quad -a \cdot \beta^{-1} \quad \mod p$$

$$y^a \cdot a^b \equiv g^{q^\alpha \cdot y^\beta} \cdot (q^\alpha \cdot y^\beta)^{-a \cdot \beta^{-1}} \mod p$$

$$\equiv g^{q^\alpha \cdot y^\beta} \cdot (q^\alpha \cdot y^\beta)^{-q^\alpha \cdot y^\beta \cdot \beta^{-1}}$$

$$\equiv \cancel{g^{q^\alpha \cdot y^\beta}} \cdot \cancel{g^{-\cancel{\beta} \cdot q^\alpha \cdot y^\beta \cdot \cancel{\beta^{-1}}}} \cdot q^{-\alpha \cdot q^\alpha \cdot y^\beta \cdot \beta^{-1}}$$

$$\equiv q^{\alpha \cdot \underbrace{-\underbrace{q^\alpha \cdot y^\beta}_{a} \cdot \beta^{-1}}_{b}}$$

$$\equiv q^{\alpha \cdot \beta} \equiv q^w \mod p$$

2. Given $(w, (a,b))$ it is possible to find a signature of $w' = \alpha(w - \beta \cdot b) \mod (p-1)$

$\rightarrow$ 2 used r's are the same

3. (w_1, a, b_1) and (w_2, a, b_2) allows to calculate x and thus break the signature scheme.

$b_1 = r^{-1}(w_1 - ax) \mod (p-1)$

$b_2 = r^{-1}(w_2 - ax) \mod (p-1)$

Which x is the correct one?

$g^x \equiv y \mod p$

$r b_1 = W_1 - ax \mod (p-1)$

$r b_2 = W_2 - ax \mod (p-1)$

giving you r how to calculate x?

---

how generally solve this?

$$r(b_1-b_2) \equiv (w_1-w_2) \mod (p-1)$$

how generally solve this? (because (b_1-b_2) might not be invertible mod $(p-1)$)

which of possible r's are correct? the one for which $a^r \equiv a \mod p$

$$\boxed{ax \equiv b \mod n}$$

→ n is not necessarily a prime

1.) $gcd(a,n)=1 \Rightarrow a^{-1}$ exists and $x \equiv b \cdot a^{-1} \mod n$

2.) $gcd(a,n)=k \wedge k$ does not divide $b \Rightarrow$ No solution

3.) $gcd(a,n)=k \wedge k \mid b$ (k divides b) ⇒ there are multiple solutions

Algorithm: Solve

$$\boxed{\frac{a}{k}x \equiv \frac{b}{k} \mod \frac{n}{k}}$$

Note $GCD(\frac{a}{k}, \frac{n}{k})=1$

Solution: $x=s$

Solutions to the original problem are

$$s+i\cdot\frac{n}{k} \text{ for } i\in\{0,1,\dots,k-1\}$$

Example $\boxed{10x \equiv 5} \mod 15$ $k = gcd(10,15)=5$

1.) $2x \equiv 1 \mod 3$

$x \equiv 2$

2. Solutions are:

$2+i\cdot 3$ for $i\in\{0,1,2,3,4\}$

$x \in \{2, 5, 8, 11, 14\}$

SUBLIMINAL CHANNELS

Note that ElGamal (DSA, OSS) use two random numbers to calculate signatures: random $\bar{r}$

random x

if x is shared with another user, r can be used to send a secret message.

$a = g^r \bmod p$

$b = \boxed{r^{-1}} (w - a x) \bmod p-1$

$\boxed{(w, (a, b))}$

$r \cdot b = (\boxed{w} - a x) \bmod p-1$

if receiver knows x as well they can calculate r.