

Securitatea Sistemelor Informatice



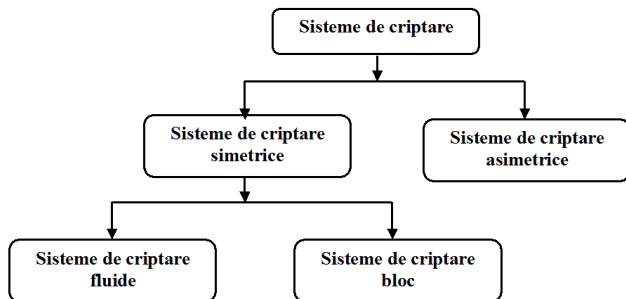
- Curs 14 -
Mai multe despre criptografie

Adela Georgescu

Facultatea de Matematică și Informatică
Universitatea din București

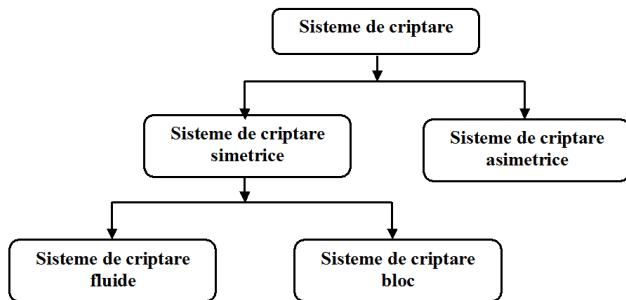
Primitive criptografice studiate

- Am studiat în timpul cursului **sisteme de criptare**:



Primitive criptografice studiate

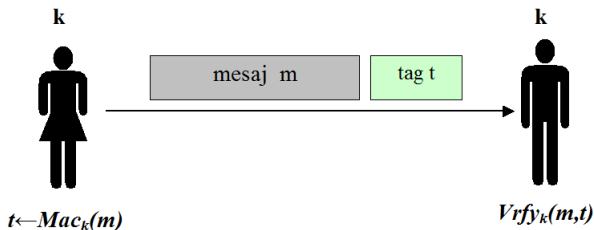
- Am studiat în timpul cursului **sisteme de criptare**:



- Acestea au rolul de a asigura **confidențialitatea**.

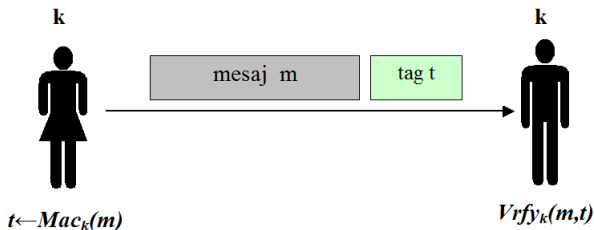
Primitive criptografice studiate

- Am studiat în timpul cursului construcțiile **MAC**, dar și **semnăturile digitale**:



Primitive criptografice studiate

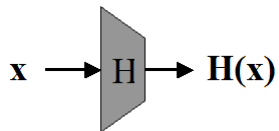
- Am studiat în timpul cursului construcțiile **MAC**, dar și **semnăturile digitale**:



- Acestea au rolul de a asigura **integritatea**.

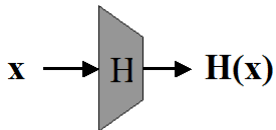
Primitive criptografice studiate

- ▶ Am studiat în timpul cursului funcții **hash**:



Primitive criptografice studiate

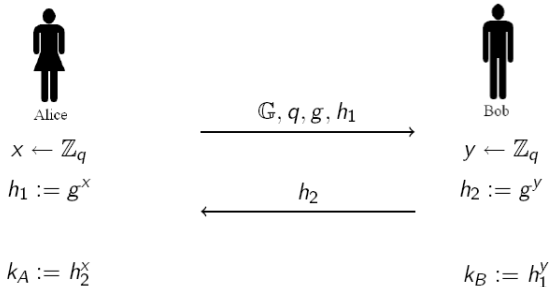
- ▶ Am studiat în timpul cursului funcții **hash**:



- ▶ Acestea asigură **integritatea** și **autentificarea** datelor prin utilizare în MAC-uri, semnături digitale...

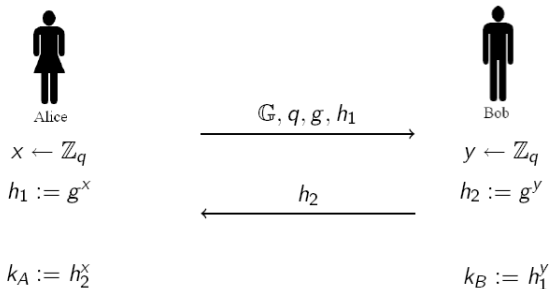
Primitive criptografice studiate

- Am studiat în timpul cursului, protocoale de **schimb de chei** (Diffie-Hellman):



Primitive criptografice studiate

- Am studiat în timpul cursului, protocoale de **schimb de chei** (Diffie-Hellman):



- Acestea asigură **stabilirea unei chei comune**, utilizată ulterior în scopuri criptografice (ex. criptare).

Alte primitive criptografice

- ▶ Am studiat sisteme de criptare care asigură confidențialitatea între 2 participanți;

Alte primitive criptografice

- ▶ Am studiat sisteme de criptare care asigură confidențialitatea între 2 participanți;
- ▶ Există însă și sisteme de criptare de tip **broadcast (broadcast encryption)**;

Alte primitive criptografice

- ▶ Am studiat sisteme de criptare care asigură confidențialitatea între 2 participanți;
- ▶ Există însă și sisteme de criptare de tip **broadcast (broadcast encryption)**;
- ▶ Acestea permit comunicarea criptată (unidirecțională) peste un canal de tip *broadcast* (către toți participanții) a.î. numai participanții autorizați să poată decripta;

Alte primitive criptografice

- ▶ Am studiat sisteme de criptare care asigură confidențialitatea între 2 participanți;
- ▶ Există însă și sisteme de criptare de tip **broadcast (broadcast encryption)**;
- ▶ Acestea permit comunicarea criptată (unidirecțională) peste un canal de tip *broadcast* (către toți participanții) a.î. numai participanții autorizați să poată decripta;
- ▶ Exemple de utilizare: transmisiuni TV criptate;

Alte primitive criptografice

- ▶ Am studiat sisteme de criptare care asigură confidențialitatea între 2 participanți;
- ▶ Există însă și sisteme de criptare de tip **broadcast (broadcast encryption)**;
- ▶ Acestea permit comunicarea criptată (unidirecțională) peste un canal de tip *broadcast* (către toți participanții) a.î. numai participanții autorizați să poată decripta;
- ▶ Exemple de utilizare: transmisiuni TV criptate;
- ▶ Noțiuni similare:
 - ▶ **threshold encryption**: pentru decriptare este necesar să coopereze un număr de participanți care să depășească un anumit prag.

Alte primitive criptografice

- ▶ Am studiat construcțiile MAC care asigură integritatea în criptografia simetrică;

Alte primitive criptografice

- ▶ Am studiat construcțiile MAC care asigură integritatea în criptografia simetrică;
- ▶ Dar și **semnăturile digitale**, care atestă în plus și originea mesajului.

Alte primitive criptografice

- ▶ Am studiat protocolul de schimb Diffie-Hellman care stabilește o cheie comună între 2 participanți;

Alte primitive criptografice

- ▶ Am studiat protocolul de schimb Diffie-Hellman care stabilește o cheie comună între 2 participanți;
- ▶ Există însă și **protocoale de stabilire a cheilor de grup**;

Alte primitive criptografice

- ▶ Am studiat protocolul de schimb Diffie-Hellman care stabilește o cheie comună între 2 participanți;
- ▶ Există însă și **protocoale de stabilire a cheilor de grup**;
- ▶ Acestea permit stabilirea unei chei comune între mai mulți participanți;

Alte primitive criptografice

- ▶ Am studiat protocolul de schimb Diffie-Hellman care stabilește o cheie comună între 2 participanți;
- ▶ Există însă și **protocoale de stabilire a cheilor de grup**;
- ▶ Acestea permit stabilirea unei chei comune între mai mulți participanți;
- ▶ Exemple de utilizare: comunicație criptată, (video-) conferințe, acces la resurse ...

Alte primitive criptografice

- ▶ **Schemele de partajare a secretelor** permit partajarea unui secret în mai multe componente distribuite unor participanți astfel încât numai mulțimile *autorizate* de participanți să poată reconstitui secretul;

Alte primitive criptografice

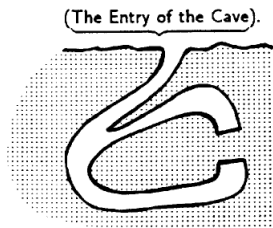
- ▶ **Schemele de partajare a secretelor** permit partajarea unui secret în mai multe componente distribuite unor participanți astfel încât numai mulțimile *autorizate* de participanți să poată reconstitui secretul;
- ▶ Exemple de utilizare: controlul accesului, stocarea fișierelor în cloud, ...

Alte primitive criptografice

- ▶ **Schemele de partajare a secretelor** permit partajarea unui secret în mai multe componente distribuite unor participanți astfel încât numai mulțimile *autorizate* de participanți să poată reconstitui secretul;
- ▶ Exemple de utilizare: controlul accesului, stocarea fișierelor în cloud, ...
- ▶ Alte primitive criptografice la nivel de grup: **multiparty computation, protocoale de vot electronic** ...

Alte primitive criptografice

- Protocoale de tip **zero-knowledge** permit unei entități (*prover*) să demonstreze cunoașterea unui secret unei alte entități (*verifier*) fara a dezvalui nici un fel de informatie despre secret;



[J.J.Quisquater, L.C.Guillou, T.A.Berson,
How to Explain Zero-Knowledge Protocols to Your Children]

Mai mult despre criptografie

- ▶ Am studiat criptografia bazată pe teoria numerelor și criptografia bazată pe curbe eliptice;

Mai mult despre criptografie

- ▶ Am studiat criptografia bazată pe teoria numerelor și criptografia bazată pe curbe eliptice;
- ▶ Dar există și alte tipuri de criptografie, precum **criptografia bazată pe latici**:



$$\{\sum_{i=1}^n a_i v_i \mid a_i \in \mathbb{Z}, v_i \text{ bază}\}$$

Mai mult despre criptografie

- ▶ Am studiat criptografia bazată pe teoria numerelor și criptografia bazată pe curbe eliptice;
- ▶ Dar există și alte tipuri de criptografie, precum **criptografia bazată pe latici**:

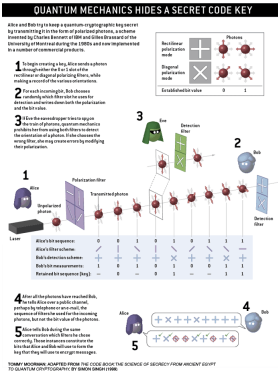


$$\{\sum_{i=1}^n a_i v_i \mid a_i \in \mathbb{Z}, v_i \text{ bază}\}$$

- ▶ Probleme dificile: **SVP (Shortest Vector Problem)**, **CVP (Closest Vector Problem)**, ...

Mai mult despre criptografie

► Criptografia cuantică:



Important de reținut!

- ▶ Există încă multe aspecte criptografice interesante de studiat!