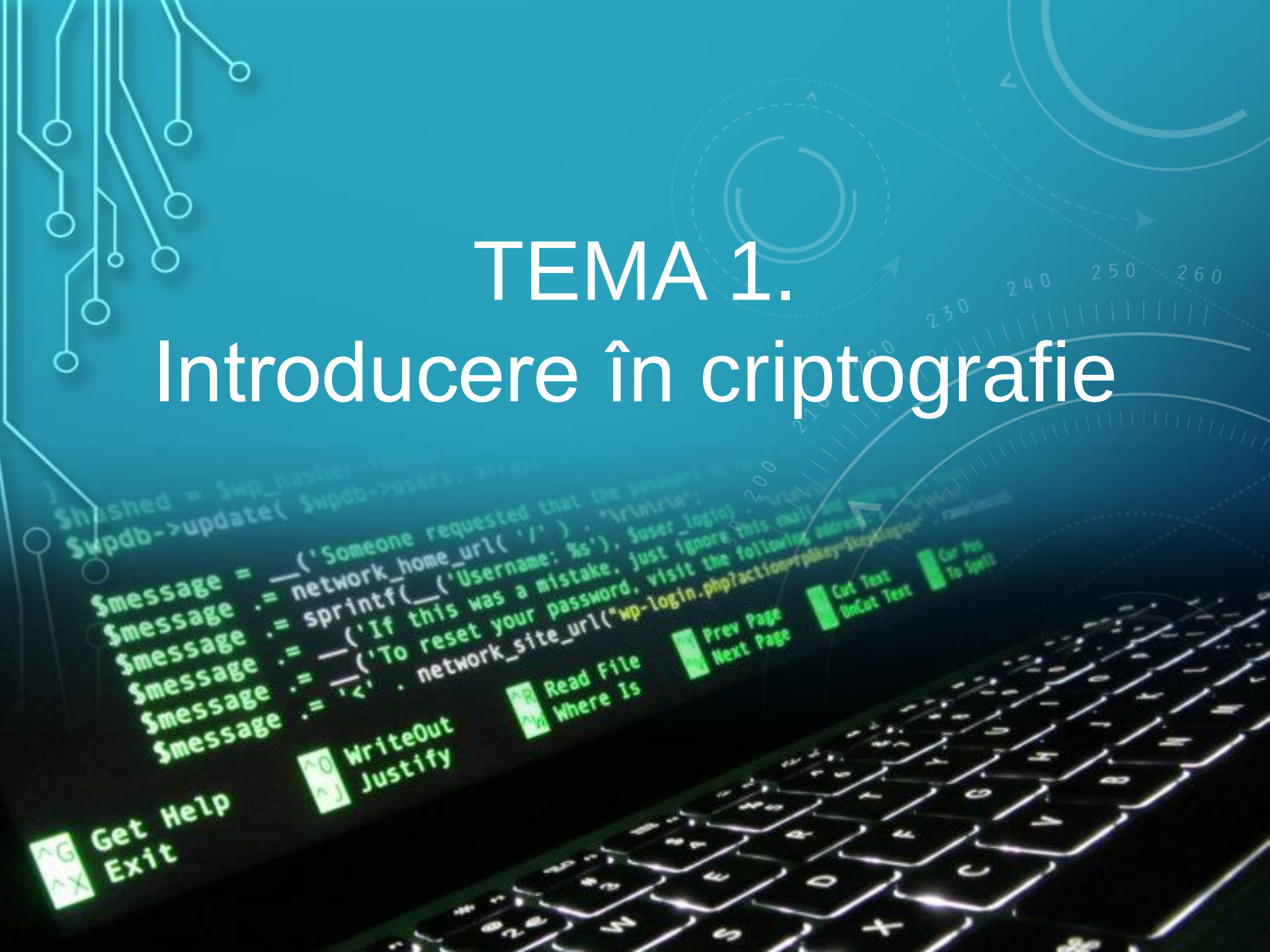
TEMA 1.
Introducere în criptografie



Repere

- Noțiuni de bază
- Studiu de caz
- Criptarea

NOȚIUNI DE BAZĂ

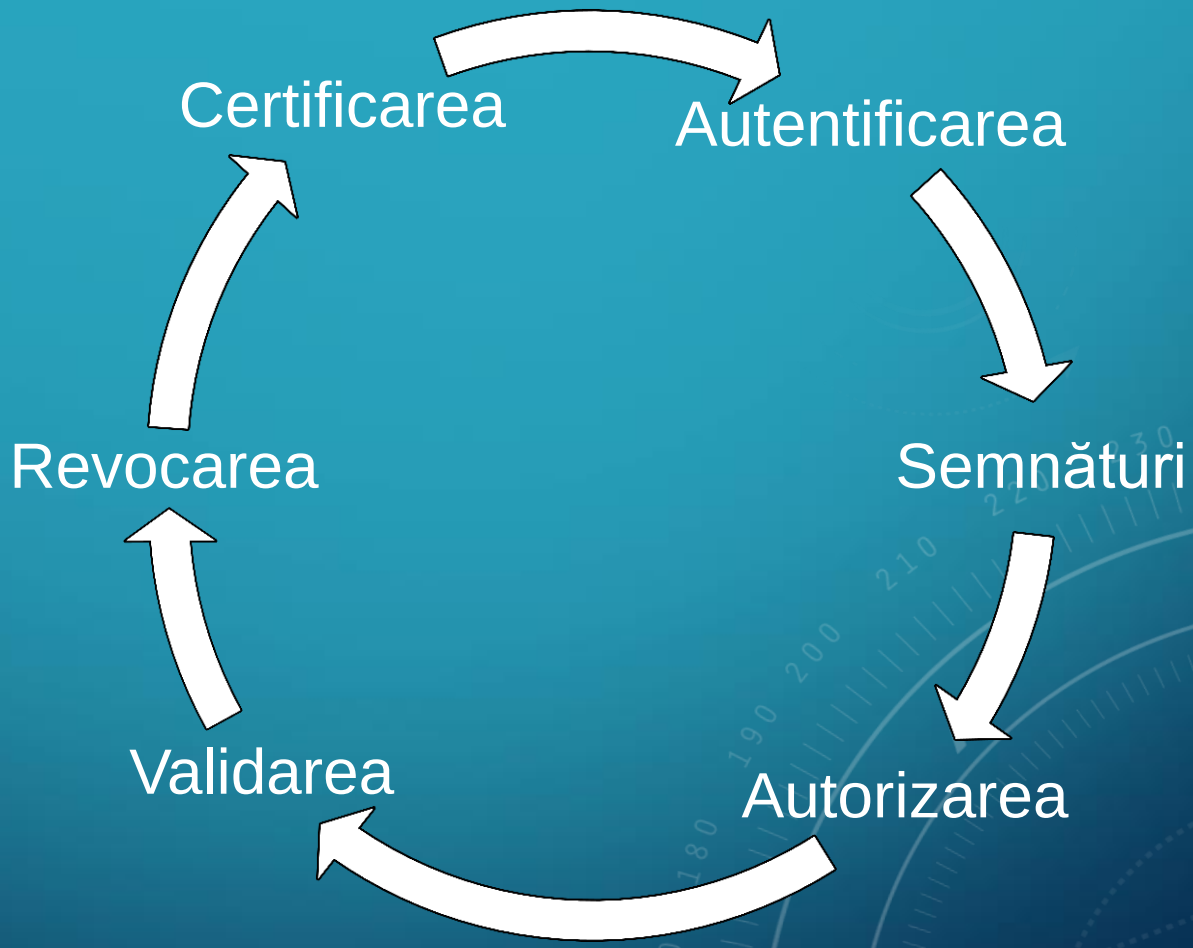
kryptós + *gráfein* = CRIPTOGRAIE

kryptós + *analýein* = CRIPTANALIZA

CRIPTOGRAIE + CRIPTANALIZA
= CRIPTOLOGIA

- Confedențialitate: păstrarea secretului informației, accesul la informația sensibilă find disponibilă doar persoanelor autorizate
- Integritate datelor: eliminarea posibilității de modicare (schimbare, inserare, ștergere) neautorizată a informației

- Disponibilitate: permiterea entităților autorizate să acceseze în timp util și fiabil informația
- Autentificare: identică o entitate conform anumitor standarde
- Non-repudiere: previne negarea unor evenimente anterioare

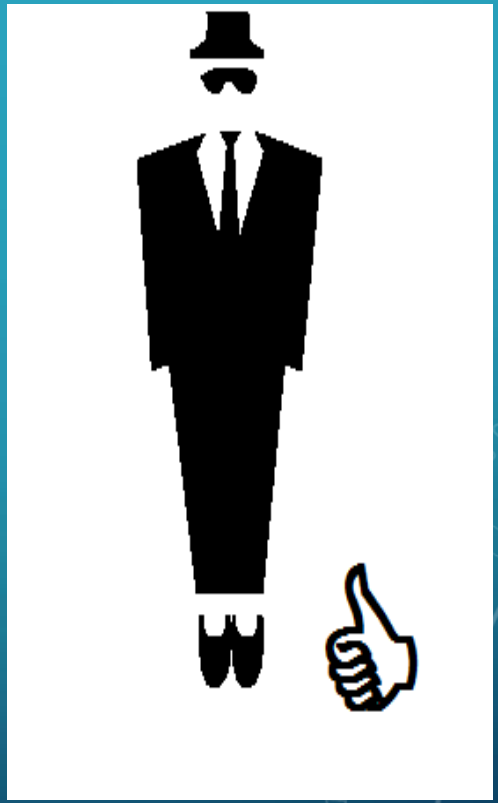

Certificarea
Autentificarea
Semnături
Autorizarea
Validarea
Revocarea

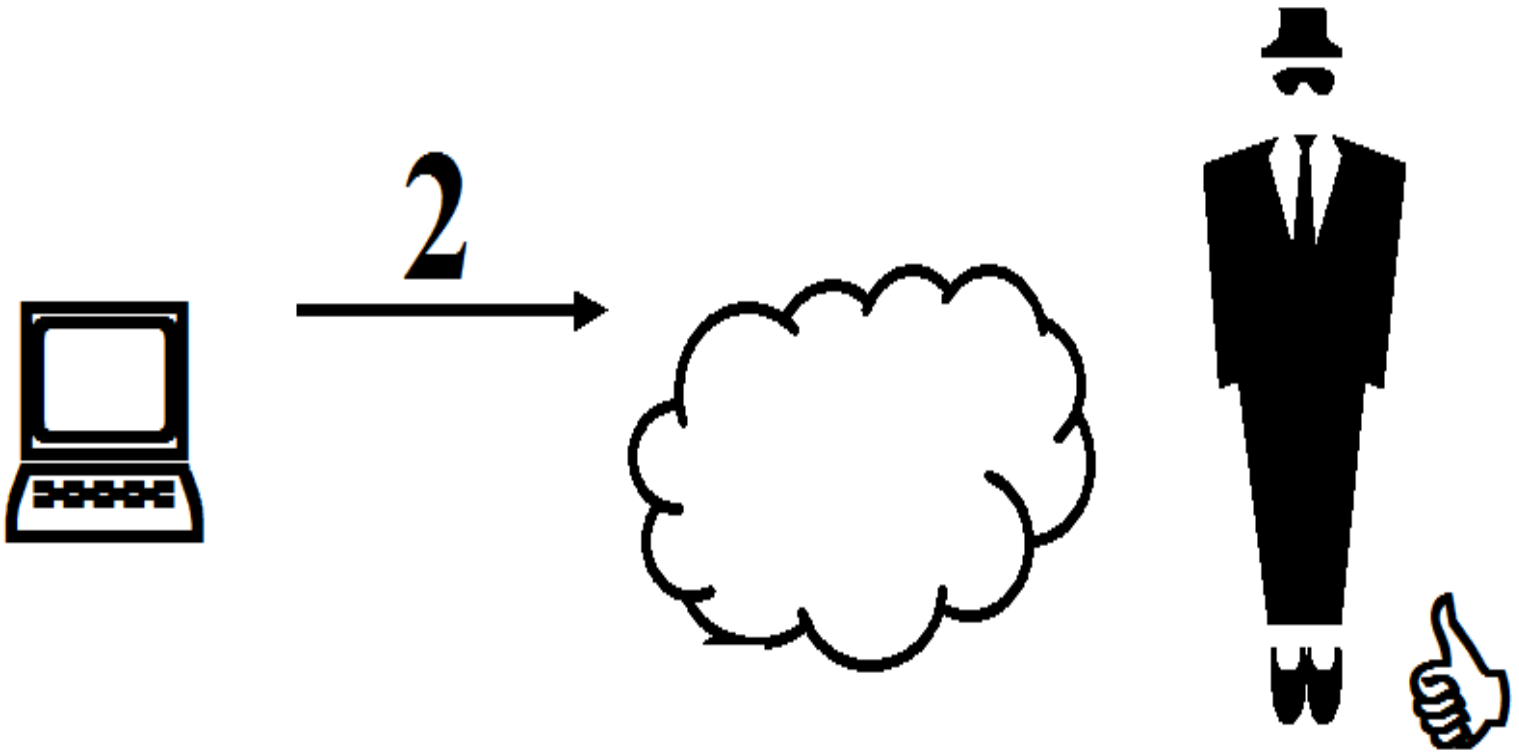
Întrebare de control

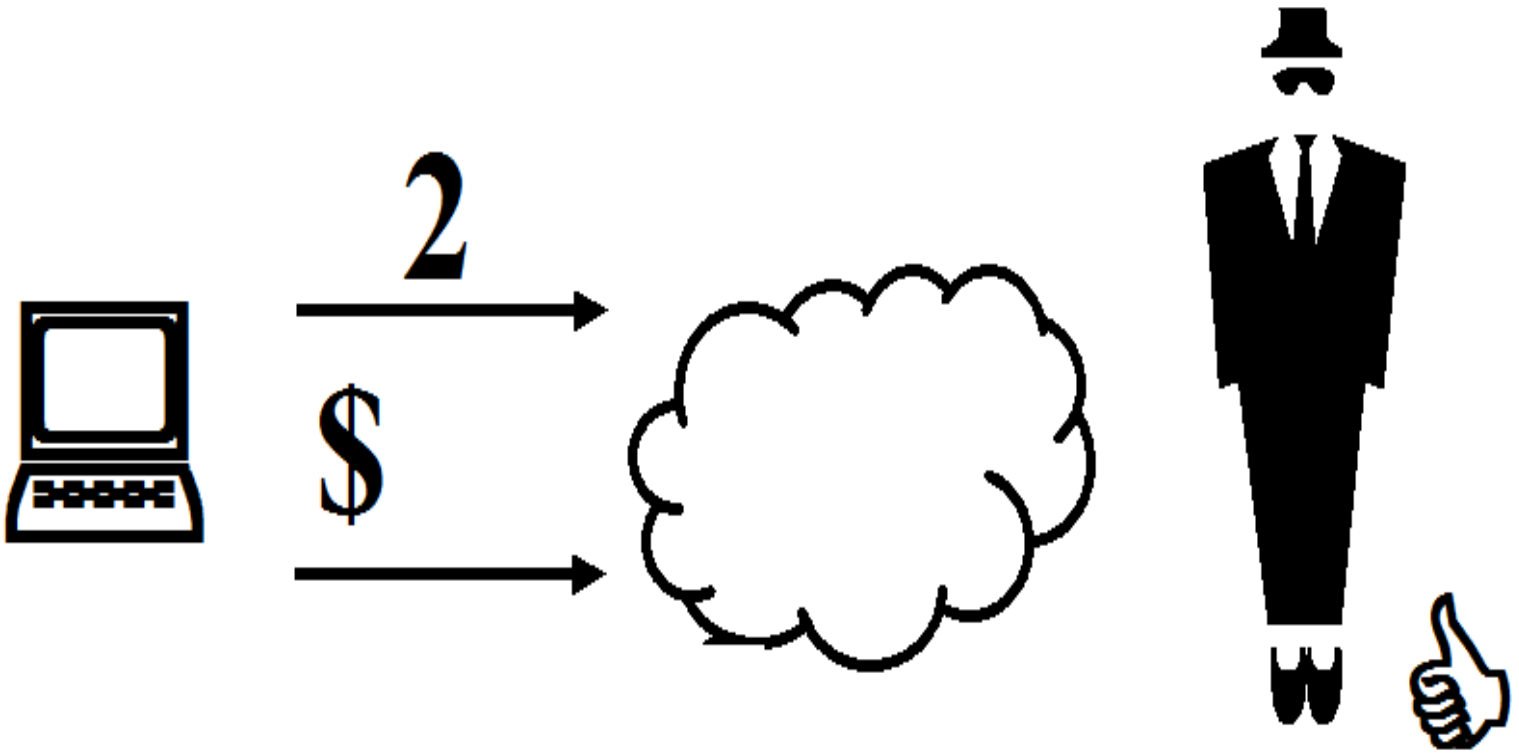
- Ce este criptologia?
- În ce domeniu poate fi aplicat?

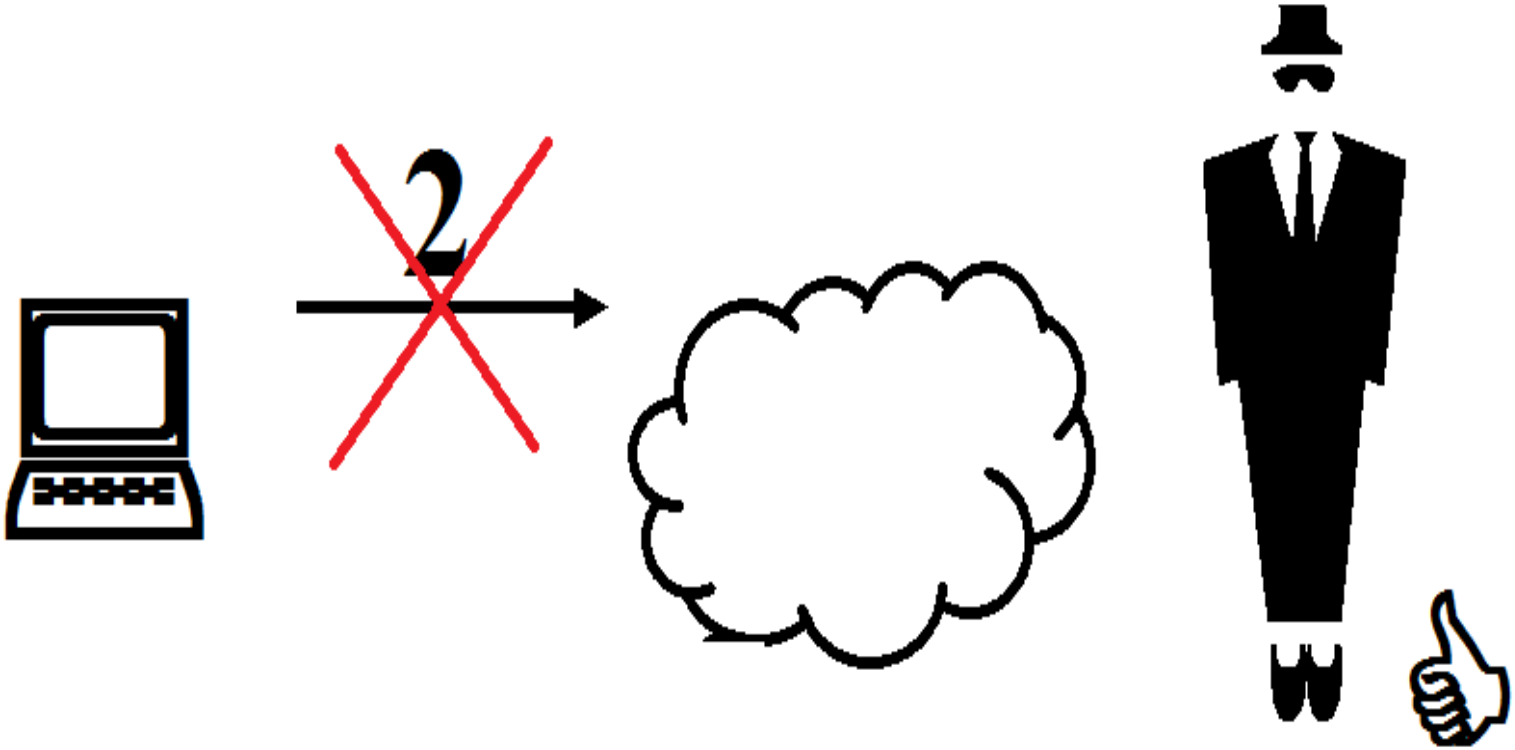
STUDIU DE CAZ

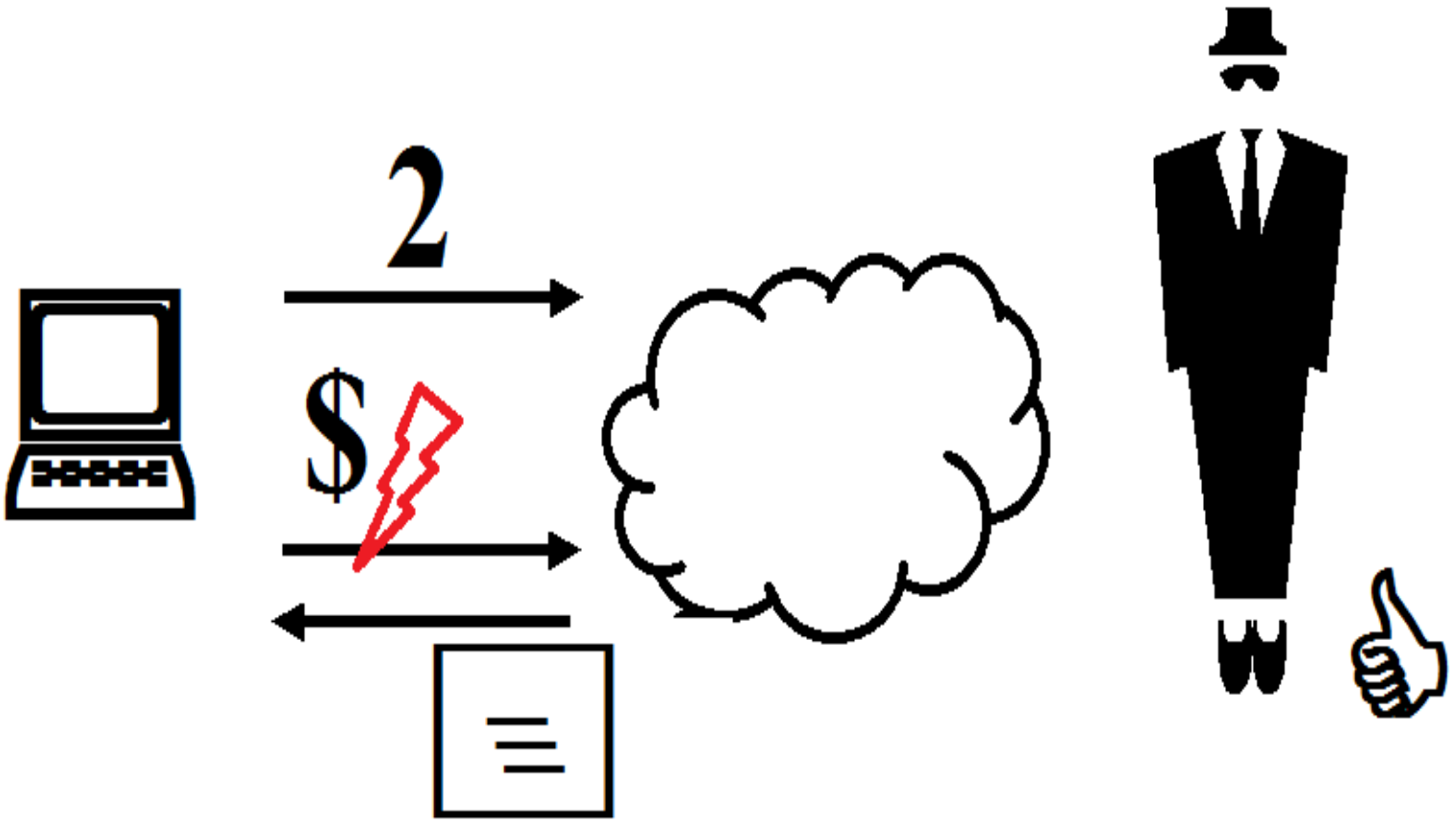
1. Un artist bun anunță un concert.
2. Biletele sunt puse în vânzare online.

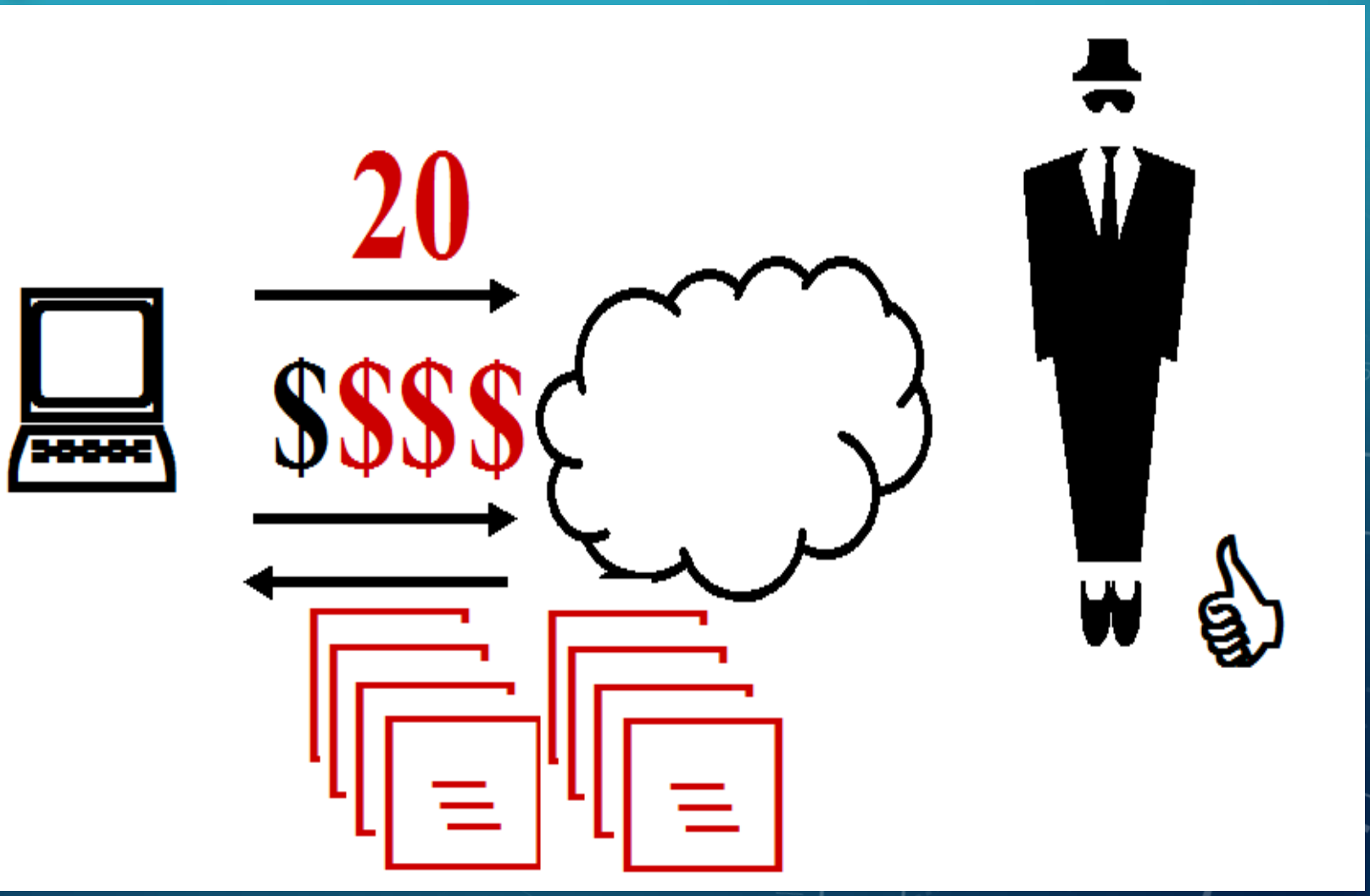


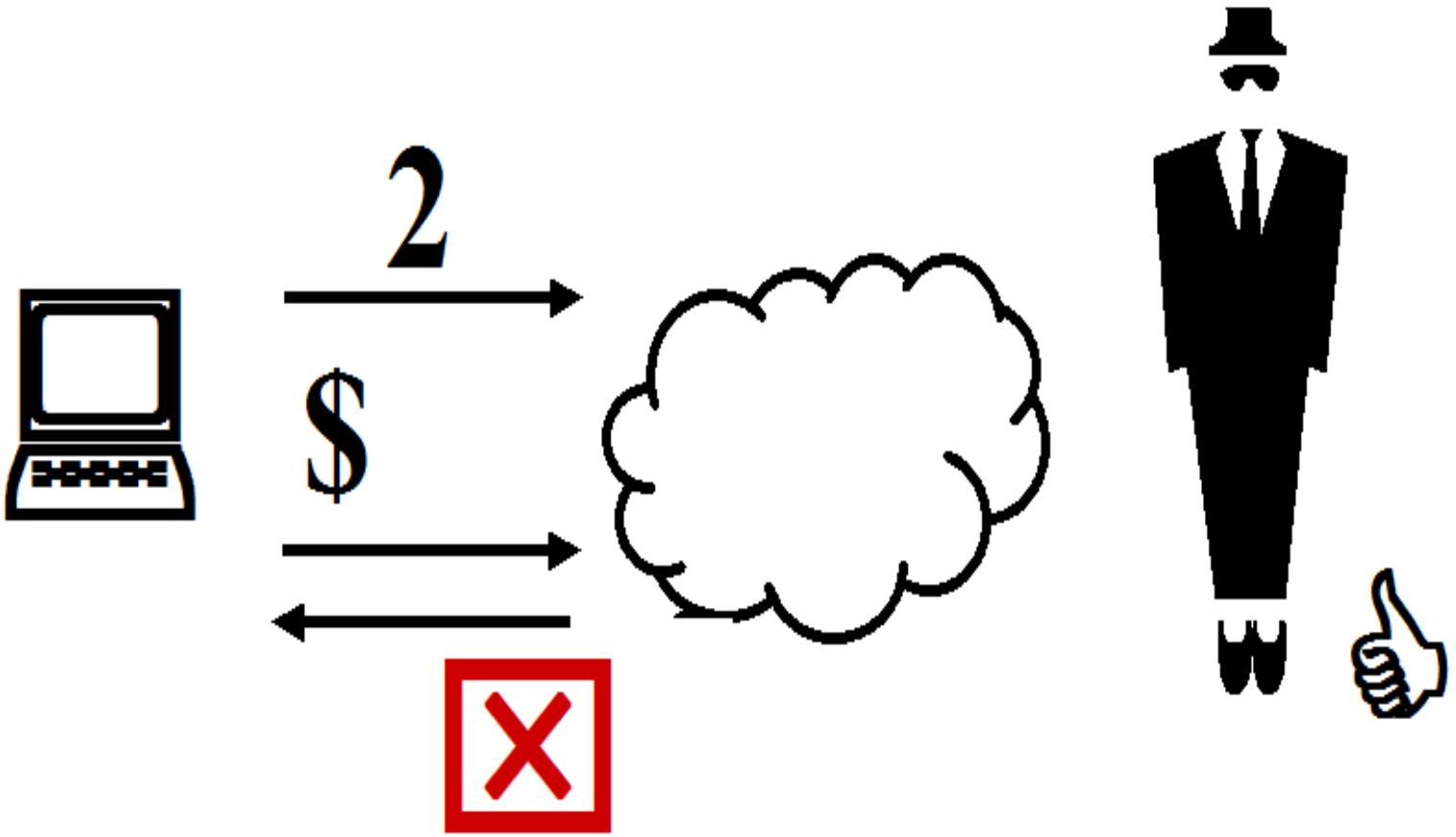

2

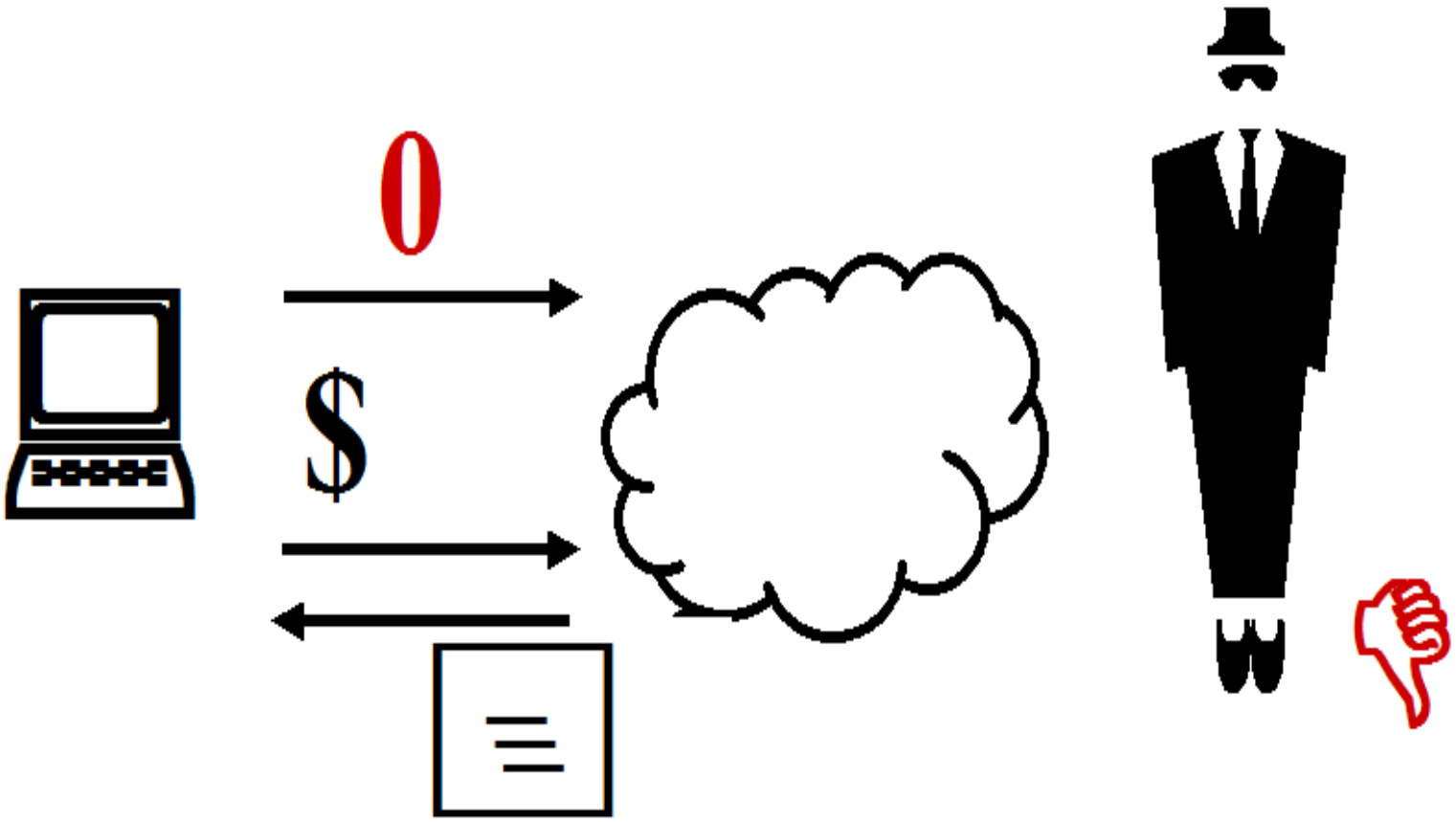

2
$


2


2
$


20
$$$$

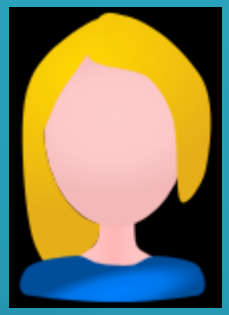

2
$


0
$

Întrebare de control

- Enumerați care sunt motivile pentru a „codifica” informația?
- Dați exemple de aplicații unde are loc criptarea datelor?

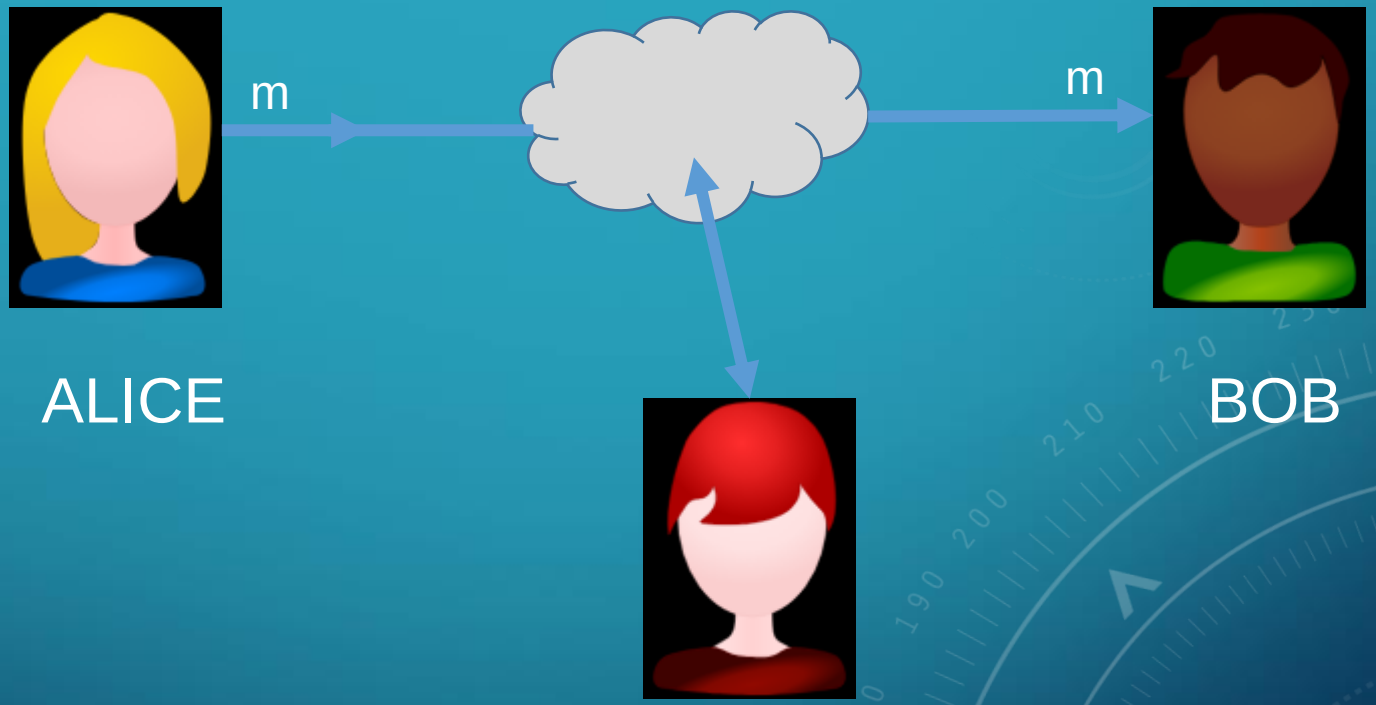
CRIPTAREA



ALICE

EVE

BOB


m
m
ALICE
BOB
EVE

P = $\{pt/pt \in T^*\}$ - spaţiul textelor în clar;

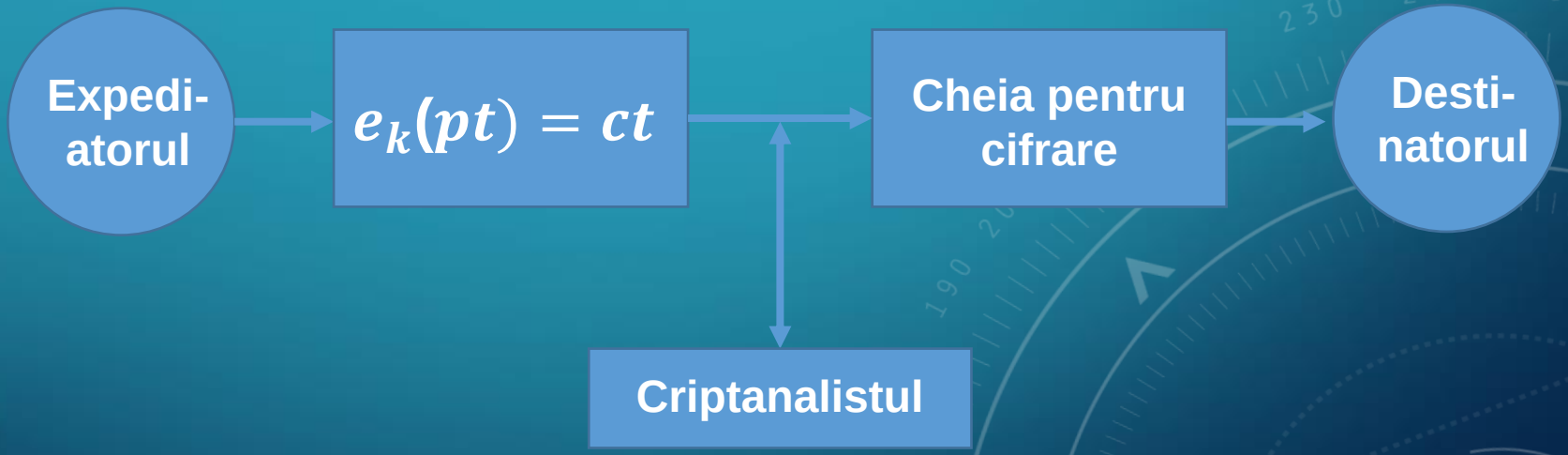
K = spaţiul cheilor de criptare k, $k \in K$;

E = $E_k : \mathrm{P} \to C, E_k = \{e_k/e_k(pt) = ct\}$;

D = $D_k : C \to P, D_k = \{d_k/d_k(e_k(pt)) = pt, \quad pt \in P\}$;

C = $\{ct$ / există $k \in K, a \in P, \ ct = E_k(a)\}$;

Schema aplicării unui sistem de criptare



Steganografia (steganography) = tehnica ascunderii mesajelor secrete în alte mesaje, în aşa fel încât existenta mesajelor secrete să fie invizibilă.

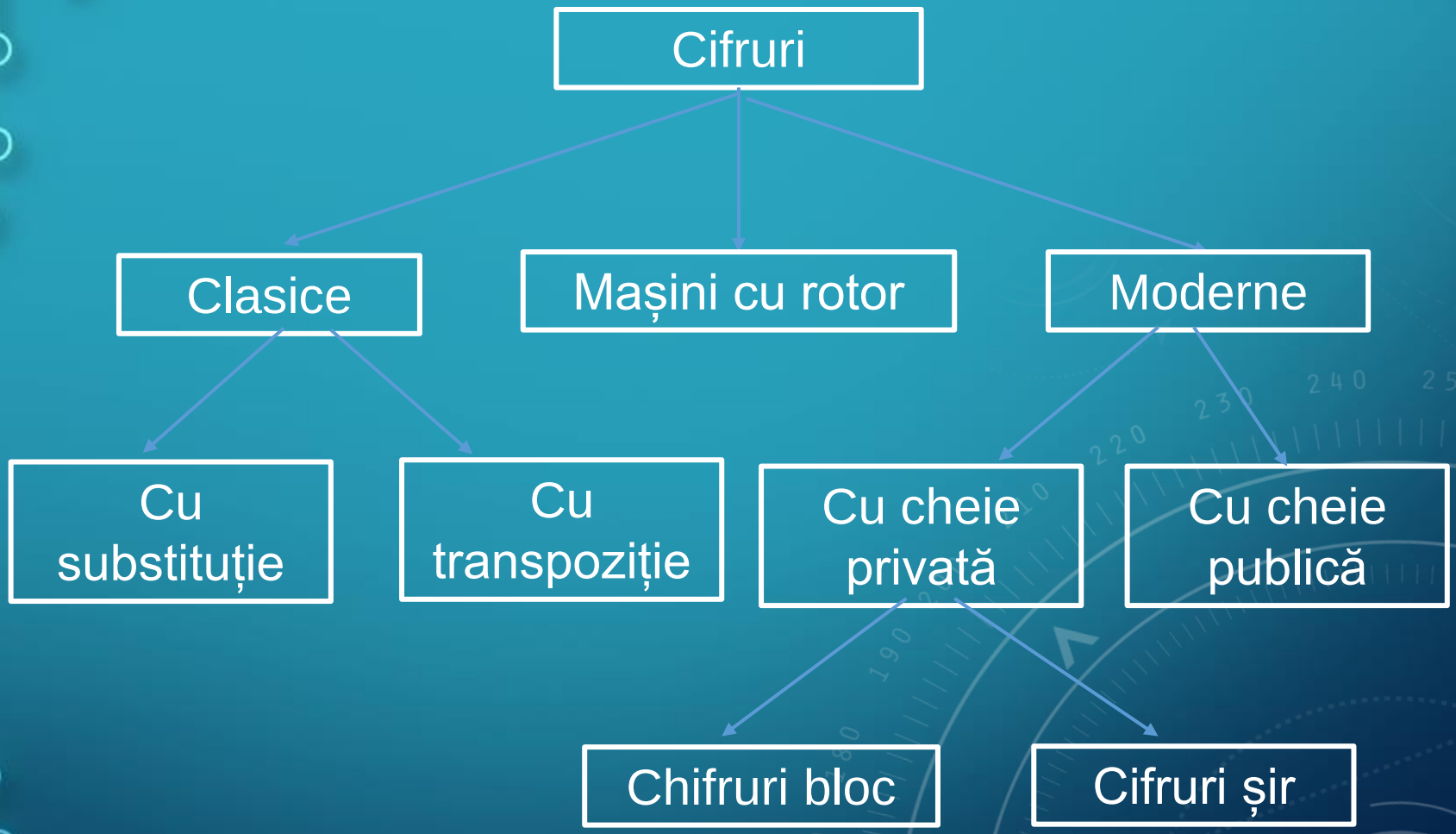
1. In funcţie de tipul operaţiilor folosite:
   - Bazate pe substituţii;
   - Bazate pe transpuneri;

2. In funcţie de tipul de chei folosite:

- Sisteme Simetrice (single-key, secret-key, private-key);
- Sisteme Asimetrice (two-key, public-key);

3. Metoda prin care datele sunt procesate:

   - Cu cifruri bloc;
   - Cu cifruri fluide (flux, şir, “stream”);


Cifruri
Clasice
Mașini cu rotor
Moderne
Cu substituție
Cu transpoziție
Cu cheie privată
Cu cheie publică
Chifruri bloc
Cifruri șir

Întrebare de control

Sistemele de criptare se clasifică...?

ÎNTREBĂRI RECAPITULATIVE

- Ce este criptologia?
- În ce domeniu poate fi aplicat?

- Enumerați care sunt motivile pentru a „codifica” informația?
- Dați exemple de aplicații unde are loc criptarea datelor?
- Sistemele de criptare se clasifică…?

NOŢIUNI DE BAZĂ ALE CRIPTOGRAFIEI