Tutorial 7 SK

27 October 2021 18:00

DIGITÁLNE PODPISY

- RSA podpisom
- ElGamal podpisom
  - existenciálnych útokoch
  - Subliminálnym kanálom

Digitálne podpisy

Podpis správy w závisí na samotnej správe

$Sig(w)$

$(w, Sig(w)) \xrightarrow{\text{Výpočtovo ťažké}} (w_1, Sig(w_1))$

1.) Verifikovať podpis dokáže každý užívateľ s verejným kľúčom

2.) Podpisovať dokumenty dokáže len užívateľ s tajným kľúčom

RSA podpis

Základné prvky: p, q – dve veľké prvočísla

$$n = p.q$$

$$e, d : e \equiv d^{-1} \mod \varphi(n)$$

$$\mod (p-1)(q-1)$$

tajný kľúč: d

verejný kľúč: e, n

Verejný kľúč: e, n

Podpis správy: w je $Sig(w) = w^d \bmod n$

$(w, Sig(w))$

Overenie podpisu: $Sig(w)^e \bmod n \overset{?}{=} w \bmod n$

$(w^d)^e \bmod n$

$w^{d \cdot e} \overset{= 1 \bmod \varphi(n)}{\bmod n}$

$w \bmod n$

Ako nafalšovať podpis?

1.) Faktorizácia n ☹
2.) Spočítať $\varphi(n)$
3.) spočítať inverziu $e \bmod \varphi(n)$ (RSA problém)
4.) $(w, w^d \bmod n) \rightsquigarrow$ spočítať d z w a $Sig(w)$
(problém diskrétneho logaritmu)

Aké typy útokov existujú?

Univerzálne falšovanie: útočník dokáže podpísať ľubovoľnú správu

Existenciálne falšovanie: Existuje správa (množina správ), pre ktorú je jednoducho spočítať podpis.

RSA - existenciálne falšovanie:

Až má útočník platný podpis $(w, Sig(w))$ dokáže spočítať iné platné podpisy?

$(w^k, Sig(w)^k)$ pre ľubovoľné k je tiež platný podpis

Až $(w_1, Sig(w_1))$ a $(w_2, Sig(w_2))$ sú platné podpisy, potom $(w_1 w_2, Sig(w_1) Sig(w_2))$ je tiež platný podpis.

Hash funkcie

$h: I \to K \quad |I| >> |K| \quad (320\text{-bitové } |K|)$

1.) je ťažké otočiť funkciu h: ak viem $k \in K$, je ťažké spočítať $i \in I$ t.ž. $h(i) = k$.

-> 2.) je ťažké nájsť kolízie, $i_1, i_2 \in I$ t.ž. $h(i_1) = h(i_2)$

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

1.) podpis sa počíta zo správy fixnej veľkosti

2.) Stačí existenciálne útok

$$\{w, h(w), Sig(h(w))\} \stackrel{?}{=} \{w_2, \underbrace{h(w)}_{h(w_2)}, Sig(h(w))\}$$

$[w', h(w)^2, sig^2(h(w))]$ Najít w' t.ž. $h(w') = h(w)$

El Gamal signatures

Základní prvky: p – velké prvočíslo

q – primitivní prvek

x – $0 < x < p-1$

$y = q^x \bmod p$

$\mathbb{Z}_p^*$ multiplikativní grupa mod p

$\mathbb{Z}_p^* = \{1, \dots, p-1\} = \{q, q^2, q^3, \dots, q^{p-1}\}$

Veřejný klíč: y, q, p

tajný klíč: x

Podpis správy w:

1.) Náhodně zvol $r \in \mathbb{Z}_{p-1}^*$ (čísla invertibilní mod $p-1$ ⇕ r t.č. $\gcd(r, p-1) = 1$)

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

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

Verifikační $(w, (a,b))$:

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

$$= (q^x)^a \cdot a^{r \cdot b} \bmod p$$

$$\equiv (g^x)^a \, g^{r \cdot b} \pmod p$$

$r \equiv 1 \pmod{(p-1)}$

$$\equiv g^{x \cdot a \; (r \cdot r^{-1})(w - ax)} \pmod p$$

$$\equiv g^w \pmod p$$

Zranitelnosti a existenciálne falšovanie ElGamal podpisu

1.) Existenciálne falšovanie bez znalosti platného podpisu (w, a, b)

Rodina platných podpisov parametrizovaná α, β

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

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

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

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

2.) Platná trojica $(w, (a, b))$ umožňuje nájsť podpis správy

$$w' = \alpha (w - \beta \cdot b) \bmod p-1$$ pomocou r!

3.) z podpisov (w_1, a, b_1) a (w_2, a, b_2)

5.) + príklady (w_1, a, b_1) a (w_2, a, b_2)

Sa dá spočítať x.

$a_2 = (a_1^3)$

$a_2 = a^{3r}\ a_1 = a^r \mod p$

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

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

$r.b_1 \equiv (w_1 - ax) \mod (p-1) \Rightarrow$

$r.b_2 \equiv (w_2 - ax) \mod (p-1)$

$r.b_1 - w_1 \equiv -ax$

má $\gcd(p-1, p-1-a)$ riešení

správne dá $a^r = 5 \mod p$

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

⚠ Vo všeobecnosti má veľa riešení ($\gcd(p-1, b_1 - b_2)$)

Správne dáva $a^r = a \mod p$

$ax \equiv b \mod n$, kde n nie je prvočíslo

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

2.) $\gcd(a, n) = k \wedge k$ nedelí $b \Rightarrow$ Nexistuje riešenie

3.) $\gcd(a, n) = k \wedge k \mid b \Rightarrow$ existuje riešenie

Spočítaj $\frac{a}{k} x \equiv \frac{b}{k} \mod \frac{n}{k}$ $\gcd\left(\frac{a}{k}, \frac{n}{k}\right) = 1$

Ak je Riešenie $x \equiv s$

Riešenie pôvodného problému je $s + i \cdot \frac{n}{k}$ pre $i \in \{0, \dots, k-1\}$

Príklad: $10x \equiv 5 \mod 15$ $\quad \gcd(10, 15) = 5$

$2x \equiv 1 \mod 3$

$x \equiv 2$

$x = 2 + i \cdot 3 \quad i \in \{0, \dots, 4\}$

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

Subliminálny komunikačný kanál

Mnohé podpisové schémy (El Gamal, DSA, OSS) používajú dve tajné čísla: náhodné r
náhodné x

Až Alica a Bob zdieľajú x, dá sa r použiť na komunikáciu. [w, (a, b)]

r nie je náhodné ale obsahuje správu

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