



# Criptografie și Securitate

## - Prelegerea 16 - Criptografia asimetrică

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

# Cuprins

1. Limitările criptografiei simetrice

2. Criptografia asimetrică

# Limitările criptografiei simetrice

- ▶ Am studiat până acum criptografia simetrică;

# Limitările criptografiei simetrice

- ▶ Am studiat până acum criptografia simetrică;
- ▶ Aceasta asigură confidențialitatea și integritatea mesajelor transmise pe canale nesecurizate;

# Limitările criptografiei simetrice

- ▶ Am studiat până acum criptografia simetrică;
- ▶ Aceasta asigură confidențialitatea și integritatea mesajelor transmise pe canale nesecurizate;
- ▶ Însă rămân multe probleme nerezolvate...

# Problema 1 - Distribuirea cheilor

- ▶ Criptarea simetrică necesită o cheie secretă comună părților comunicante;

# Problema 1 - Distribuirea cheilor

- ▶ Criptarea simetrică necesită o cheie secretă comună părților comunicante;
- ▶ **Întrebare:** Cum se obțin și se distribuie aceste chei?

# Problema 1 - Distribuirea cheilor

- ▶ Criptarea simetrică necesită o cheie secretă comună părților comunicante;
- ▶ **Întrebare:** Cum se obțin și se distribuie aceste chei?
- ▶ **Varianta 1.** Se transmit printr-un canal de comunicație nesecurizat;



# Problema 1 - Distribuirea cheilor

- ▶ Criptarea simetrică necesită o cheie secretă comună părților comunicante;
- ▶ **Întrebare:** Cum se obțin și se distribuie aceste chei?
- ▶ **Varianta 1.** Se transmit printr-un canal de comunicație nesecurizat;
- ▶ NU! Un adversar pasiv le poate intercepta și utiliza ulterior pentru decriptarea comunicației.

# Problema 1 - Distribuirea cheilor

- ▶ **Varianta 2.** Se transmite printr-un canal de comunicație sigur care presupune un serviciu de mesagerie de încredere;

# Problema 1 - Distribuirea cheilor

- ▶ **Varianta 2.** Se transmite printr-un canal de comunicație sigur care presupune un serviciu de mesagerie de încredere;
- ▶ Opțiunea poate fi posibilă la nivel guvernamental sau militar;

# Problema 1 - Distribuirea cheilor

- ▶ **Varianta 2.** Se transmit printr-un canal de comunicație sigur care presupune un serviciu de mesagerie de încredere;
- ▶ Opțiunea poate fi posibilă la nivel guvernamental sau militar;
- ▶ Dar nu va fi niciodată posibilă în cazul organizațiilor numeroase;

# Problema 1 - Distribuirea cheilor

- ▶ **Varianta 2.** Se transmite printr-un canal de comunicație sigur care presupune un serviciu de mesagerie de încredere;
- ▶ Opțiunea poate fi posibilă la nivel guvernamental sau militar;
- ▶ Dar nu va fi niciodată posibilă în cazul organizațiilor numeroase;
- ▶ Presupunem doar cazul în care fiecare manager trebuie să partajeze o cheie secretă cu fiecare subordonat;

# Problema 1 - Distribuirea cheilor

- ▶ **Varianta 2.** Se transmit printr-un canal de comunicație sigur care presupune un serviciu de mesagerie de încredere;
- ▶ Opțiunea poate fi posibilă la nivel guvernamental sau militar;
- ▶ Dar nu va fi niciodată posibilă în cazul organizațiilor numeroase;
- ▶ Presupunem doar cazul în care fiecare manager trebuie să partajeze o cheie secretă cu fiecare subordonat;
- ▶ Problemele care apar sunt multiple: pentru fiecare nou angajat este necesară stabilirea cheilor, organizația are sedii în mai multe țări, ...

## Problema 2 - Stocarea secretă a cheilor

- ▶ Rămânem la exemplul anterior al unei organizații numeroase cu  $N$  angajați;

## Problema 2 - Stocarea secretă a cheilor

- ▶ Rămânem la exemplul anterior al unei organizații numeroase cu  $N$  angajați;
- ▶ **Întrebare:** Câte chei sunt necesare pentru ca fiecare 2 angajați să poată comunica criptat?



## Problema 2 - Stocarea secretă a cheilor

- ▶ Rămânem la exemplul anterior al unei organizații numeroase cu  $N$  angajați;
- ▶ **Întrebare:** Câte chei sunt necesare pentru ca fiecare 2 angajați să poată comunica criptat?
- ▶ **Răspuns:**  $C_N^2 = N(N - 1)/2$ ;

## Problema 2 - Stocarea secretă a cheilor

- ▶ Rămânem la exemplul anterior al unei organizații numeroase cu  $N$  angajați;
- ▶ **Întrebare:** Câte chei sunt necesare pentru ca fiecare 2 angajați să poată comunica criptat?
- ▶ **Răspuns:**  $C_N^2 = N(N - 1)/2$ ;
- ▶ La acestea se adaugă cheile necesare pentru accesul la resurse (servere, imprimante, baze de date ...);

## Problema 2 - Stocarea secretă a cheilor

- ▶ Rămânem la exemplul anterior al unei organizații numeroase cu  $N$  angajați;
- ▶ **Întrebare:** Câte chei sunt necesare pentru ca fiecare 2 angajați să poată comunica criptat?
- ▶ **Răspuns:**  $C_N^2 = N(N - 1)/2$ ;
- ▶ La acestea se adaugă cheile necesare pentru accesul la resurse (servere, imprimante, baze de date ...);
- ▶ Apare o problemă de **logistică**: foarte multe chei sunt dificil de menținut și utilizat;

## Problema 2 - Stocarea secretă a cheilor

- ▶ Rămânem la exemplul anterior al unei organizații numeroase cu  $N$  angajați;
- ▶ **Întrebare:** Câte chei sunt necesare pentru ca fiecare 2 angajați să poată comunica criptat?
- ▶ **Răspuns:**  $C_N^2 = N(N - 1)/2$ ;
- ▶ La acestea se adaugă cheile necesare pentru accesul la resurse (servere, imprimante, baze de date ...);
- ▶ Apare o problemă de **logistică**: foarte multe chei sunt dificil de menținut și utilizat;
- ▶ Și apare o problemă de **securitate**: cu cât sunt mai multe chei, cu atât sunt mai dificil de stocat în mod sigur, deci cresc șansele de a fi furate de adversari;

## Problema 2 - Stocarea secretă a cheilor

- ▶ Sistemele informatice sunt deseori infectate de programe malițioase care fură cheile secrete și le transmit prin internet către atacator;

## Problema 2 - Stocarea secretă a cheilor

- ▶ Sistemele informatice sunt deseori infectate de programe malițioase care fură cheile secrete și le transmit prin internet către atacator;
- ▶ Totuși dacă numărul de chei este mic, există soluții de stocare cu securitate crescută;

## Problema 2 - Stocarea secretă a cheilor

- ▶ Sistemele informatice sunt deseori infectate de programe malițioase care fură cheile secrete și le transmit prin internet către atacator;
- ▶ Totuși dacă numărul de chei este mic, există soluții de stocare cu securitate crescută;
- ▶ Un exemplu îl reprezintă dispozitivele de tip *smartcard*;

## Problema 2 - Stocarea secretă a cheilor

- ▶ Sistemele informatice sunt deseori infectate de programe malițioase care fură cheile secrete și le transmit prin internet către atacator;
- ▶ Totuși dacă numărul de chei este mic, există soluții de stocare cu securitate crescută;
- ▶ Un exemplu îl reprezintă dispozitivele de tip *smartcard*;
- ▶ Acestea realizează calculele criptografice folosind cheia stocată, asigurând faptul că niciodată cheia secretă nu ajunge în calculator;



## Problema 2 - Stocarea secretă a cheilor

- ▶ Sistemele informatice sunt deseori infectate de programe malițioase care fură cheile secrete și le transmit prin internet către atacator;
- ▶ Totuși dacă numărul de chei este mic, există soluții de stocare cu securitate crescută;
- ▶ Un exemplu îl reprezintă dispozitivele de tip *smartcard*;
- ▶ Acestea realizează calculele criptografice folosind cheia stocată, asigurând faptul că niciodată cheia secretă nu ajunge în calculator;
- ▶ Capacitatea de stocare a unui smartcard este însă limitată, neputând memora, de exemplu mii de chei criptografice.

## Problema 3 - Medii de comunicare deschise

- ▶ Deși dificil de stocat sau utilizat, criptografia simetrică ar putea (cel puțin în teorie) să rezolve aceste probleme;

## Problema 3 - Medii de comunicare deschise

- ▶ Deși dificil de stocat sau utilizat, criptografia simetrică ar putea (cel puțin în teorie) să rezolve aceste probleme;
- ▶ Dar este insuficientă în medii deschise, în care participanții nu se întâlnesc niciodată;

## Problema 3 - Medii de comunicare deschise

- ▶ Deși dificil de stocat sau utilizat, criptografia simetrică ar putea (cel puțin în teorie) să rezolve aceste probleme;
- ▶ Dar este insuficientă în medii deschise, în care participanții nu se întâlnesc niciodată;
- ▶ Astfel de exemple includ: o tranzacție prin internet sau un e-mail transmis unei persoane necunoscute;

*"Solutions that are based on private-key cryptography are not sufficient to deal with the problem of secure communication in open systems where parties cannot physically meet, or where parties have transient interactions."*

(J.Katz, Y.Lindell: Introduction to Modern Cryptography)

## Problema 4 - Imposibilitatea non-repudierii

- ▶ O cheie simetrică este deținută de cel puțin 2 părți;

## Problema 4 - Imposibilitatea non-repudierii

- ▶ O cheie simetrică este deținută de cel puțin 2 părți;
- ▶ Este imposibil de demonstrat de exemplu că un MAC a fost produs de una dintre cele 2 părți comunicante;

## Problema 4 - Imposibilitatea non-repudierii

- ▶ O cheie simetrică este deținută de cel puțin 2 părți;
- ▶ Este imposibil de demonstrat de exemplu că un MAC a fost produs de una dintre cele 2 părți comunicante;
- ▶ De aceea nu se poate utiliza autentificarea simetrică pentru a atesta sursa unui mesaj sau document.

# Criptografia asimetrică

- ▶ Criptografia cu cheie publică este introdusă de W.Diffie și M.Hellman în 1976 ca o soluție la problemele enumerate anterior:

*"Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of written signature. This paper suggests ways to solve these currently open problems."*

(W.Diffie, M.Hellman: New Directions in Cryptography - abstract)





# Criptografia asimetrică



[[http://cisac.stanford.edu/people/whitfield\\_diffie/](http://cisac.stanford.edu/people/whitfield_diffie/)]



[<http://www-ee.stanford.edu/~hellman/>]



Home > Awards > CRYPTOGRAPHY PIONEERS RECEIVE ACM A.M. TURING AWARD

## CRYPTOGRAPHY PIONEERS RECEIVE ACM A.M. TURING AWARD

### Diffie and Hellman's Invention of Public-Key Cryptography and Digital Signatures Revolutionized Computer Security

ACM, the Association for Computing Machinery, today named Whitfield Diffie, former Chief Security Officer of Sun Microsystems and Martin E. Hellman, Professor Emeritus of Electrical Engineering at Stanford University, recipients of the 2015 ACM A.M. Turing Award for critical contributions to modern cryptography. The ability for two parties to use encryption to communicate privately over an otherwise insecure channel is fundamental for billions of people around the world. On a daily basis, individuals establish secure online connections with banks, e-commerce sites, email servers and the cloud. Diffie and Hellman's

[<https://www.acm.org/awards/2015-turing>]

# Sisteme de criptare asimetrice

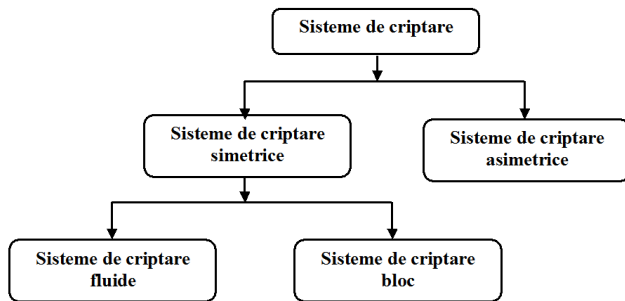
- ▶ Am studiat sisteme de criptare care folosesc **aceeași cheie** pentru criptare și decriptare - **sisteme de criptare simetrice**;

# Sisteme de criptare asimetrice

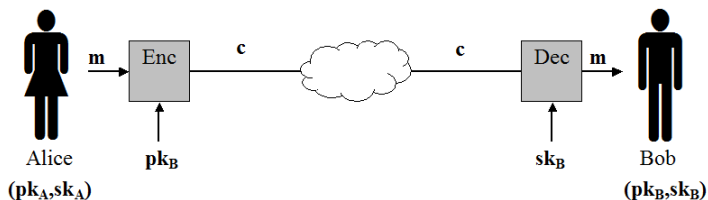
- ▶ Am studiat sisteme de criptare care folosesc **aceeași cheie** pentru criptare și decriptare - **sisteme de criptare simetrice**;
- ▶ Vom studia sisteme de criptare care folosesc **chei diferite** pentru criptare și decriptare - **sisteme de criptare asimetrice**;

# Sisteme de criptare asimetrice

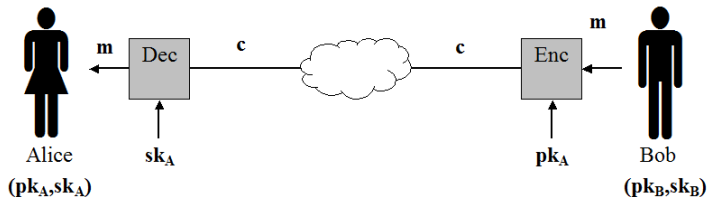
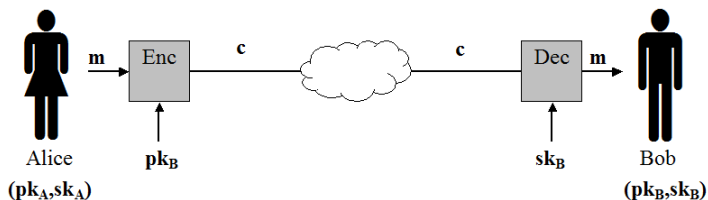
- ▶ Am studiat sisteme de criptare care folosesc **aceeași cheie** pentru criptare și decriptare - **sisteme de criptare simetrice**;
- ▶ Vom studia sisteme de criptare care folosesc **chei diferite** pentru criptare și decriptare - **sisteme de criptare asimetrice**;



# Criptarea asimetrică (cu cheie publică)



# Criptarea asimetrică (cu cheie publică)



# Criptarea asimetrică (cu cheie publică)

## Definiție

Un *sistem de criptare asimetric* definit peste  $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ , cu:

- ▶  $\mathcal{K} = \mathcal{K}_{pk} \times \mathcal{K}_{sk} =$  spațiul cheilor, de forma unor perechi  $(pk, sk)$ , unde  $pk$  este **cheia publică** și  $sk$  este **cheia secretă**
- ▶  $\mathcal{M} =$  spațiul textelor clare (mesaje)
- ▶  $\mathcal{C} =$  spațiul textelor criptate

este un dublet  $(\text{Enc}, \text{Dec})$ , unde:

1.  $\text{Enc} : \mathcal{K}_{pk} \times \mathcal{M} \rightarrow \mathcal{C}$
2.  $\text{Dec} : \mathcal{K}_{sk} \times \mathcal{C} \rightarrow \mathcal{M}$

a.î.  $\forall m \in \mathcal{M}, (pk, sk) \in \mathcal{K} : \text{Dec}_{sk}(\text{Enc}_{pk}(m)) = m.$



# Terminologie

- Spre deosebire de criptarea simetrică, criptarea asimetrică folosește o pereche de chei:

# Terminologie

- ▶ Spre deosebire de criptarea simetrică, criptarea asimetrică folosește o pereche de chei:
- ▶ Cheia publică **pk** este folosită pentru criptare;

# Terminologie

- ▶ Spre deosebire de criptarea simetrică, criptarea asimetrică folosește o pereche de chei:
- ▶ Cheia publică **pk** este folosită pentru criptare;
- ▶ Cheia secretă **sk** este folosită pentru decriptare;

# Terminologie

- ▶ Spre deosebire de criptarea simetrică, criptarea asimetrică folosește o pereche de chei:
- ▶ Cheia publică **pk** este folosită pentru criptare;
- ▶ Cheia secretă **sk** este folosită pentru decriptare;
- ▶ Cheia publică este larg răspândită pentru a asigura posibilitatea de criptare oricui dorește să transmită un mesaj către entitatea căreia îi corespunde;

# Terminologie

- ▶ Spre deosebire de criptarea simetrică, criptarea asimetrică folosește o pereche de chei:
- ▶ Cheia publică **pk** este folosită pentru criptare;
- ▶ Cheia secretă **sk** este folosită pentru decriptare;
- ▶ Cheia publică este larg răspândită pentru a asigura posibilitatea de criptare oricui dorește să transmită un mesaj către entitatea căreia îi corespunde;
- ▶ Cheia secretă este privată și nu se cunoaște decât de entitatea căreia îi corespunde;

# Terminologie

- ▶ Spre deosebire de criptarea simetrică, criptarea asimetrică folosește o pereche de chei:
- ▶ Cheia publică **pk** este folosită pentru criptare;
- ▶ Cheia secretă **sk** este folosită pentru decriptare;
- ▶ Cheia publică este larg răspândită pentru a asigura posibilitatea de criptare oricui dorește să transmită un mesaj către entitatea căreia îi corespunde;
- ▶ Cheia secretă este privată și nu se cunoaște decât de entitatea căreia îi corespunde;
- ▶ Considerăm (pentru simplitate) că ambele chei au lungime cel puțin  $n$  biți.

# Criptografia asimetrică vs. Criptografia simetrică

## Criptografia simetrică

- ▶ necesită secretizarea întregii chei
- ▶ folosește aceeași cheie pentru criptare și decriptare
- ▶ rolurile emițătorului și ale receptorului pot fi schimbate
- ▶ pentru ca un utilizator să primească mesaje criptate de la mai mulți emițători, trebuie să partajeze cu fiecare câte o cheie

## Criptografia asimetrică

- ▶ necesită secretizarea unei jumătăți din cheie
- ▶ folosește chei distincte pentru criptare și decriptare
- ▶ rolurile emițătorului și ale receptorului nu pot fi schimbate
- ▶ o pereche de chei asimetrice permite oricui să transmită informație criptată către entitatea căreia îi corespunde

# Criptografia asimetrică

## Avantaje

- ▶ număr mai mic de chei
- ▶ simplifică problema distribuirii cheilor
- ▶ fiecare participant trebuie să stocheze o singură cheie secretă de lungă durată
- ▶ permite comunicarea sigură pe canale publice
- ▶ rezolvă problema mediilor de comunicare deschise

## Dezavantaje

- ▶ criptarea asimetrică este mult mai lentă decât criptarea simetrică
- ▶ compromiterea cheii private conduce la compromiterea tuturor mesajelor criptate primite, indiferent de sursă
- ▶ necesită verificarea autenticității cheii publice (PKI rezolvă această problemă)



# Important de reținut!

- ▶ Criptografia simetrică NU rezolvă toate problemele criptografiei
- ▶ Criptografia asimetrică apare în completarea criptografiei simetrice