Kryptografické systémy
digitálny podpis

doc. RNDr. Jozef Jirásek, PhD.

ZS 2023

Bezpečnostné ciele budovania informačnej bezpečnosti

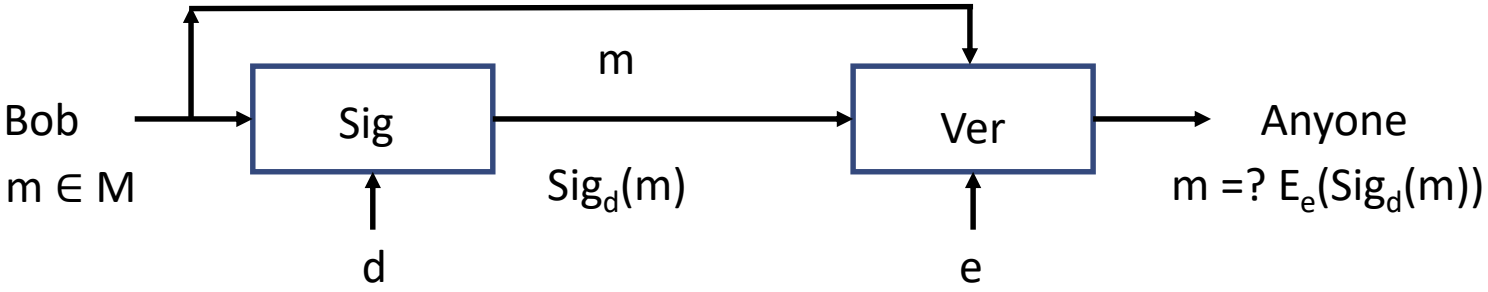
bezpečnostné ciele, dosahované použitím kryptografických systémov a bezpečnostných mechanizmov (ISO/IEC 27000)

- dôvernosť (data confidentiality) = šifrovanie (asymetrická, symetrická kryptografia, blokové, prúdové šifry)
  - dôvernosť spojenia, jednotlivého bloku, časti správy, toku dát
- celistvosť (data integrity) = integritné schémy (MDC funkcie)
  - možnosť opravy, integrita časti správ, detekcia zámeny (replay)
- pôvodnosť (data authentication) = autentifikačné postupy (MAC funkcie)
  - pôvodnosť zdroja, identita komunikujúcich
- nepopierateľosť (nonrepudiation) = digitálne podpisovacie schémy (asymetrická, symetrická kryptografia, MAC, MDC)
  - nepopierateľnosť odosielateľa, príjemcu

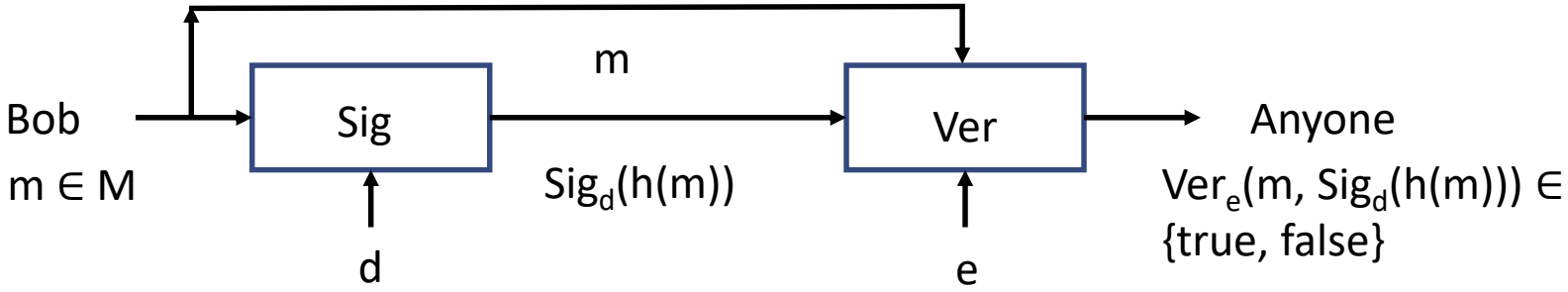
Digitálne podpisovacie schémy

- nepopierateľnosť pôvodcu správy –
  správa zviazaná s nepopierateľným dôkazom vlastníctva súkromného tajomstva odosielateľa
- pôvodca správy – osoba, systém, hw so súkromným kľúčom
- podpisovací algoritmus $Sig_d(m)$ (zviazanie správy so súkromným kľúčom – môže urobiť len vlastník kľúča)
- verifikačný algoritmus $Ver_e(m, Sig_d(m))$ (overenie správnosti podpisu pomocou verejného kľúča, správy a jej podpisu)
- na digitálny podpis je možné využiť kľúče a čiastočne aj postupy šifrovania asymetrickej kryptografie
- je nebezpečné používať tie isté kľúče súčasne na podpisovanie aj na šifrovanie !

Digitálne podpisovacie schémy



- schéma s dešifrovaním (len pre krátke správy s redundanciou) šifrovanie súkromným kľúčom nie je dôverné !



- schéma s apendixom (k správe sa pripojí jej podpísaný haš – silná CRF MDC funkcia)

RSA podpisovacia schéma

- $n = p \cdot q$,
  e : $\gcd(e,(p-1)(q-1)) = 1$ $\quad$ d : $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$
- s dešifrovaním $\mathrm{Sig}_d(m) = m^d \bmod n$
  $\mathrm{Ver}_e(m, \mathrm{Sig}_d(m)) = m \stackrel{?}{=} (\mathrm{Sig}_d(m)^e \bmod n)$

- falšované náhodné správy so správnym podpisom
  k náhodnému podpisu s vypočíta útočník správu $m = s^e \bmod n$
  $\mathrm{Ver}_e(m, s) = m \stackrel{?}{=} (s^e \bmod n)$ – čo je stále pravda
- falšovanie využitím homomorfnej vlastnosti RSA
- upraviť správy, aby sa falšovanie dalo odhaliť – odolnosť proti EUF-CMA (existential unforgeability – chosen message attack)

RSA podpisovacia schéma s apendixom

- $n = p \cdot q$,
  e : $\gcd(e,(p-1)(q-1)) = 1$ $\quad$ $d : e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$
- s MDC funkciou $\quad Sig_d(m) = h(m)^d \bmod n$
  $Ver_e(m, Sig_d(m)) = h(m) =? (Sig_d(m)^e \bmod n)$

- správy ľubovoľnej dĺžky (podpisuje sa len haš)
- MDC musí byť silná CRF
- väčšinou býva haš menší ako kryptografický blok -> padding + randomizácia + proti falšovaným utokom (podobne ako OEAP pre šifrovanie)

RSA výplň pre podpis

- PKCS #1 v 1.5

H(m) = 0x00 | 0x01 | 0xff | . . . | 0xff | 0x00 | h(m)

- PSS (Probabilistic Signature Scheme) PKCS #1 v 2.1

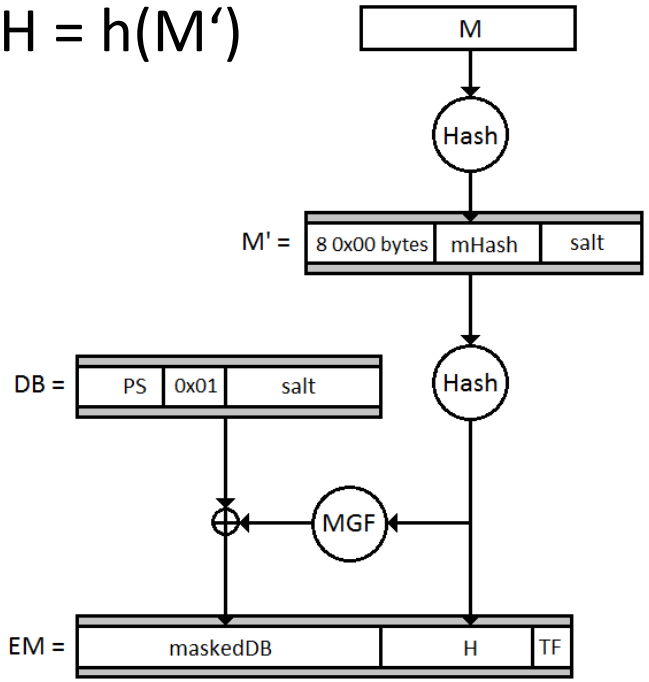
salt – náhodné bity, mHash = h(M), H = h(M‘)

PS – padding 0x00 | ... | 0x00

MGF – mask generation function (ako v OAEP)

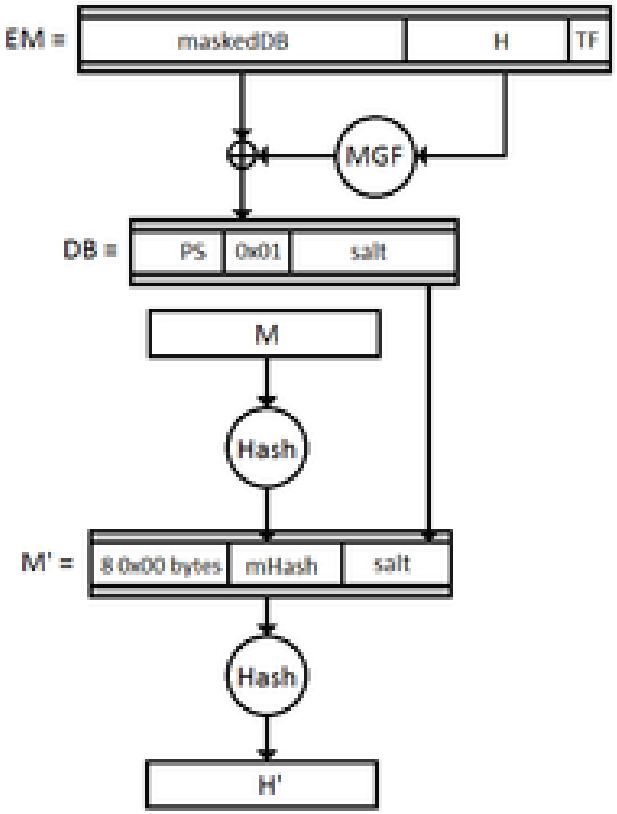
TF – 0xbc, |EM|< n

EMSA (encoding method for signature with appendix)



Verifikácia RSA-PSS

- $Sig_d(m)^e \bmod n = EM$
- EM => maskedDB | H | 0xbc
- DB = maskedDB ⊕ MGF(H)
- DB => padding | 0x01 | salt
- H =? Hash($(0x00)^8$ | h(M) | salt)



OAEP (Optimal Asymmetric Encryption Padding)

k-bitový blok (2048 b)

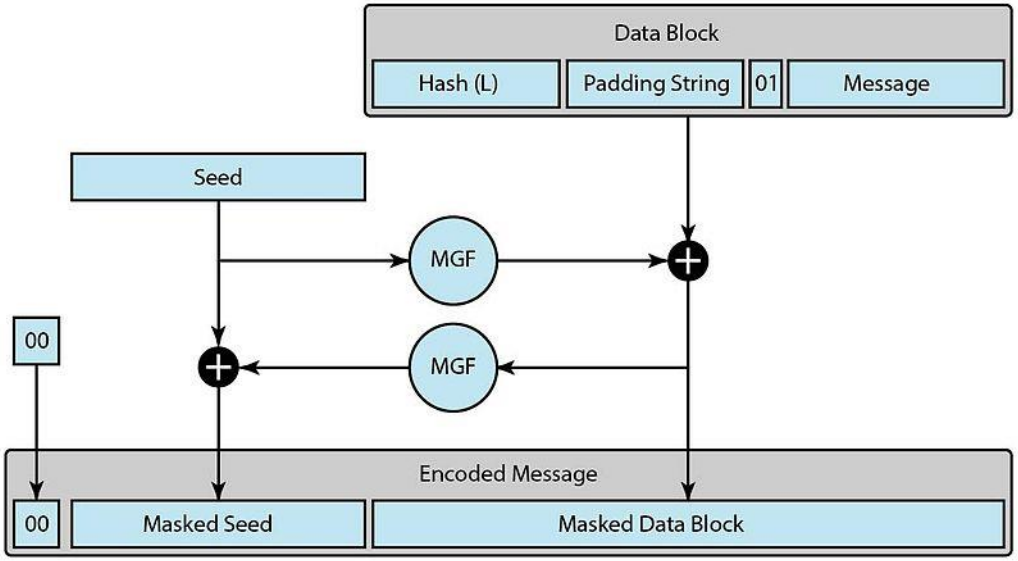
$|m| = 160\ (256)$ b

L – label (nemusí byť)

$|seed| = |Hash(L)| = h$

2 Feistelove rundy

$MGF_h: \{0,1\}^{k-h-1} \rightarrow \{0,1\}^h$



$MGF_{k-h-1}: \{0,1\}^h \rightarrow \{0,1\}^{k-h-1}$ funkcie na generovanie masky

PS – reťazec $k - |m| - 2 \cdot h - 2$ nulových bajtov 0x00

$DB = Hash(L) \mid PS \mid 0x01 \mid m$

$EM = 0x00 \mid seed \oplus MGF_h(DB \oplus MGF_{k-h-1}(seed)) \mid$
$\quad \mid (DB \oplus MGF_{k-h-1}(seed))$

Slepý podpis

- Bob chce potvrdiť od Alice, že vytvoril dokument, ale nechce, aby sa oboznámila s jeho obsahom
- zvolí náhodné k (gcd(k,n)=1) a nechá Alici podpísať správu $t = k^e m \bmod n$
- ak Alica podpíše - $s = t^d \bmod n = k^{ed} m^d \bmod n = k m^d \bmod n$
- Bob získa správu podpísanú Alicou pomocou k^{-1} (mod n) $k^{-1} s \bmod n = k^{-1} k m^d \bmod n = m^d \bmod n$

Podpisovacia schéma ElGamal

- p – prvočíslo, g - generátor grupy $\mathbb{Z}_p^*$
  d ∈ {2, ..., p-2} , e = g^d mod p
- E(m) = (r, s) ... na dešifrovanie potrebujem dvojicu – nemožno podpísať dešifrovaním, tak ako v RSA schéme
- náhodné (vždy iné!) k ∈ $\mathbb{Z}_{p-1}$: gcd(k, p-1) = 1

$$Sig_d(m) = (r, s) = (g^k \bmod p, (h(m) - d \cdot r)\, k^{-1} \bmod (p-1))$$

$$Ver_e(m, (r, s)) = e^r r^s \bmod p \stackrel{?}{=} g^{h(m)} \bmod p$$

(dk: $e^r r^s \equiv g^{dr} \cdot g^{ks} \equiv g^{dr+ks} \stackrel{?}{\equiv} g^{h(m)} \pmod p$
v exponente $h(m) \equiv dr + ks \pmod{(p-1)}$ podľa FLT)

- ak by sa m nehašovala – hrozí opäť posielanie falošných správne podpísaných dát (existential forgery attack)

DSA - Digital Signature Algorithm

NIST štandard pre digitálny podpis (DSS) FIPS 186-4

- p – prvočíslo s prvočíselným faktorom q čísla (p-1) (napr. |p|=1024, |q|=160)
- $h \in \mathbb{Z}_{p-1}$ také, že $g = h^{(p-1)/q} > 1$ (potom ord(g)=q)
- súkromný kľúč $d \in \{2, ..., q-2\}$
  verejný kľúč $(p, q, g, e = g^d \bmod p)$
- náhodné (vždy iné!) $k \in \mathbb{Z}_{q-1}$
  $Sig_d(m) = (r, s) = ((g^k \bmod p) \bmod q, (h(m) + d \cdot r)\, k^{-1} \bmod q)$

  $sinv = s^{-1} \bmod q$, $u1 = h(m) \cdot sinv \bmod q$, $u2 = r \cdot sinv \bmod q$
  $Ver_e(m, (r, s)) = (g^{u1}\, e^{u2} \bmod p) \bmod q =? r$

  (dk: $(g^{u1}\, e^{u2} \bmod p) \bmod q = (g^{(h(m)+dr)sinv} \bmod p) \bmod q =$
  $= (g^k \bmod p) \bmod q = r$)

DSA - Digital Signature Algorithm

$Sig_d(m) = (r, s) = ((g^k \bmod p) \bmod q, (h(m) + d \cdot r)\, k^{-1} \bmod q)$

$Ver_e(m, (r, s)) = (g^{u1}\, e^{u2} \bmod p) \bmod q =? r$
(pre $u1 = h(m) \cdot s^{-1} \bmod q$, $u2 = r \cdot s^{-1} \bmod q$)

Príklad : pre $h(m) = 26$

- $p = 59$, $q = 29$, $g = 3$, $d = 7$, $e = 3^7 \bmod 59 = 4$
- $k = 10$, $k^{-1} \bmod 29 = 3$, $r = (3^{10} \bmod 59) \bmod 29 = 49 \bmod 29 = 20$
  $Sig_7(m) = (r, s) = (20, (26 + 7 \cdot 20) \cdot 3 \bmod 29) = (20, 5)$
- $5^{-1} \bmod 29 = 6$, $u1 = 26 \cdot 6 \bmod 29 = 11$, $u2 = 20 \cdot 6 \bmod 29 = 4$
  $(3^{11} \cdot 4^4 \bmod 59) \bmod 29 = 49 \bmod 29 = 20 =? 20$ => valid

DSA bezpečnosť

- 2x riešenie DLP problému
  $e = g^d \bmod p$ (útoky z teórie čísel)
  výpočty a hašovanie v podgrupe mod q (narodeninový útok)

p	q	|h(m)|	security
1024	160	160	80
2048	224	224	112
3072	256	256	128

- výhodné výpočty v menšom module, krátky podpis, možno predkalkulovať k a k^{-1}
- hrozba predikovateľnosti resp. viacnásobného použitia k

ECDSA – Elliptic Curve Digital Signature Alg.

- využitie EC kryptografie FIPS 186-5
- (E, +) , generátor G ∈ E podgrupy ord(G) = q prvočíslo
- súkromný kľúč $d \in \mathbb{Z}_q$, verejný kľúč E, q, G, Y = dG
- náhodné $k \in \mathbb{Z}_q$, R = kG, $|h(m)| \geq |q|$
  $Sig_d(m) = (r, s) = (R_x \bmod q, (h(m) + d \cdot r)\, k^{-1} \bmod q)$
- $u_1 = h(m) \cdot s^{-1} \bmod q$, $u_2 = r \cdot s^{-1} \bmod q$

  $Ver_Y(m, (r, s)) = ((u_1 G + u_2 Y)_x \bmod q) \stackrel{?}{=} r$

ECDSA bezpečnosť

- riešenie ECDLP problému - $\approx \sqrt{q}$
- výpočty nad E mod p p ≈ q

q	|h(m)|	security
192	192	96
224	224	112
256	256	128
384	384	192
512	512	256

Schnorrov digitálny podpis

- DSA parametre p, q (p=qt+1), g (ord(g)=q), h: $\{0,1\}^* \to \mathbb{Z}_q$
- súkromný kľúč d ∈ {2, ..., q-2}
  verejný kľúč (p, q, g, e = g^d mod p)
- náhodné (vždy iné!) k ∈ $\mathbb{Z}_q$
  $Sig_d(m) = (r, s) = (h(m \mid (g^k \bmod p)), (k + d \cdot r) \bmod q)$
- $Ver_e(m, (r, s)) = h(m \mid g^s e^{-r} \bmod p) =? r$

  (dk: $g^s e^{-r} \equiv g^{k+dr} \cdot g^{-dr} \equiv g^k \pmod p$)

- EUF-CMA odolná (dokázateľne výpočtovo ekvivalentná DLP)
- EdDSA – Edwards Curve Digital Signature Algorithm – RFC 8032
  Ed25519 = EdDSA + Curve25519 + SHA256

Elektronický podpis

- využitie mechanizmov digitálneho podpisu na dosiahnutie nepopierateľnosti
- kvalifikovaný elektronický podpis (KEP) – umožní realizovať právne úkony, ktoré vyžadujú písomnú formu – nahrádza písomnú podobu vlastnoručného podpisu
  - autenticita – možnosť overenia identity zhotoviteľa podpisu
  - integrita – po podpísaní nedošlo k zmene obsahu dokumentu
  - nepopierateľnosť – zhotoviteľ nemôže poprieť autorstvo
- KEP – musí byť vyhotovený na kvalifikovanom zariadení s kvalifikovaným certifikátom (na podpis sa môže využiť súkromný kľúč z občianskeho preukazu s platným kvalifikovaným certifikátom)

OTS - Jednorazová podpisovacia schéma (Lamport)

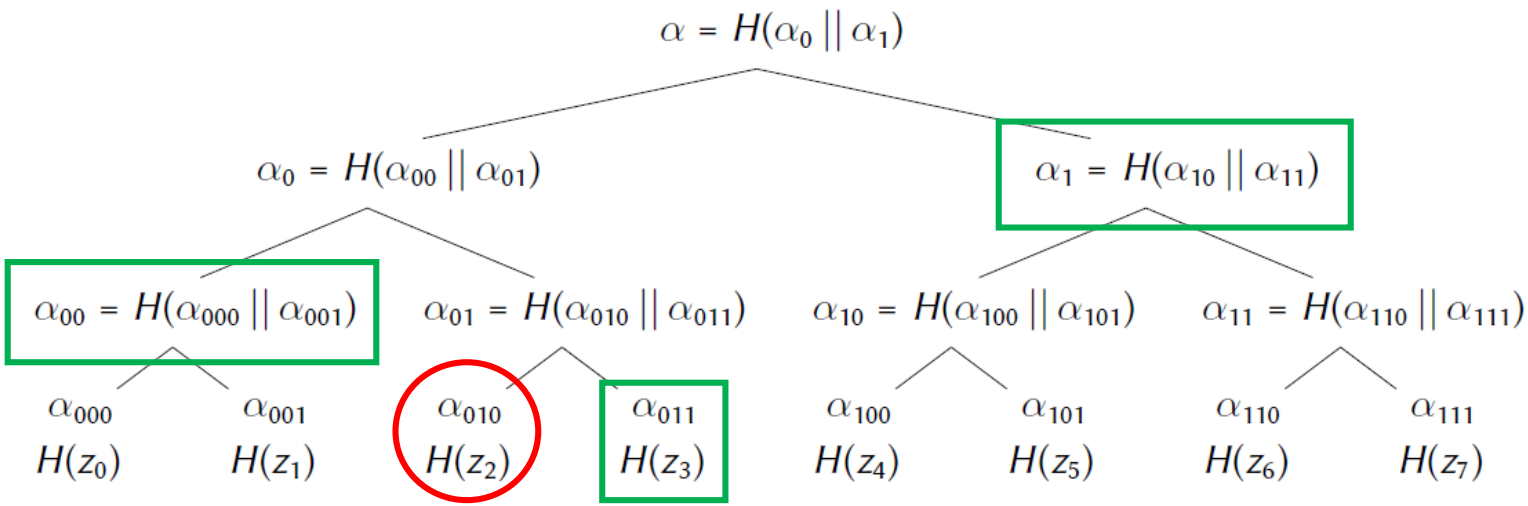
- n – počet bitov správy m
- súkromné kľúče - náhodné $x(i, j)$ pre $i = 1, \ldots, n$ $j \in \{0, 1\}$
- verejné kľúče $y(i, j) = h(x(i, j))$
- podpis $m = m_1, m_2, \ldots, m_n$ je $(x(1, m_1), x(2, m_2), \ldots, x(n, m_n))$
- overenie $\forall i : \quad h(x(i, m_i)) =? y(i, j)$

- dlhé kľúče (2 x 256 x 256 = 16 kB pre n = 256) a podpisy
- len na jednorazové použitie

+ nie je potrebná asymetrická kryptografia a certifikáty
+ odolná voči kvantovým výpočtom

MSS Merkle Signature Scheme

- Merkle hašovací strom – pre 2^n OTS kľúčov
- vstupy pre $i = 0, \ldots, 2^n-1$ - verejné OTS kľúče z_i s hašom $H(z_i)$
- $H(a \| b)$ – haš ľavého a pravého potomka v binárnom strome koreň α – spoločný haš na overenie integrity
- podpis = OTS podpis + z_i (OTS VK) + postupnosť hodnôt súrodeneckých vrcholov na ceste ku koreňu (dĺžky n)



MSS Merkle Signature Scheme

- Merkleho strom pre podpisy viacerých správ pomocou jedného verejného overovacieho kľúča
- koreň – haš stromu – jediný verejný kľúč (na overovanie)
- podpis – OTS podpis, verejný kľúč OTS, autentifikačná cesta (na konštrukciu hašu pre overovanie v koreni) dĺžky n
- overenie

  overiť podpis správy verejným OTS kľúčom

  z VK správy vypočítať haš, pomocou autentifikačnej cesty vypočítať haš celého stromu a porovnať s verejným overovacím kľúčom (hodnotou v koreni)

v poslednom liste stromu – podpis VK nasledujúceho stromu – reťazenie stromov

Ďakujem za pozornosť.

jozef.jirasek@upjs.sk