Securitate in IT

Universitatea “Transilvania” din Brasov

3. Principiile criptografiei

Cuprins: Securitatea in Tehnologia Informatiei

3 Principiile criptografiei

3.1 Criptare si confidentialitate

- Substitutie mono- si polialfabetica
- On-time Pad
- Steganografia

3.2 Sisteme de criptare si confidentialitate

- Metoda simetrica si asimetrica
- Sisteme hibrid
- Criptosisteme cu cifruri bloc si cu cifruri secventiale

3.3 Valoarea Hash si integritatea datelor

- Functia hash
- Integritatea datelor

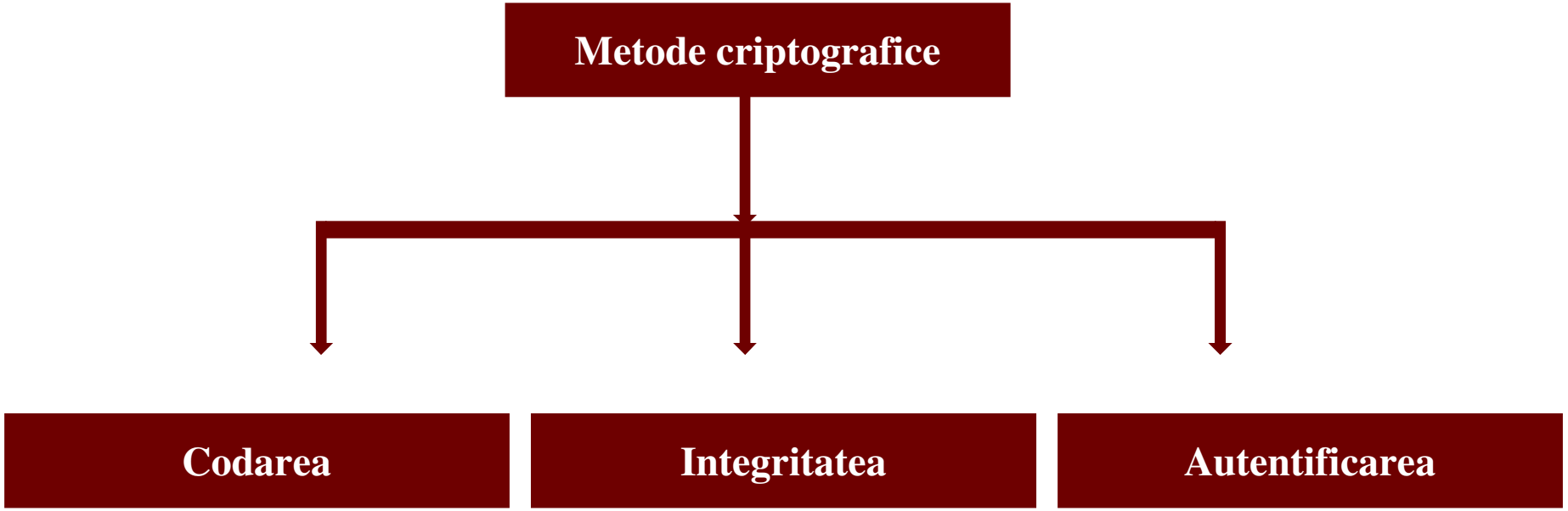
3.4 Semnatura digitala si autentificare

- Semnatura digitala
- Semnatura digitala standard

3.5 Criptare pe curbe eliptice

Tipul de amenintare		Modul de securitate
❑Cai Troieni Ingineria Sociala	→	Confidentialitatea
❑Attack Applets Virusuri Cai Troieni	→	Integritatea
❑ Mail-Spoofing, IP-, ARP-, DNS-Spoofing Violarea politicii de securitate	→	Autentificare
❑Respingerea de comenzi	→	Non-repudierea
❑Passwort Cracking, Session-Hijacking ICMP-Tunneling	→	Controlul accesului

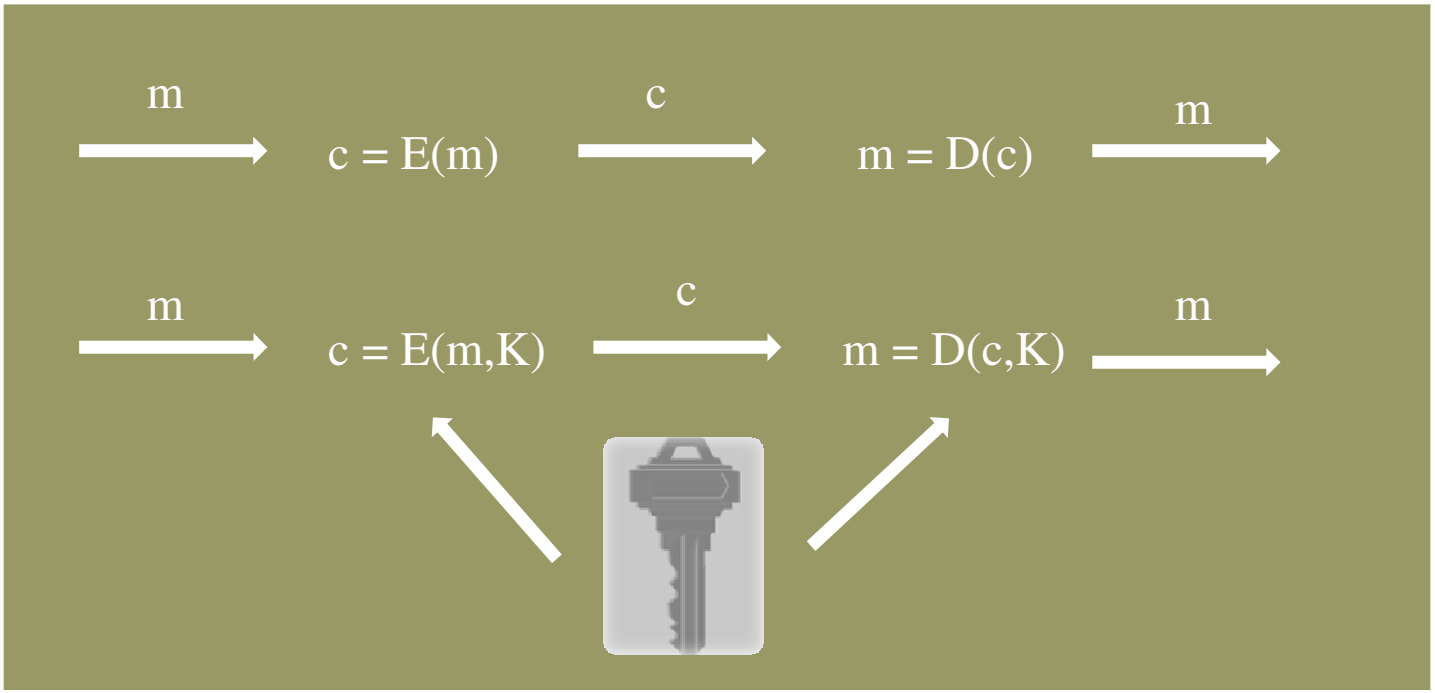
Principiile criptografiei



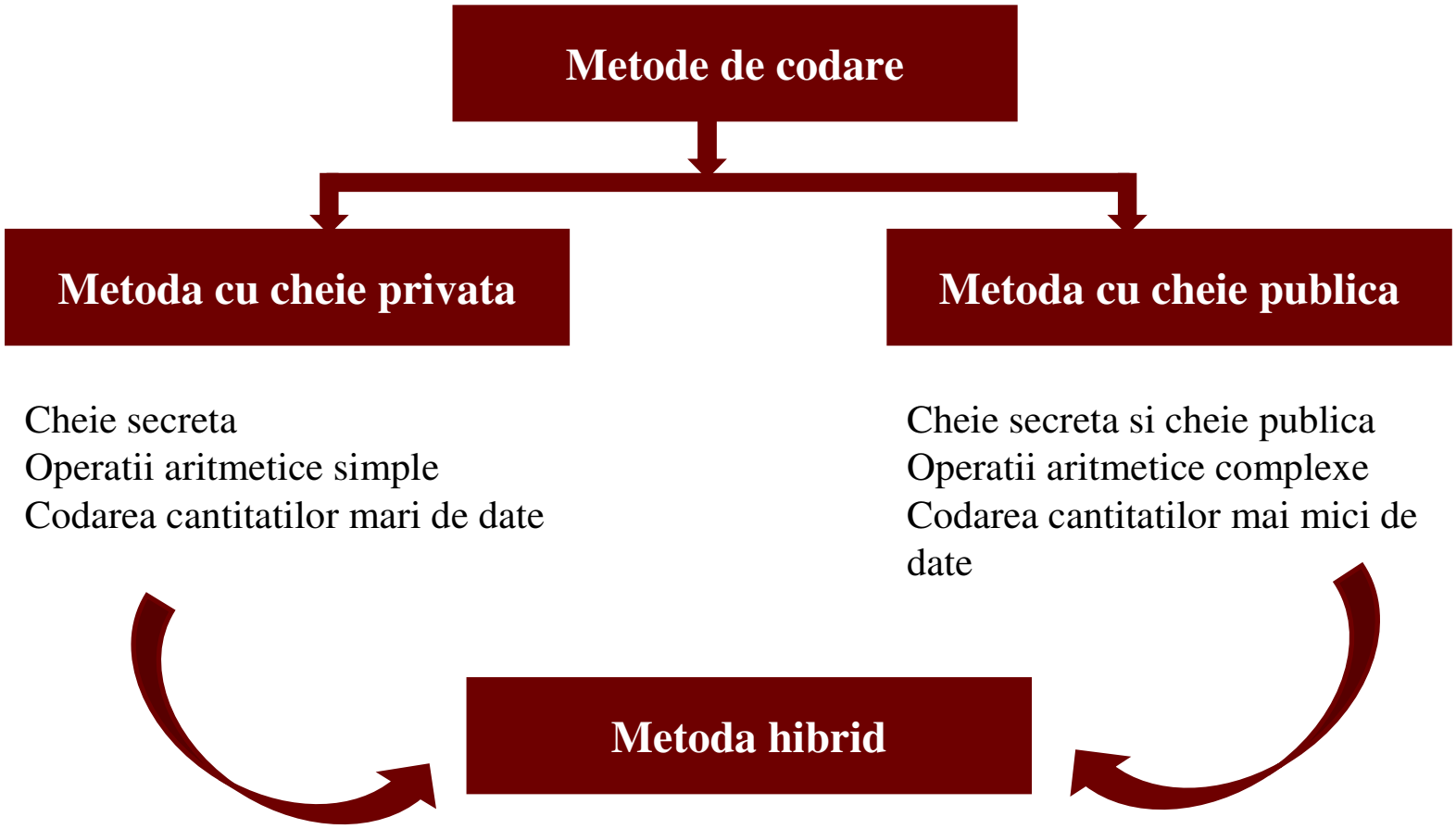
Metodele criptografice constituie baza teoretica pentru aplicatii de securitate in retele de calculatoare!

Codarea

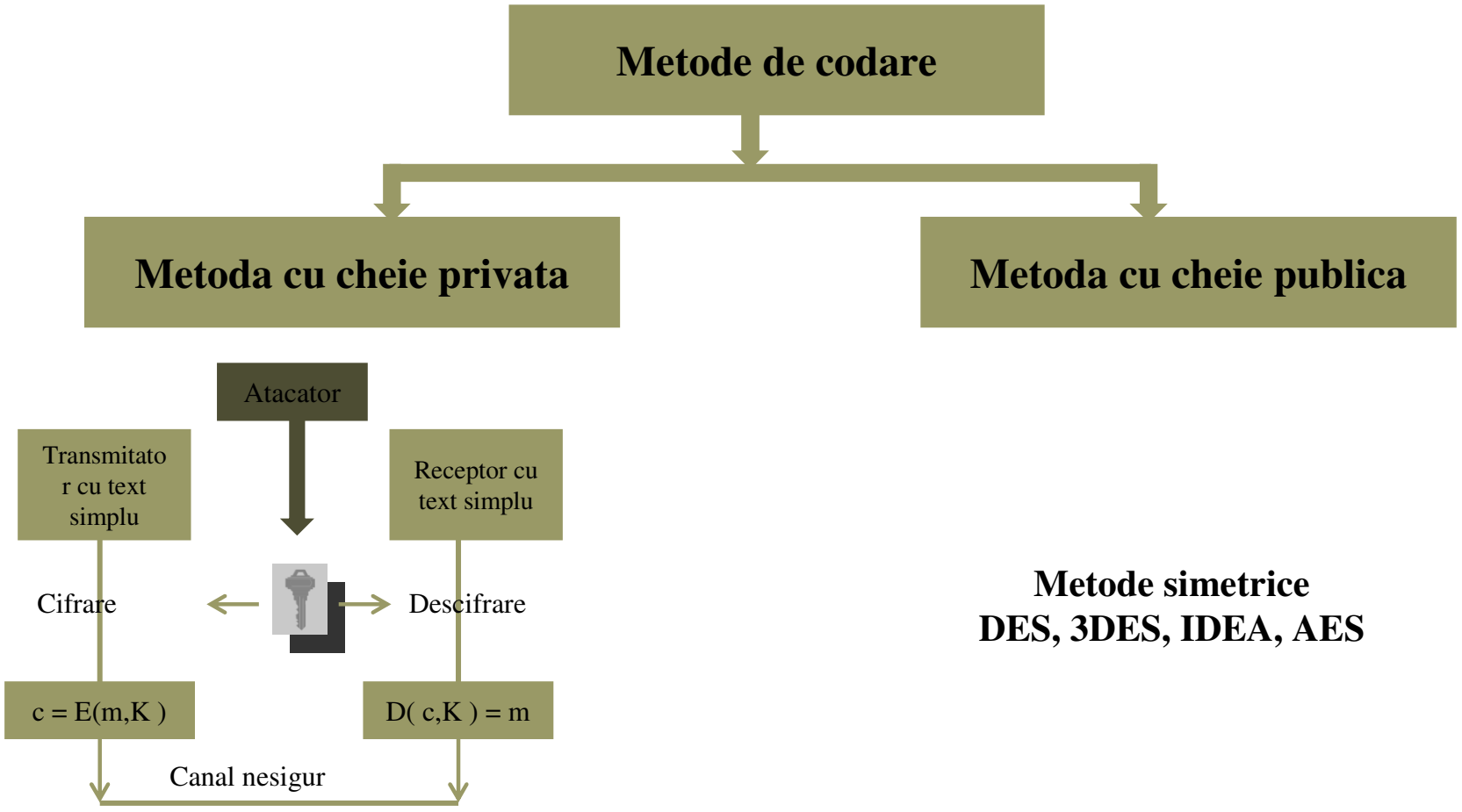
Principiile codarii



Codarea


Metode de codare
Metoda cu cheie privata
Metoda cu cheie publica
Cheie secreta
Operatii aritmetice simple
Codarea cantitatilor mari de date
Cheie secreta si cheie publica
Operatii aritmetice complexe
Codarea cantitatilor mai mici de date
Metoda hibrid

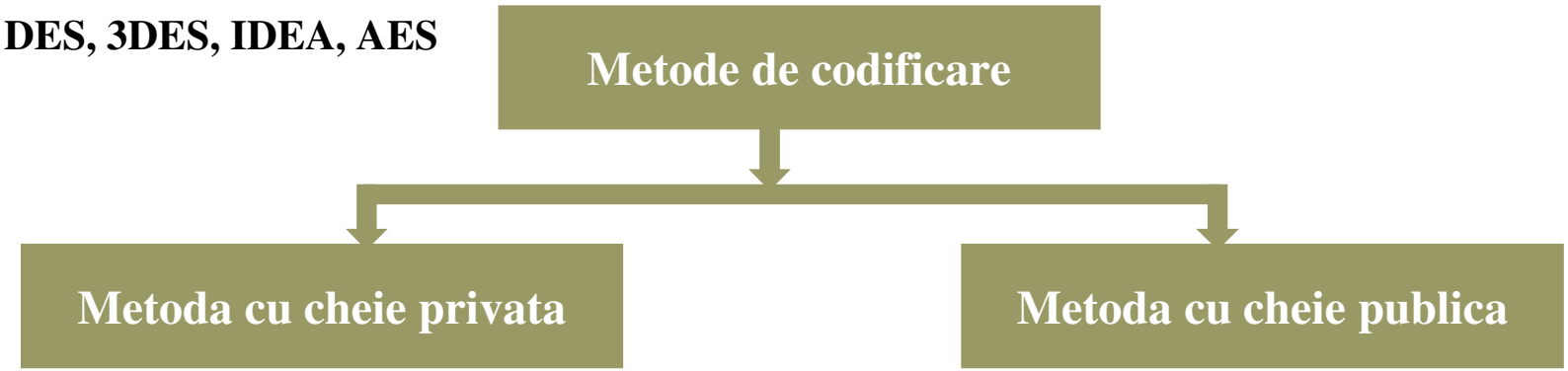
Codarea



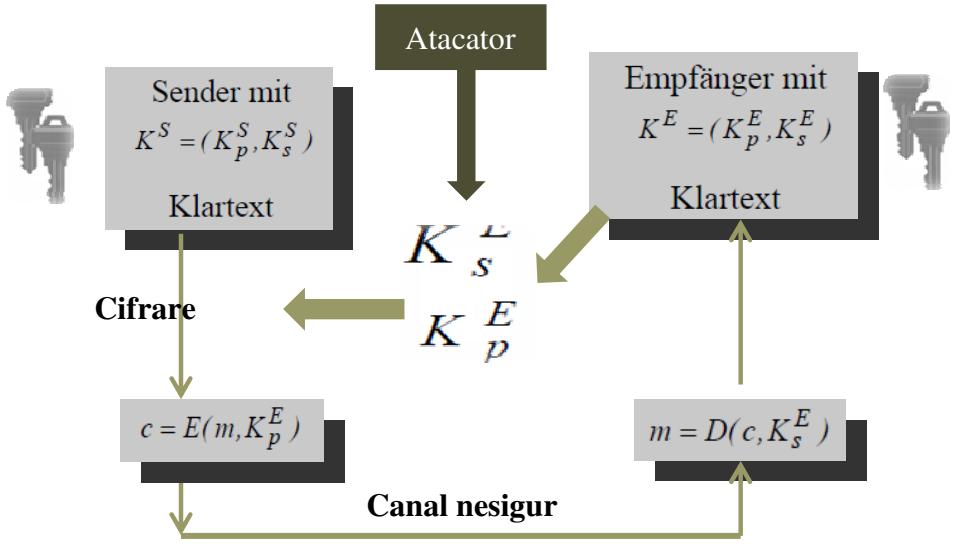
Metode simetrice
DES, 3DES, IDEA, AES

Codarea

Metode simetrice
DES, 3DES, IDEA, AES



Metode asimetrice
RSA, DH, ElGamal,
EC-DH, EC-ElGamal



Codarea

Exemplu Algoritmul RSA

- **Dezvoltare** — Ron Rivest, Adi Shamir, Leonard Adleman, 1978, bazat pe factorizare.

- **Initializare** — p,q prim n = p* q φ (n) = (p – 1)* (q – 1) d ∈Zφ (n) = {0,1,...,φ (n) – 1},d ≠ 0
  ggT(d ,φ (n)) = 1 e* d =1 mod φ (n)

$$K^E = (K_p^E, K_s^E) \qquad K_p^E \equiv (n,e) \qquad K_s^E \equiv (d)$$

- **Codare**

$$c = E(m,e) = m^e \bmod n$$

- **Decodare**

$$m = D(c,d) = c^d \bmod n$$

Apoi : $c^d \bmod n = (m^e)^d \bmod n = m^{e \cdot d} \bmod n = m$

Codarea

Calcul: Algoritmul RSA

❑ **(1)**

p = 47 q = 59 n = 2773 φ (n) = 46 * 58 = 2668

d = 157 0 < e < 2668 e* 157 = 1 mod 2668 e = 17

Cheie $K_p^E = (2773,17)$ $K_s^E = (157)$

Codare $c = E(m,17) = m^{17} \bmod 2773$

Decodare $m = D(c,157) = c^{157} \bmod 2773$

❑ **(2)**

p = 3 q = 17 n = 51 φ (n) = 2* 16 = 32

d = 13 0 < e < 32 e * 13 = 1 mod 32 e = 5 Sei m = 19

Cheie $K_p^E = (51,5)$ $K_s^E = (13)$

Codare $c = E(19,5) = 19^5 \bmod 51 = (19^2 19^2 19) \bmod 51 = (4 \cdot 4 \cdot 19) \bmod 51$

$(4 \cdot 76) \bmod 51 = (4 \cdot 25) \bmod 51 = 49 \rightarrow c = 49.$

Decodare $m = D(49,13) = 49^{13} \bmod 51 = (-2)^{13} \bmod 51 = (1024 \cdot (-8)) \bmod 51$

$= (4 \cdot (-8)) \bmod 51 = (-32) \bmod 51 = 19 \bmod 51 = 19$

Integritatea

Principiul functiei Hash

Mesaj m = (10011010...1000110)

Cu lungime arbitrara

Valoarea hash h = (01...101)

Cu lungime fixa (128, 160 Bit)

Functia Hash $m \rightarrow h = H(m)$

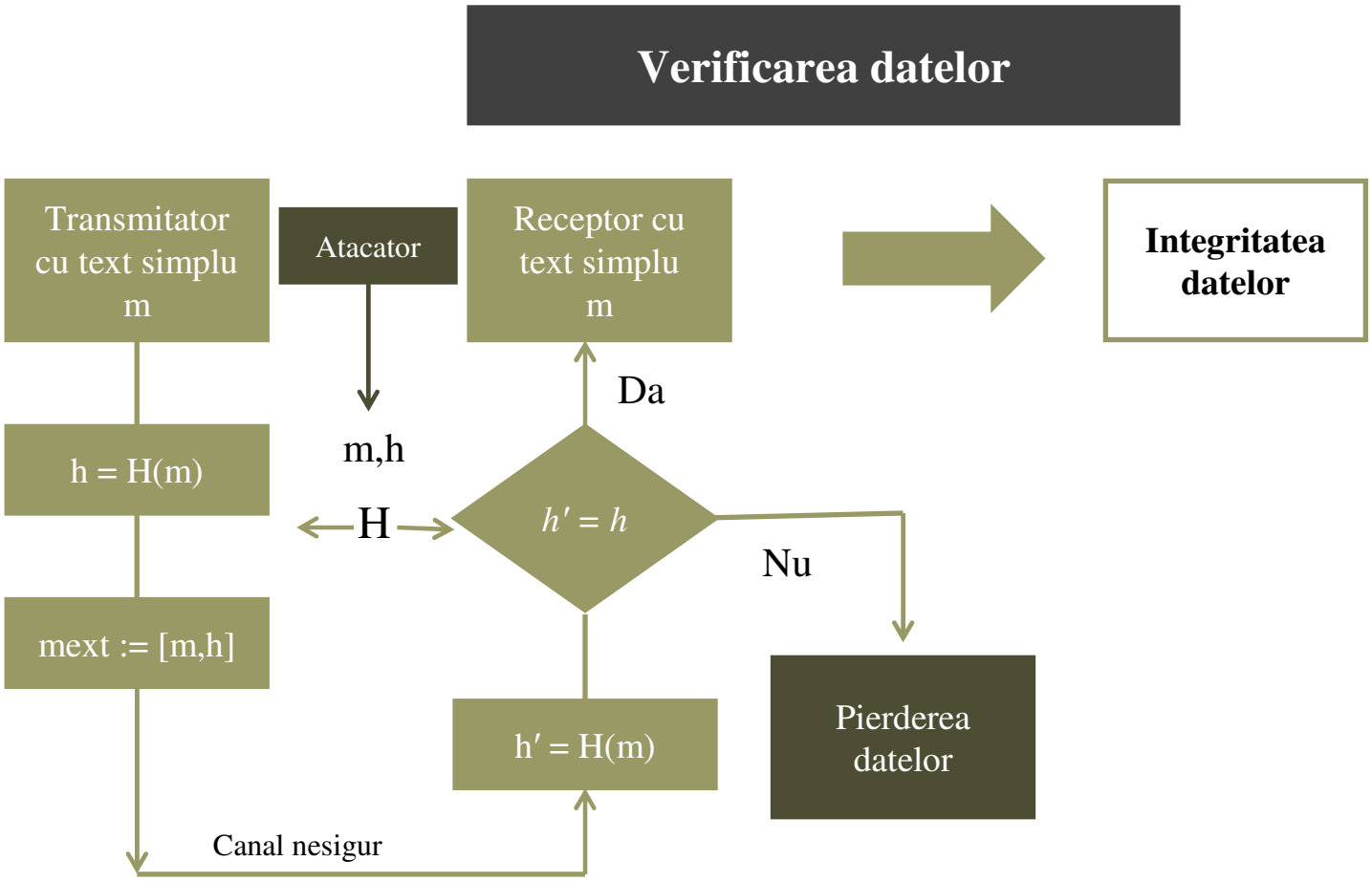
- Functia disponibila

  $H(m) \Rightarrow m$

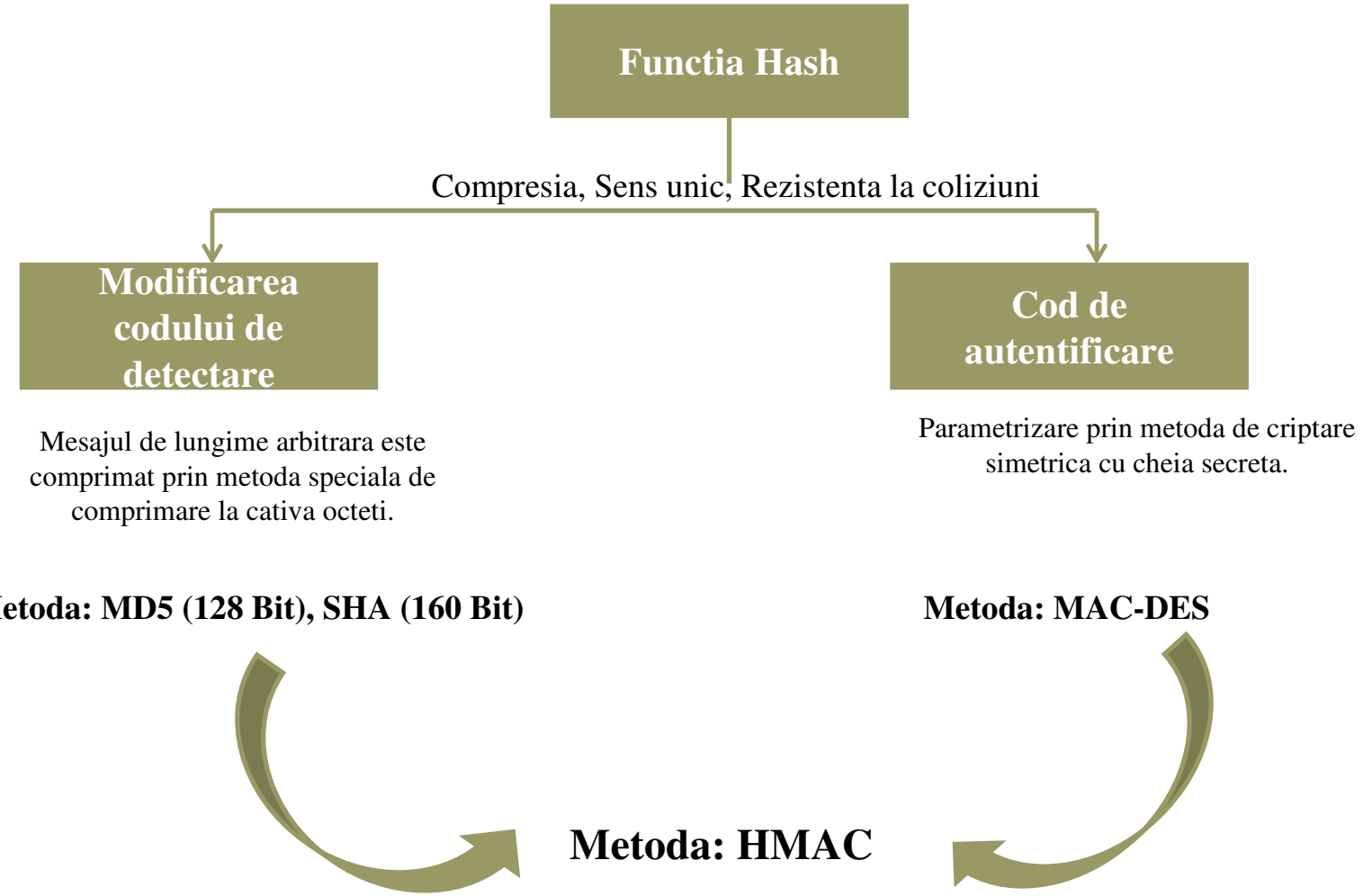
- Rezistenta la coliziune

  $m \neq m' \Rightarrow H(m) \neq H(m')$

Integritatea



Integritatea



Integritatea

Algoritmul HMAC

❑Algoritmul HMAC a fost dezvoltat in anul 1996 si este cel mai frecvent MDC bazat pe algoritmul MAC. Dintr-un mesaj m de lungime arbitrara si o cheie secreta K se creaza o valoare fixa H, dupa cum urmeaza:

❑ **Functia Hash** H(m) (meist MD5 oder SHA-1) **Cheie secreta K**

Mesajul m descompus in blocuri de 64 biti.

Cheia secreta K este umpluta cu zerouri pana la lungimea blocului.

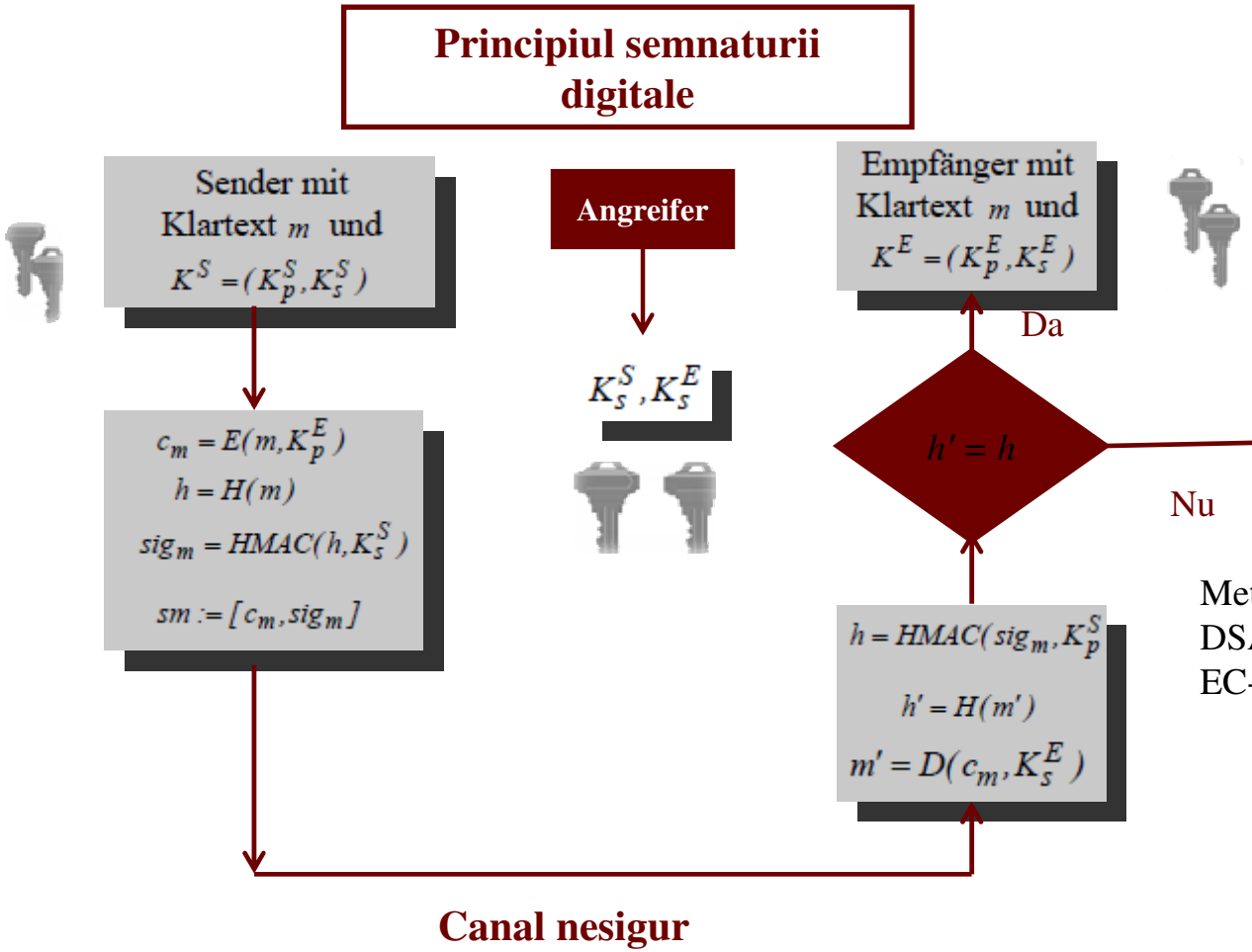
❑ **Cheie de ajtor**

$$S_i := K^+ \otimes ipad \qquad ipad = (00110110)_{64mal} = (36)_{64mal}$$
$$S_o := K^+ \otimes opad \qquad opad = (01011100)_{64mal} = (5C)_{64mal}$$

Valoarea Hash

$$h := HMAC(m,K) := H(S_o \,|\, H^+(S_i \,|\, m)) \equiv H(K^+ \otimes opad, H^+(K^+ \otimes ipad, m))$$

Autentificarea



Autentificarea transmitatorilor necunoscuti si integritatea datelor.

Metoda semnaturii
DSA, RSA, RIPEMD, ElGamal, EC-DSA, EC-ElGamal

Autentificarea

Strucutura de baza: Metoda semnaturii digitale

- **Parametru** — **Perechi de chei de la statiile de comunicare**
  Functia Hash

- **Generarea de semnatura** — **Generarea mesajului transmis**
  (a) Valoarea Hash
  (b) Parametrul semnaturii

- **Examinarea semnaturii** — **Calcularea measjului primit**
  (a)Valori ajutatoare
  (b)Valoarea de comparare pentur parametrul semnaturii
  (c)Testul de comparare

Autentificarea

Exemplu: Algoritmul semnaturii digitale(DSA)

- **Dezvoltare:** Dezvoltat de NSA, in functie de problema logaritmului discret.
- **Setup:**

$$G = Z_p,\ p\ prime \quad q\ prim\ mit\ q \mid (p-1) \quad und\ g \in G\ mit\ ord g = q$$
$$Schlüsselpaar\ K^{user} := (k_p^u, k_s^u)\ mit\ k_s^u := l \in Z_q^*,\ l \neq 1\ und\ k_p^u := g^l \in Z_p^*$$
$$Hashalgorithmus\ SHA-1 \qquad K_p \equiv (p,q,g,k_p^u)\ und \quad K_s \equiv (k_s^u)$$

- **Generare:**

$$(1)\ random\ k \in Z_q^*, k \neq 1,\ und\ Wert\ r := g^k \bmod p$$
$$(2)\ berechne\ r' := r \bmod q\ und\ s := (k^{-1}(k_s^{Send} \cdot r' + H(m)) \bmod q$$
$$\Rightarrow Signatur\ von\ m\ ist\ sig := (r', s)$$

- **Verificare:**

$$(1)\ 1 \leq r', s \leq q-1$$
$$(2)\ (a)\ berechne\ Hilfswerte\ u := s^{-1} \bmod q,\ v_1 := (u \cdot H(m)) \bmod q,\ v_2 := (u \cdot r') \bmod q$$
$$(b)\ berechne\ Vergleichswert\ w := ((g^{v_1}(k_p^{Send})^{v_2}) \bmod p) \bmod q$$
$$\Rightarrow akzeptiere,\ falls\ r' = w$$

Trust Center

Cheile publice trebuie sa fie autentificate!!!

Hierarchical Trust
PKIX-Standard

Trust Center, Certification Service Provider
(Certification Authority)

Serviciul de certificare

Serviciul de registrare

Verzeichnisdienst

Zeitstempeldienst

- **Generarea cheii**
- **Cheie cu informatie suplimentara (CA-Signatur)**
- **Salvarea si distribuirea cheii**
- **Tasta de blocare sau reeditare (Zertifikate-Management)**