TEMA 8.
Scheme de semnătură digitală

Cuprins

- Particularități teoretice
- Schema de semnătură RSA
- Schema de semnătură El Gamal
- Standardul DSS de semnătură digitală

PARTICULARITĂȚI TEORETICE

O schemă de semnătură digitală se bazează pe trei algoritmi:

- algoritmul de selectare aleatoare a unei chei private care se va asocia unei chei publice;

Algoritmul de semnare care, aplicat unei chei private şi unui document digital, generează semnătura digitală;

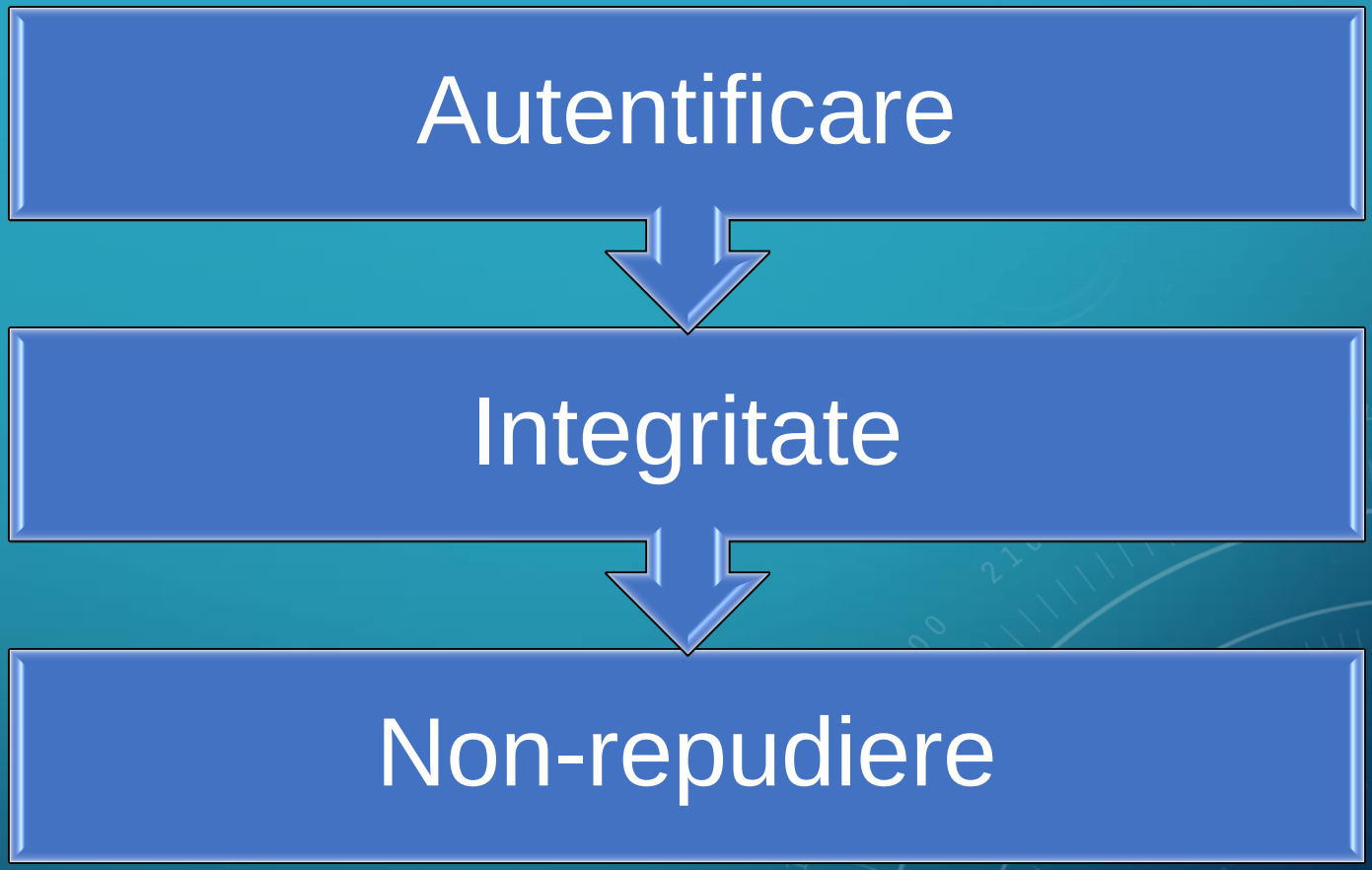
Algoritmul de verificare a semnăturii digitale, care aplicat cheii publice şi semnăturii digitale, acceptă sau respinge mesajul de conformitate.

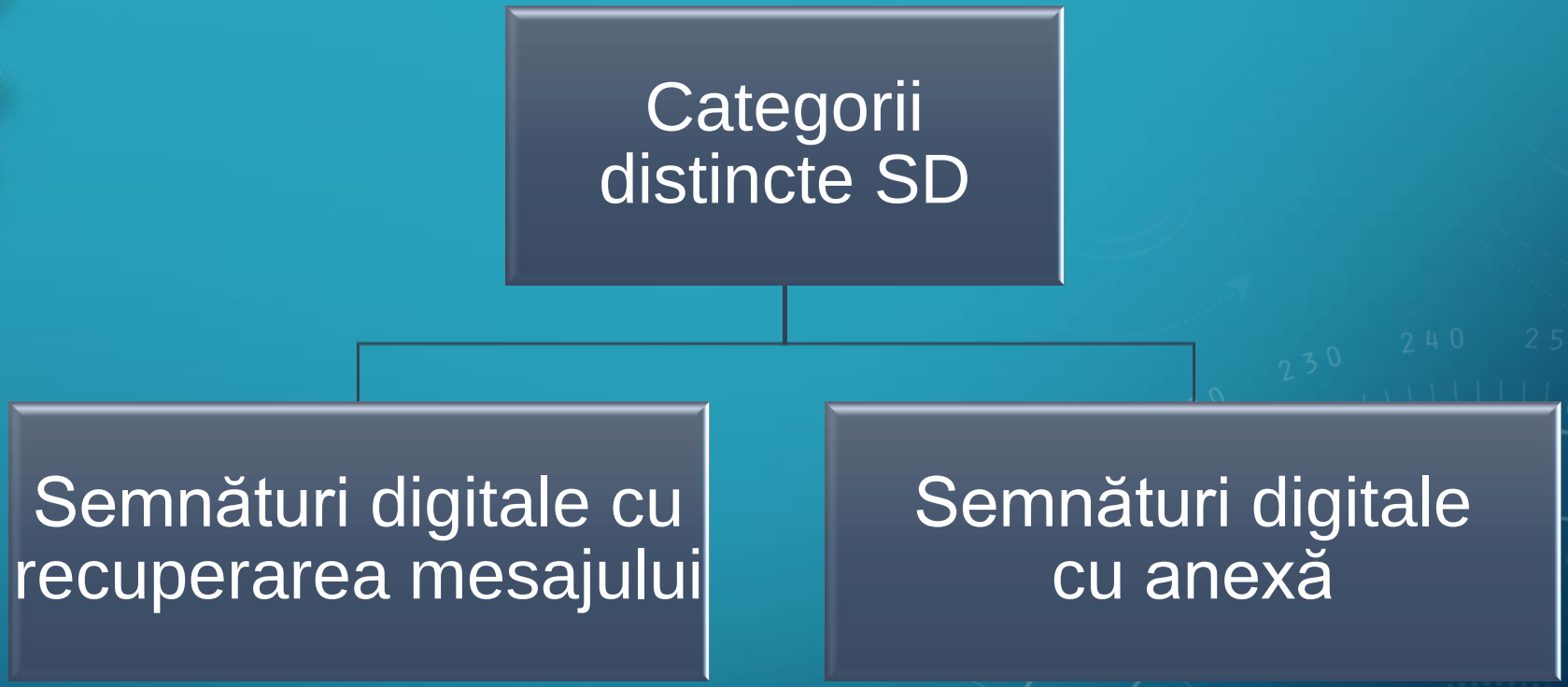
În primul rând, o semnătură generată dintr-un mesaj fix și o cheie fixă privată ar trebui să verifice autenticitatea acestui mesaj utilizând cheia publică corespunzătoare.

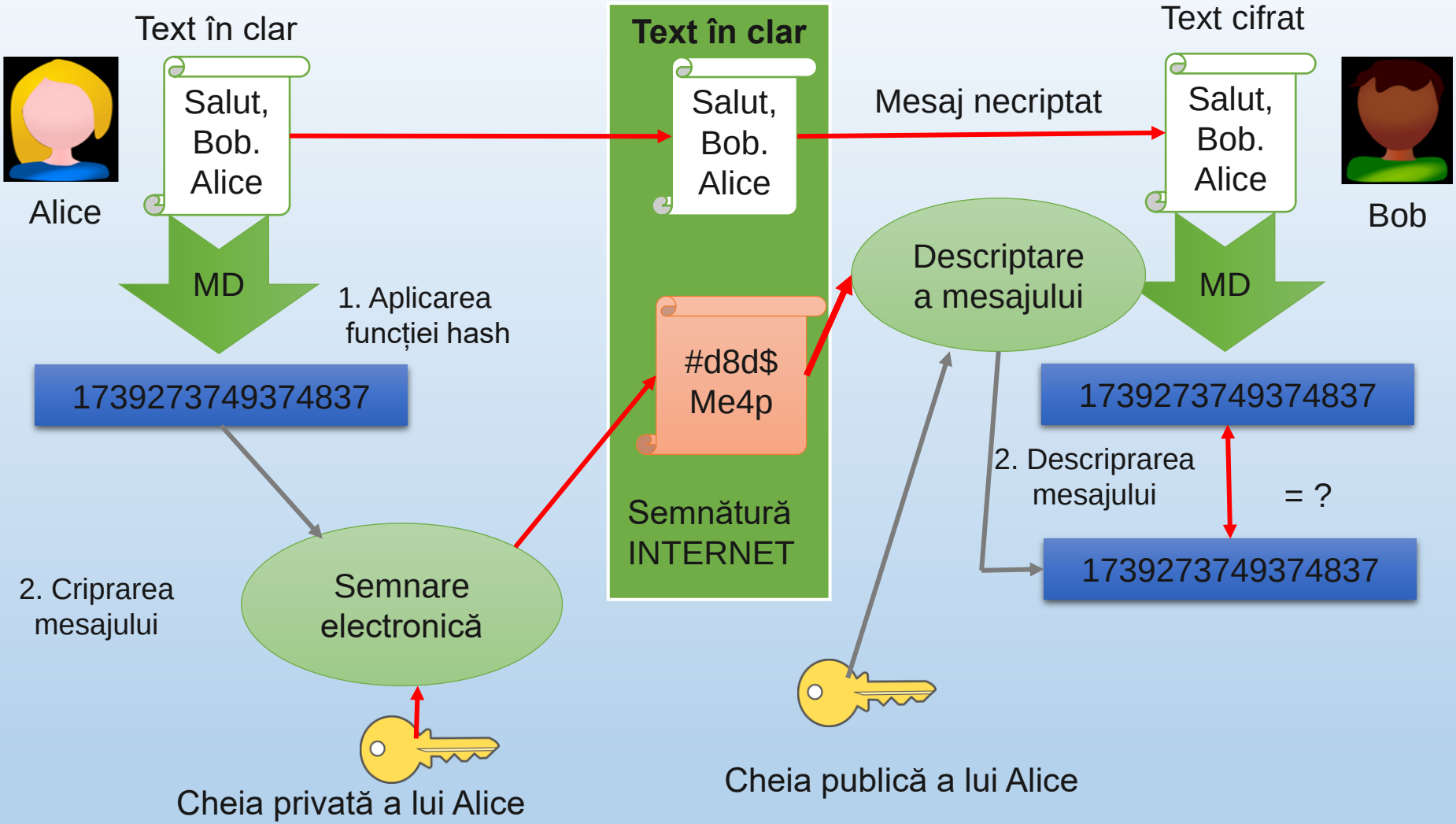
În al doilea rând, ar trebui să fie imposibil de generat o semnătură validă pentru o entitate care nu posedă cheia privată.

Proprietățile semnăturii digitale:

- Trebuie să fie uşor de calculat doar de către cel care semnează mesajul;
- Trebuie să fie uşor de verificat de către oricine;
- Trebuie să deţină o durată de viaţă corespunzătoare.


Autentificare
Integritate
Non-repudiere


Categorii distincte SD
Semnături digitale cu recuperarea mesajului
Semnături digitale cu anexă


Text în clar
Salut,
Bob.
Alice
Alice
MD
1. Aplicarea
funcției hash
1739273749374837
2. Criprarea
mesajului
Semnare
electronică
Cheia privată a lui Alice
Text în clar
Salut,
Bob.
Alice
#d8d$
Me4p
Semnătură
INTERNET
Mesaj necriptat
Descriptare
a mesajului
Text cifrat
Salut,
Bob.
Alice
MD
Bob
1739273749374837
2. Descriprarea
mesajului
= ?
1739273749374837
Cheia publică a lui Alice

Întrebare de control

- Unde poate fi aplicată semnătura digitală?
- Putem utiliza aceeași semnătură pentru acelaşi mesaj de fiecare dată?

SCHEMA DE SEMNĂTURĂ RSA

Particularitate: utilizatorii au modul diferit, iar blocurile în clar sau cifrate au lungimi diferite (k, respectiv 1, k < 1).

Fie S semnătura pe care A vrea să o trimită lui B

Generarea cheilor:

- Generează două numere prime mari p şi q;
- Calculează $n = p*q$ şi $\varphi(n) = (p–1) * (q–1)$;
- Selectează aleator un număr întreg e, $1< e < \varphi(n)$, astfel încât *cmmdc* $(e, \varphi(n)) = 1$

Generarea cheilor:

- Calculează numărul întreg d, $1 < d < \varphi(n)$, astfel încât

$$e * d = 1 \pmod{\varphi(n)};$$

- Cheia publică a entităţii A este perechea (e, n); cheia privată este d sau (d, n).

Generarea semnăturii:

- Calculează $S = [H(m)]^d \pmod{n}$, unde H este o funcţie hash;
- Semnătura mesajului m este S.

Verificarea semnăturii:

- Obţine cheia publică autentică (e, n) a entităţii A;
- Calculează $H_1 = S^e$ şi $H_2 = H(m) \pmod{n}$.

Întrebare de control

- Exepmlificați algoritmul de generare a cheilor RSA?
- Generarea cheilor?
- Generarea semnăturii?
- Verificarea semnăturii?

SCHEMA DE SEMNĂTURĂ EL GAMAL

Generarea cheilor:

- Generează un număr prim mare p şi un generator α al grupului multiplicativ Z_p *;
- Selectează aleator un număr întreg a astfel încât 1 ≤ a ≤ p–2;
- Calculează y = α^a mod p;
- Cheia publică a entităţii A este (p, α, y); cheia privată este a.

Generarea semnăturii:

- Selectează aleator un număr intreg secret k, $1 \le k \le p-2$, astfel

  încât $cmmdc(k, p-1) = 1$;

- Calculează $r = \alpha^k \bmod p$ şi $k^{-1} \bmod (p-1)$;
- Calculează $s = k^{-1} (H(m) - a*r) \bmod (p-1)$, unde H este o funcţie hash;
- Semnătura mesajului m este perechea (r, s).

Verificarea semnăturii:

- Obţine cheia publică autentică (p, α, y) a entităţii A ;
- Verifică dacă $1 \leq r \leq p - 1$;
- Calculează $v_1 = y^r r^s \, mod \, p$;
- Calculează $H(m)$ şi $v_2 = \alpha^{H(m)}$;
- Semnătura (r, s) este acceptată dacă şi numai dacă $v1 = v2$.

Întrebare de control

- Exepmlificați algoritmul de generare a cheilor El Gamal?
- Generarea cheilor?
- Generarea semnăturii?
- Verificarea semnăturii?

STANDARDUL DSS DE SEMNĂTURĂ DIGITALĂ

Generarea cheilor:

- Generează un număr prim q astfel incat $2^{159} < q < 2^{160}$;
- Generează un număr prim p astfel incat $2^{512} \leq p < 2^{1024}$ şi $q|(p-1)$;
- Selectează un generator α pentru grupul ciclic Z_p de ordin q;

- Alege un element $g \in Z_p^*$ şi calculează $\alpha = g^{(p-1)/q} \bmod p$;

  dacă $\alpha = 1$, atunci alege alt element g;
- Se selectează un număr intreg α astfel incat $1 \leq a \leq q - 1$;
- Se calculează $y = \alpha^a \bmod p$;
- *Cheia publică* a entităţii A este (p, q, α, y), iar *cheia privată* este a.

Generarea semnăturii:

- Selectează aleator un număr intreg k astfel încât $0 < k < q$;
- Calculează $r = (\alpha^k \bmod p) \bmod q$.
- Calculează $k^{-1} \bmod q$;
- Calculează $s = k^{-1} (H(m) + a*r) \bmod q$, unde H o funcție hash;
- Semnătura mesajului m este perechea (r, s).

Verificarea semnăturii:

- Obţine cheia publică autentică (p, q, α, y) a entităţii B;
- Verifică dacă $0 < r < q$ şi $0 < s < q$;
- Calculează $w = s^{-1} \bmod q$ şi $H(m)$;

- Calculează u_1 = *w*H(m)* mod *q* şi u_2 = *r*w* mod *q*;
- Calculează $v = (\alpha^{u_1} y^{u_2} \ mod \ p)$ mod q;
- Semnătura *(r, s)* a mesajului *m* este acceptată dacă şi numai dacă *v = r*.

Întrebare de control

Ce se întâmplă în cazul când a fost transmis un document fără a fi criptat fiind necesară numai semnătura digitală?

ÎNTREBĂRI RECAPITULATIVE

- Unde poate fi aplicată semnătura digitală?
- Putem utiliza aceeași semnătură pentru acelaşi mesaj de fiecare dată?

- Exepmlificați algoritmul de generare a cheilor El Gamal?
- Generarea cheilor?
- Generarea semnăturii?
- Verificarea semnăturii?

Ce se întâmplă în cazul când a fost transmis un document fără a fi criptat fiind necesară numai semnătura digitală?

SEMNĂTURI DIGITALE