Tutorial VII

20 November 2020 16:00

DIGITAL SIGNATURES

↳ RSA Signatures

↳ El Gamal Signatures

↳ Subliminal channels

Digital signatures

Sign a message w

$Sig(w)$

$(w, Sig(w)) \overset{\text{impossible}}{\rightsquigarrow} (w_1, Sig(w_1))$

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

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

RSA signatures

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

$e = d^{-1} \bmod \varphi(n)$ → Euler's totient function

$\varphi(n) = (p-1)(q-1)$

Private: $d, (p, q)$

Public: e, n

Signature of message w: $Sig(w) = w^d \bmod n$

Verification of $(w, Sig(w))$ check if $w = \{Sig(w)\}^e \bmod n$

$= (w^d)^e$

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

$= w \bmod n$

How to fake a signature?

1.) Factorize n

2.) Calculate $\varphi(n)$

3.) Invert e (RSA problem)

4.) From w, $w^d \bmod n$ Calculate d (discrete logarithm problem)

$\Big\}$ All (computationally) hard

4.) From w, $w^d \bmod n$
Calculate d (discrete logarithm problem!)

How to break a signature scheme

Existential forgery: There exists a message w for which signatures are easy to calculate

Universal forgery: All messages can be signed efficiently by the adversary (recovering the private key is possible

RSA existential forgery

Given valid pair (w, s) we can create more valid pairs.

(w^2, s^2)

$Sig(w^2) = (w^2)^d = (w^d)^2 = (s)^2 \mod n$

(w_1, s_1) (w_2, s_2)

$(w_1 w_2, s_1 s_2)$

$Sig(w_1 w_2) = w_1^d w_2^d = s_1 s_2 \mod n$

Hash functions

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

Cryptographic hash function

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

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

$[w, h(w), Sig(h(w))]$

1. Advantage $\rightsquigarrow$ signatures need to be calculated only for small messages (320-bit)

2. Advantage $\rightsquigarrow$

$[w, h(w), Sig(h(w))]$

$[w?, h(w)^2, Sig(h(w)^2)]$

In order to use the existential forgery described above, the adversary needs to find w' s.t. $h(w') = h(w)^2$.

In order to use the existential forgery described above, the adversary needs to find w_i s.t. $h(w_i) = h(w)$.
This is computationally hard, because h is a cryptographic hash function (and it cannot be inverted).

El Gamal signatures

Elements: p – a large prime

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

x – $0 < x < p-1$

$y = q^x \bmod p$

Public: y, q, p

Private: x

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

→ multiplicative group mod $(p-1)$

$r^{-1} \bmod p-1$ exists, $\gcd(r, p-1) = 1$

2.) $a = q^r \bmod p$

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

inverse of r mod $(p-1)$

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

$$q^w \stackrel{?}{\equiv} y^a \cdot a^b \mod p$$

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

$$\equiv (q^x)^a \, q^{\underbrace{r \cdot r^{-1}}_{1 \bmod (p-1)} \cdot (w - ax)} \mod p$$

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

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

Vulnerabilities of El Gamal signatures

Ex 7.19

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

$a = q^\alpha \cdot y^\beta$, $b = -a \cdot \beta^{-1} \bmod p-1$, $w = \alpha \cdot b$

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

$$\gamma^{a} a^{b} \equiv \gamma_{\delta}^{q^{\lambda} \cdot \gamma^{\beta}} \cdot \left(q^{\alpha} \gamma^{\beta}\right)^{-q^{\alpha} \gamma^{\beta} \cdot \beta^{-1}}$$

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

$$\equiv q^{\alpha \cdot b}$$

$$\equiv q^{\lambda \cdot b}$$

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

3.) $(w_1, \overset{\gamma}{a}, b_1)$ and $(w_2, \overset{\gamma}{a}, b_2)$ $\quad \gamma \quad q^r \bmod p$ (ex. 7.6)

allows to calculate x.

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

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

$$r b_1 = (w_1 - ax) \quad \bmod p-1$$

$$r b_2 = (w_2 - ax) \quad \bmod p-1$$

$$r(b_1 - b_2) \equiv w_1 - ax - w_2 + ax \quad \bmod (p-1)$$

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

This generally has $\gcd(b_1 - b_2, p-1)$ & the correct solution recover s $q^r = a \bmod p$

$$ax \equiv b \quad \bmod n$$

n → not necessarily a prime

1.) $\gcd(a, n) = 1 \Rightarrow a^{-1}$ exists and the solution is

$$x \equiv b a^{-1} \bmod n$$

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

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

Algorithm: Solve

$$\frac{a}{k} x \equiv \frac{b}{k} \mod \frac{n}{k} \qquad \text{NOTE } GCD\left(\frac{a}{k}, \frac{n}{k}\right) = 1$$

Solution $x = s$

Solutions to the original problem:

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

Example:

$$10x \equiv 5 \mod 15 \qquad k = \gcd(10, 15) = 5$$

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

$x \equiv 2$

2.) Solutions are

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

$x \in \{2, 5, 8, 11, 14\}$ ✓

SUBLIMINAL CHANNELS

Note that El Gamal (DSA, OSS) use two random numbers HW
to calculate the signatures: random r

to calculate the signatures : random r

random x

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

$$b = r^{-1}(w - ax) \mod p-1 \qquad (w, (a,b), x)$$

$$r\underset{\downarrow}{b} = (w - a\underset{\downarrow}{x}) \mod p-1$$

solve for r can have $\gcd(b, p-1)$ solutions

the secret message fullfils $q^r \equiv a \mod p$.