

TEMA 8.

Scheme de semnătură digitală



Cuprins

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



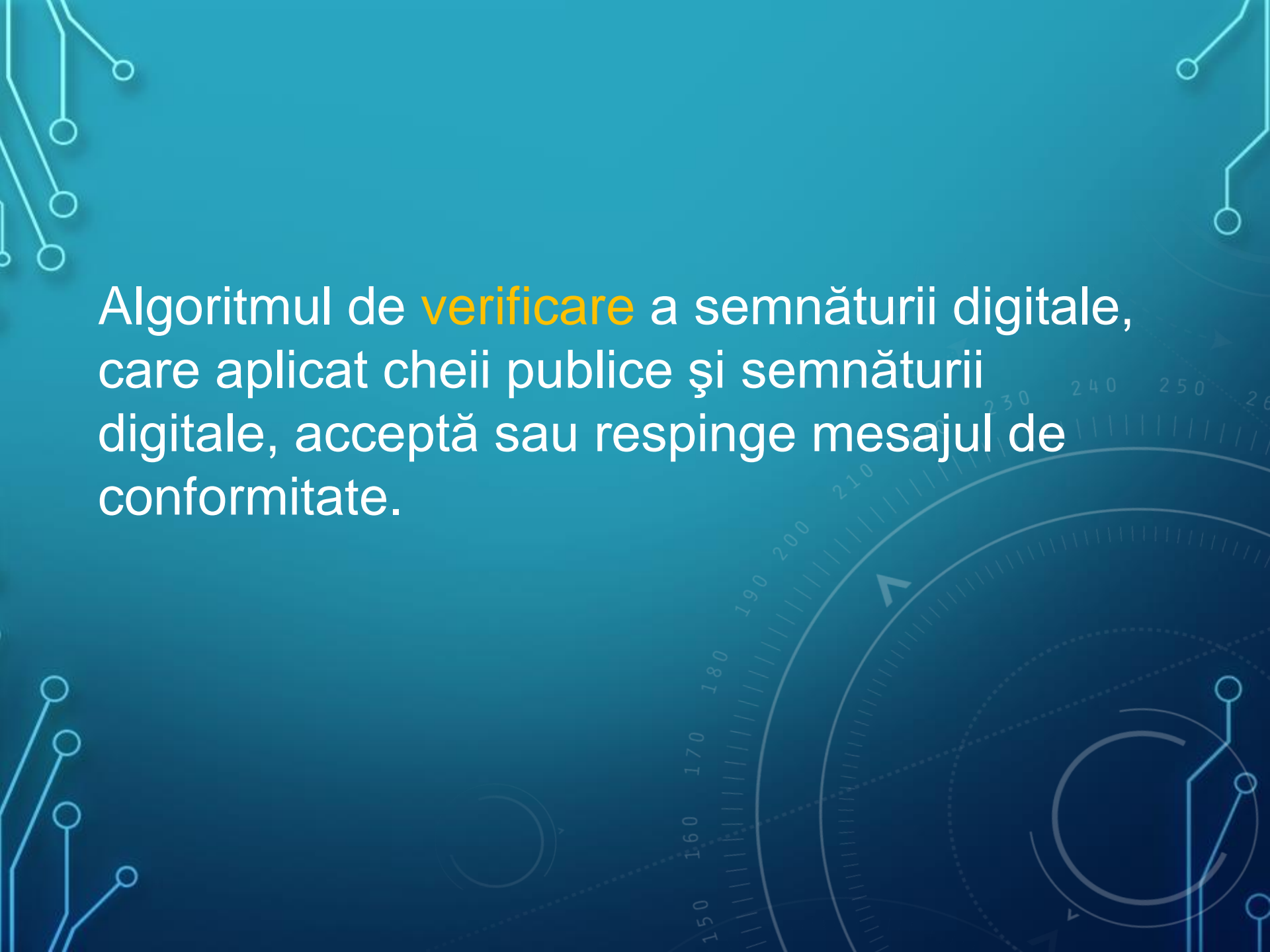
The background is a solid blue color with various white and light blue geometric and technical motifs. On the left side, there are vertical lines resembling a circuit board with small circles at the end of the lines. In the center and right, there are several circular elements: some are solid lines forming partial circles, others are dashed lines with arrows indicating a clockwise direction. A prominent feature is a semi-circular scale or gauge on the right side, with numerical markings from 150 to 260 in increments of 10. The overall aesthetic is clean, modern, and technical.

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 și unui document digital, generează semnătura digitală;

The background is a dark teal color. It features several decorative elements: white circuit-like lines with circular nodes in the corners; a large, semi-transparent circular scale in the lower right quadrant with numerical markings from 150 to 260 and a white arrow pointing upwards; and a faint, light blue circular graphic in the lower left.

Algoritmul de **verificare** a semnăturii digitale, care aplică cheia publică și 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 ușor de calculat doar de către cel care semnează mesajul;
- Trebuie să fie ușor de verificat de către oricine;
- Trebuie să dețină o durată de viață corespunzătoare.

Autenticare

```
graph TD; A[Autenticare] --> B[Integritate]; B --> C[Non-repudiare];
```

Integritate

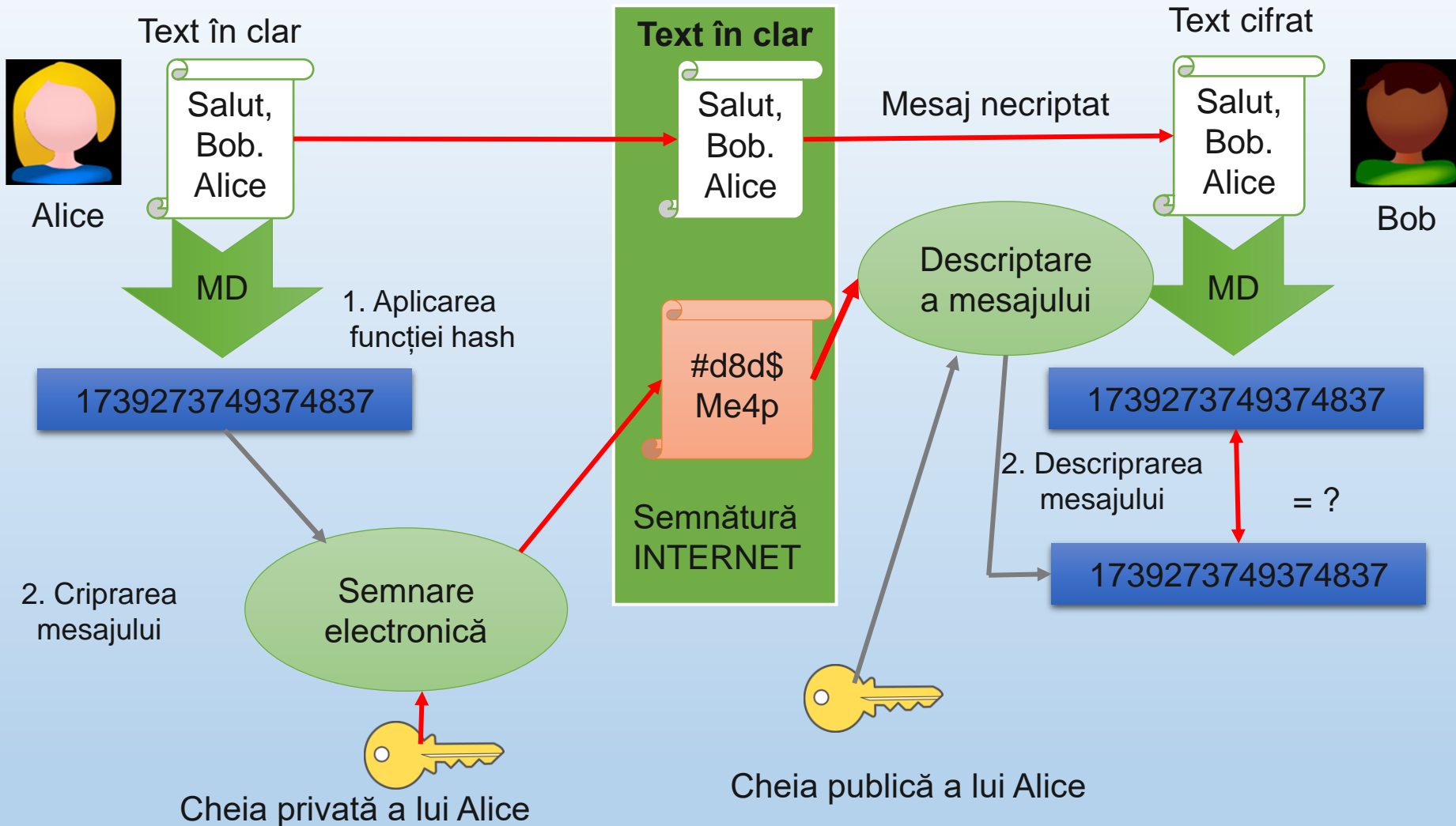
Non-repudiare

Categorii distincte SD

```
graph TD; A[Categorii distincte SD] --> B[Semnături digitale cu recuperarea mesajului]; A --> C[Semnături digitale cu anexă];
```

Semnături digitale cu
recuperarea mesajului

Semnături digitale
cu anexă



Întrebare de control

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

The background is a dark blue gradient with white and light blue technical graphics. On the left, there are vertical circuit traces with circular nodes. On the right, there are circular patterns resembling a dial or scale with numbers from 140 to 260 and arrows indicating rotation.

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 și q ;
- Calculează $n = p * q$ și $\varphi(n) = (p-1) * (q-1)$;
- Selectează aleator un număr întreg e , $1 < e < \varphi(n)$, astfel încât $\text{cmmdc}(e, \varphi(n)) = 1$

Generarea cheilor:

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

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

- Cheia publică a entității 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 funcție hash;
- Semnătura mesajului m este S .

Verificarea semnăturii:

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

Întrebare de control

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

The background is a solid teal color with various white and light blue geometric patterns. On the left side, there are vertical circuit traces with circular nodes. On the right side, there are several concentric circular patterns, some with dashed lines and arrows, and a scale-like structure with numerical values from 140 to 260. The text is centered in the middle of the image.

SCHEMA DE SEMNĂTURĂ EL GAMAL

Generarea cheilor:

- Generează un număr prim mare p și un generator α al grupului multiplicativ Z_p^* ;
- Selectează aleator un număr întreg a astfel încât $1 \leq a \leq p-2$;
- Calculează $y = \alpha^a \bmod p$;
- Cheia publică a entității A este (p, α, y) ; cheia privată este a .

Generarea semnăturii:

- Selectează aleator un număr întreg secret k , $1 \leq k \leq p-2$, astfel

încât $\text{cmmdc}(k, p-1) = 1$;

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

Verificarea semnăturii:

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

Întrebare de control

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



STANDARDUL DSS DE SEMĂTURĂ DIGITALĂ

Generarea cheilor:

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

- Alege un element $g \in Z_p^*$ și calculează $\alpha = g^{(p-1)/q} \bmod p$;
dacă $\alpha = 1$, atunci alege alt element g ;
- Se selectează un număr întreg a astfel încât $1 \leq a \leq q - 1$;
- Se calculează $y = \alpha^a \bmod p$;
- Cheia publică a entității A este (p, q, α, y) , iar cheia privată este a .

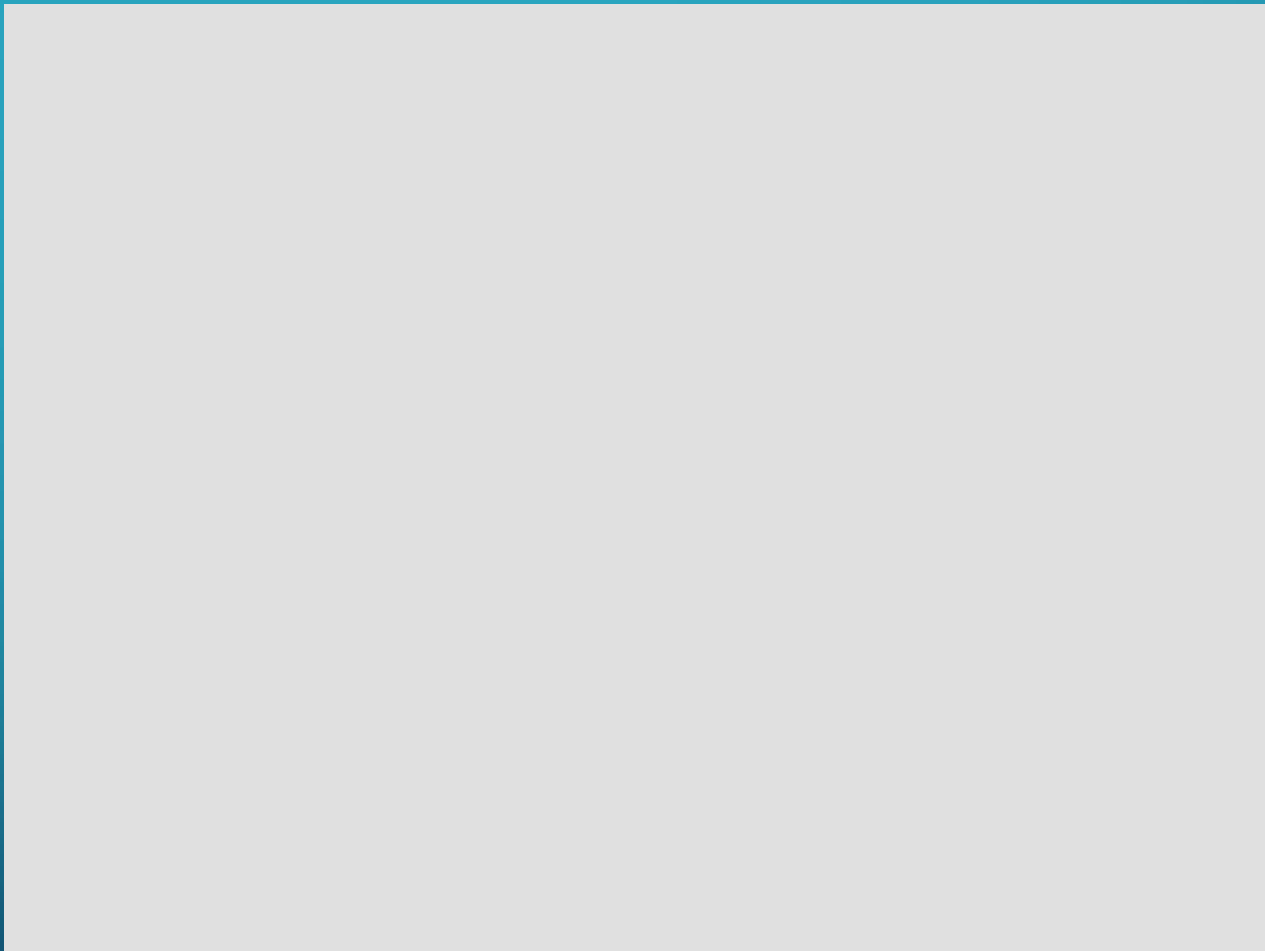
Generarea semnăturii:

- Selectează aleator un număr întreg k astfel încât $0 < k < q$;
- Calculează $r = (a^k \bmod p) \bmod q$.
- 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:

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

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

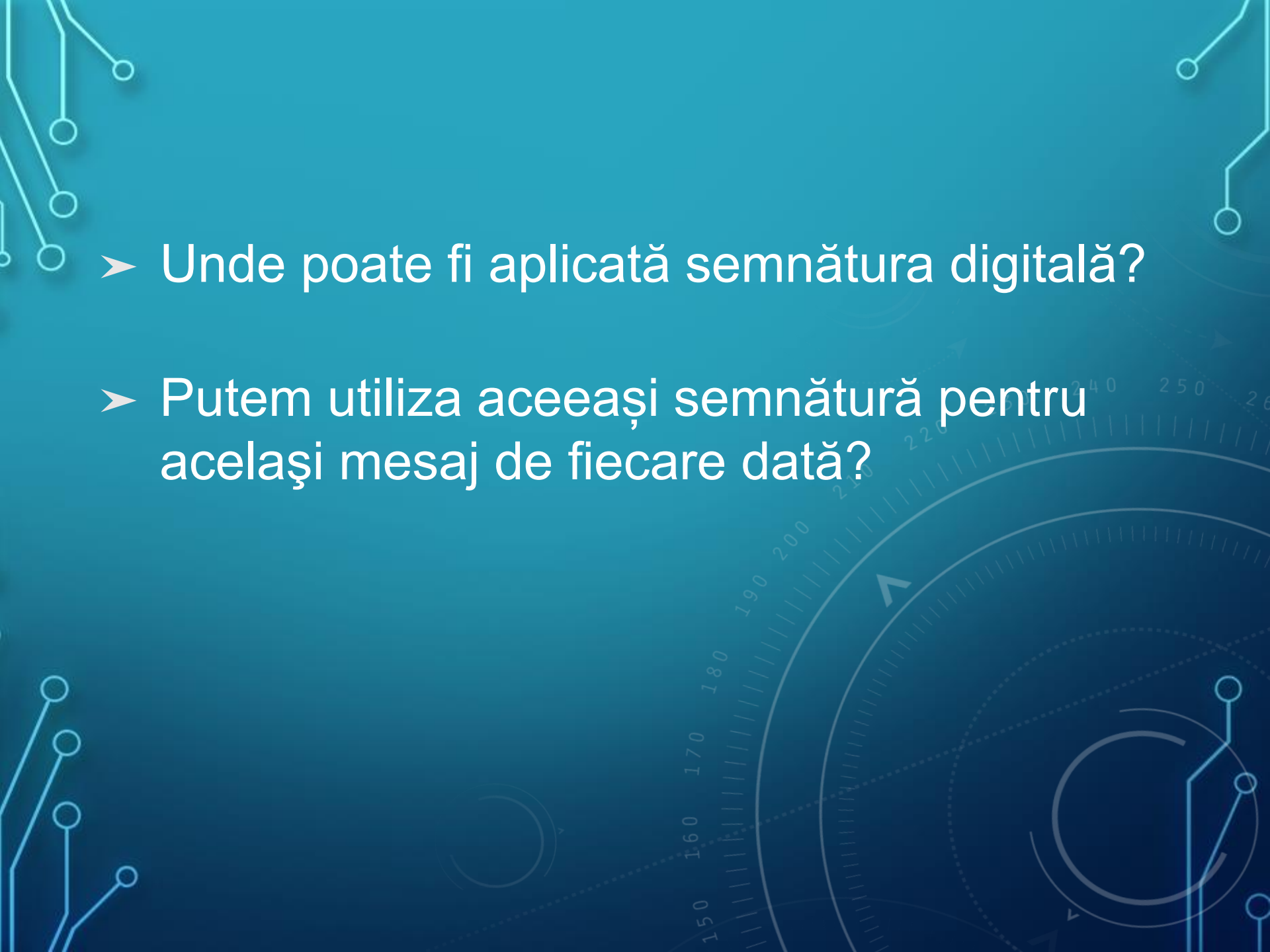


Întrebare de control

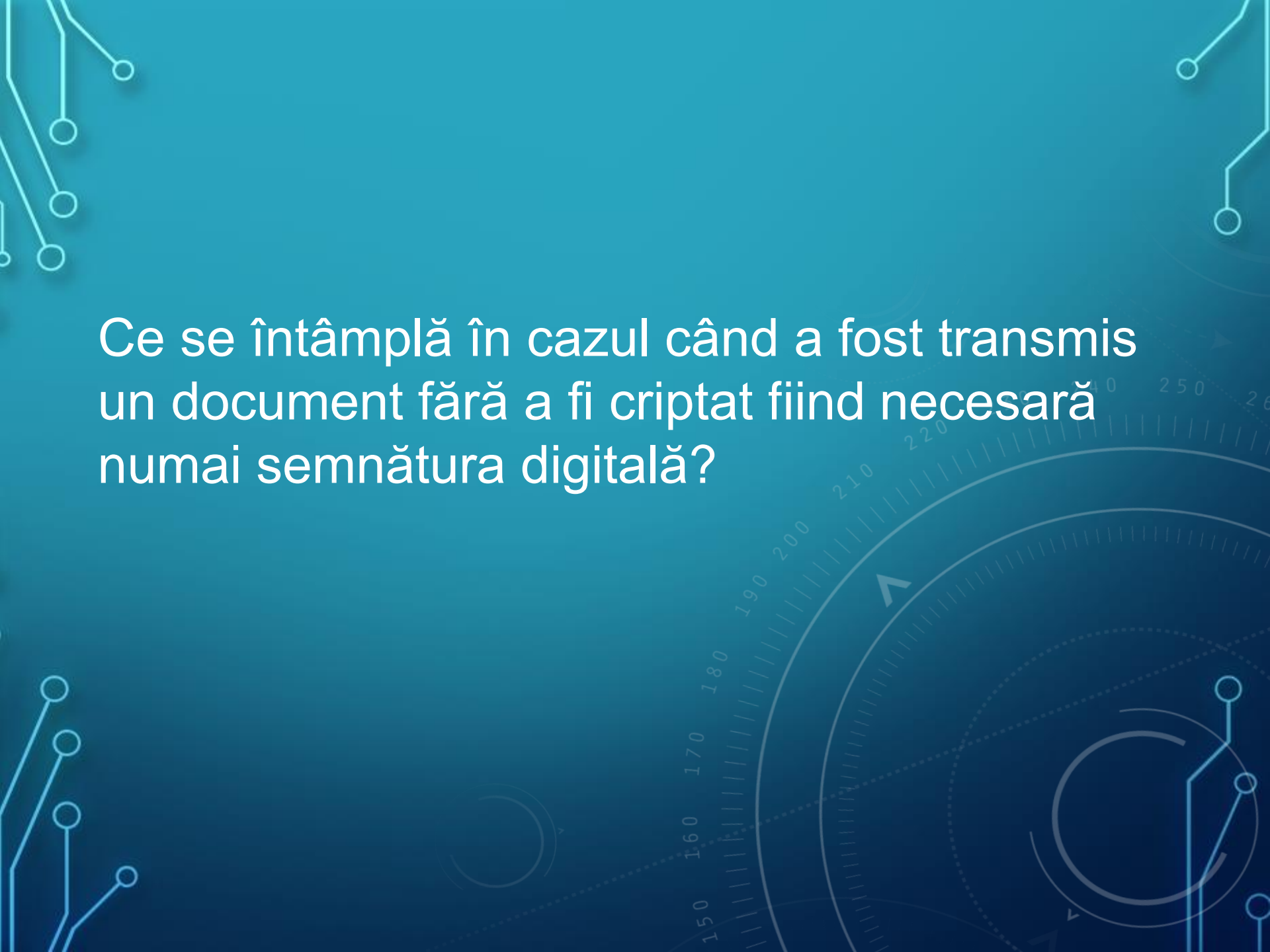
Ce se întâmplă în cazul când a fost transmis un document fără a fi criptat fiind necesară numai semnătura digitală?



ÎNTREBĂRI RECAPITULATIVE

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

- Exemplificați 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

