



Criptografie și Securitate

- Prelegerea 1 - Introducere. Motivație. Principii

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

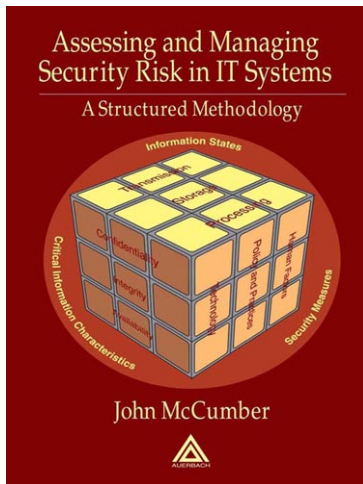
1. Ce este criptografia?
2. Motivație
3. Principiile lui Kerckhoffs

Ce este criptografia?

cripto + graphe (scriere) = "scriere secretă"

- ▶ *scriere secretă cu ajutorul unui cod de semne convenționale* DEX (1998), Dicționar Enciclopedic (1993)
- ▶ *the art or writing or solving codes*, The Concise Oxford Dictionary (2006)
- ▶ *the scientific study of techniques for securing digital information, transactions, and distributed computations*, J.Katz, Y.Lindell, *Introduction to Modern Cryptography* (2008)

Cubul McCumber (1991)



Obiectivele criptografiei

Confidențialitate: păstrarea secretului informației, accesul la informația sensibilă fiind disponibilă doar persoanelor autorizate.

Obiectivele criptografiei

Confidențialitate: păstrarea secretului informației, accesul la informația sensibilă fiind disponibilă doar persoanelor autorizate.

Integritate (a datelor): eliminarea posibilității de modificare (schimbare, inserare, ștergere) neautorizată a informației.

Obiectivele criptografiei

***Confidențialitate:** păstrarea secretului informației, accesul la informația sensibilă fiind disponibilă doar persoanelor autorizate.*

***Integritate (a datelor):** eliminarea posibilității de modificare (schimbare, inserare, ștergere) neautorizată a informației.*

***Disponibilitate:** permiterea entităților autorizate să acceseze în timp util și fiabil informația.*

Obiectivele criptografiei

***Confidențialitate:** păstrarea secretului informației, accesul la informația sensibilă fiind disponibilă doar persoanelor autorizate.*

***Integritate (a datelor):** eliminarea posibilității de modificare (schimbare, inserare, ștergere) neautorizată a informației.*

***Disponibilitate:** permiterea entităților autorizate să acceseze în timp util și fiabil informația.*

***Autentificare:** identifică o entitate sau atestă sursa datelor.*

Obiectivele criptografiei

***Confidențialitate:** păstrarea secretului informației, accesul la informația sensibilă fiind disponibilă doar persoanelor autorizate.*

***Integritate (a datelor):** eliminarea posibilității de modificare (schimbare, inserare, ștergere) neautorizată a informației.*

***Disponibilitate:** permiterea entităților autorizate să acceseze în timp util și fiabil informația.*

***Autentificare:** identifică o entitate sau atestă sursa datelor.*

***Non-repudiare:** previne negarea unor evenimente anterioare.*

Ce este criptografia?

Definitie

Criptografia este studiul tehnicilor matematice relaționate cu aspecte ale securității informației precum confidențialitatea, integritatea datelor, autentificarea entităților sau a originii datelor. [HAC6].

Utilizarea criptografiei

- ▶ comunicare securizată (criptată)
- ▶ criptarea fișierelor, a bazelor de date
- ▶ autentificarea utilizatorilor
- ▶ securizarea tranzacțiilor bancare (e-cash)
- ▶ vot electronic
- ▶ ...

Criptarea simetrică (cu cheie privată)



Alice

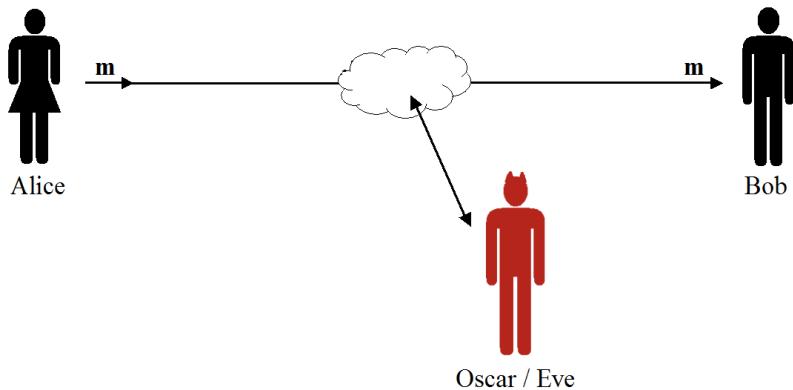


Bob

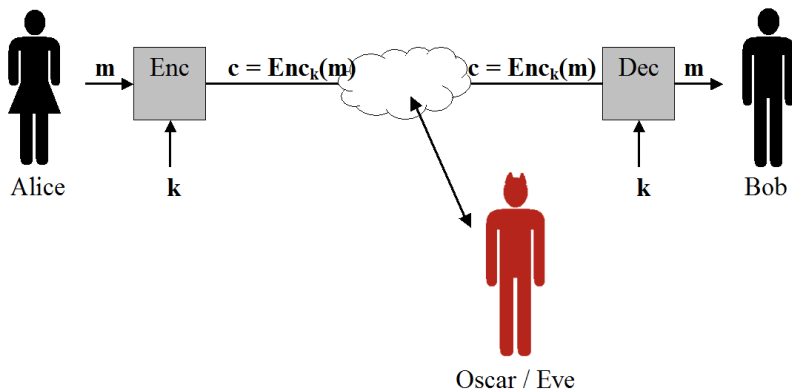


Oscar / Eve

Criptarea simetrică (cu cheie privată)



Criptarea simetrică (cu cheie privată)



Criptarea simetrică (cu cheie privată)

Definitie

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

- ▶ \mathcal{K} = spațiul cheilor
- ▶ \mathcal{M} = spațiul textelor clare (mesaje)
- ▶ \mathcal{C} = spațiul textelor criptate

este un dublet (Enc, Dec) , unde:

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

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

Terminologie

- ▶ Mesajul în forma originală se numește **text clar**;

Terminologie

- ▶ Mesajul în forma originală se numește **text clar**;
- ▶ Expeditorul rescrie mesajul folosind un sistem de criptare, adică îl **criptează** și obține un **text criptat**;

Terminologie

- ▶ Mesajul în forma originală se numește **text clar**;
- ▶ Expeditorul rescrie mesajul folosind un sistem de criptare, adică îl **criptează** și obține un **text criptat**;
- ▶ Destinatarul îl **decriptează** cunoscând metoda folosită pentru **criptare**;

Terminologie

- ▶ Mesajul în forma originală se numește **text clar**;
- ▶ Expeditorul rescrie mesajul folosind un sistem de criptare, adică îl **criptează** și obține un **text criptat**;
- ▶ Destinatarul îl **decriptează** cunoscând metoda folosită pentru **criptare**;
- ▶ Procesul de determinare a cheii aferente unui sistem de criptare, cunoscând doar textul criptat (eventual și alte informații auxiliare) se numește **criptanaliză**;

Terminologie

- ▶ Mesajul în forma originală se numește **text clar**;
- ▶ Expeditorul rescrie mesajul folosind un sistem de criptare, adică îl **criptează** și obține un **text criptat**;
- ▶ Destinatarul îl **decriptează** cunoscând metoda folosită pentru **criptare**;
- ▶ Procesul de determinare a cheii aferente unui sistem de criptare, cunoscând doar textul criptat (eventual și alte informații auxiliare) se numește **criptanaliză**;
- ▶ Decriptarea și criptanaliza au același scop: găsirea textului clar; diferența constă în faptul că la criptanaliză nu se cunoaște cheia de decriptare.

Scenarii de atac

- **Atac cu text criptat:** Atacatorul știe doar *textul criptat* - poate încerca un **atac prin forță brută** prin care se parcurg toate cheile până se găsește cea corectă;

Scenarii de atac

- ▶ **Atac cu text criptat:** Atacatorul știe doar *textul criptat* - poate încerca un **atac prin forță brută** prin care se parcurg toate cheile până se găsește cea corectă;
- ▶ **Atac cu text clar:** Atacatorul cunoaște una sau mai multe perechi (*text clar, text criptat*);

Scenarii de atac

- ▶ **Atac cu text criptat:** Atacatorul știe doar *textul criptat* - poate încerca un **atac prin forță brută** prin care se parcurg toate cheile până se găsește cea corectă;
- ▶ **Atac cu text clar:** Atacatorul cunoaște una sau mai multe perechi (*text clar, text criptat*);
- ▶ **Atac cu text clar ales:** Atacatorul poate obține criptarea unor texte clare alese de el;

Scenarii de atac

- ▶ **Atac cu text criptat:** Atacatorul știe doar *textul criptat* - poate încerca un **atac prin forță brută** prin care se parcurg toate cheile până se găsește cea corectă;
- ▶ **Atac cu text clar:** Atacatorul cunoaște una sau mai multe perechi (*text clar, text criptat*);
- ▶ **Atac cu text clar ales:** Atacatorul poate obține criptarea unor texte clare alese de el;
- ▶ **Atac cu text criptat ales:** Atacatorul are posibilitatea să obțină decriptarea unor texte criptate alese de el.

Dimensiunea cheii

Estimarea timpului de succes pentru un atac de tip *forță brută* asupra unui sistem de criptare *simetric*:

Lungime cheie (biți)	Securitate estimată
56 - 64	termen scurt (ore sau zile)
112 - 128	termen lung (în absența calculatoarelor cuantice)
256	termen lung (în prezenta calculatoarelor cuantice, folosind algoritmi cunoscuți)

Principiile lui Kerckhoffs

A. Kerckhoffs (1835 - 1903): *La Cryptographie Militaire* în *Journal des sciences militaires* (ian.1883)

Principiile lui Kerckhoffs

A. Kerckhoffs (1835 - 1903): *La Cryptographie Militaire* în *Journal des sciences militaires* (ian.1883)

1. Sistemul trebuie să fie practic, dacă nu matematic, indescifrabil.

Principiile lui Kerckhoffs

A. Kerckhoffs (1835 - 1903): *La Cryptographie Militaire* în *Journal des sciences militaires* (ian.1883)

1. Sistemul trebuie să fie practic, dacă nu matematic, indescifrabil.
2. **Principiul lui Kerckhoffs:** Sistemul nu trebuie să fie secret, poate să cadă ușor în mâinile adversarului (i.e. securitatea unui sistem de criptare nu constă decât în menținerea secretă a cheii).

Principiile lui Kerckhoffs

A. Kerckhoffs (1835 - 1903): *La Cryptographie Militaire* în *Journal des sciences militaires* (ian.1883)

1. Sistemul trebuie să fie practic, dacă nu matematic, indescifrabil.
2. **Principiul lui Kerckhoffs:** Sistemul nu trebuie să fie secret, poate să cadă ușor în mâinile adversarului (i.e. securitatea unui sistem de criptare nu constă decât în menținerea secretă a cheii).
3. Cheia trebuie să fie comunicată și menținută fără a fi notată, schimbată sau modificată la cererea corespondenților.

Principiile lui Kerckhoffs

A. Kerckhoffs (1835 - 1903): *La Cryptographie Militaire* în *Journal des sciences militaires* (ian.1883)

1. Sistemul trebuie să fie practic, dacă nu matematic, indescifrabil.
2. **Principiul lui Kerckhoffs:** Sistemul nu trebuie să fie secret, poate să cadă ușor în mâinile adversarului (i.e. securitatea unui sistem de criptare nu constă decât în menținerea secretă a cheii).
3. Cheia trebuie să fie comunicată și menținută fără a fi notată, schimbată sau modificată la cererea corespondenților.
4. Sistemul trebuie să fie compatibil cu comunicarea telegrafică.

Principiile lui Kerckhoffs

A. Kerckhoffs (1835 - 1903): *La Cryptographie Militaire* în *Journal des sciences militaires* (ian.1883)

1. Sistemul trebuie să fie practic, dacă nu matematic, indescifrabil.
2. **Principiul lui Kerckhoffs:** Sistemul nu trebuie să fie secret, poate să cadă ușor în mâinile adversarului (i.e. securitatea unui sistem de criptare nu constă decât în menținerea secretă a cheii).
3. Cheia trebuie să fie comunicată și menținută fără a fi notată, schimbată sau modificată la cererea corespondenților.
4. Sistemul trebuie să fie compatibil cu comunicarea telegrafică.
5. Sistemul trebuie să fie portabil și să nu necesite mai mult de o persoană.

Principiile lui Kerckhoffs

A. Kerckhoffs (1835 - 1903): *La Cryptographie Militaire* în *Journal des sciences militaires* (ian.1883)

1. Sistemul trebuie să fie practic, dacă nu matematic, indescifrabil.
2. **Principiul lui Kerckhoffs:** Sistemul nu trebuie să fie secret, poate să cadă ușor în mâinile adversarului (i.e. securitatea unui sistem de criptare nu constă decât în menținerea secretă a cheii).
3. Cheia trebuie să fie comunicată și menținută fără a fi notată, schimbată sau modificată la cererea corespondenților.
4. Sistemul trebuie să fie compatibil cu comunicarea telegrafică.
5. Sistemul trebuie să fie portabil și să nu necesite mai mult de o persoană.
6. Având în vedere circumstanțele în care este utilizat, sistemul trebuie să fie ușor de utilizat, fără să necesite aplicarea multor reguli.

<http://www.petitcolas.net/fabien/kerckhoffs/index.html>

Principiile lui Kerckhoffs

Întrebare: Care principii rămân valabile?

Cursul își propune:

- ▶ familiarizarea cu conceptele de bază și principiile criptografiei

Cursul își propune:

- ▶ familiarizarea cu conceptele de bază și principiile criptografiei
- ▶ cunoașterea primitivelor criptografice

Cursul își propune:

- ▶ familiarizarea cu conceptele de bază și principiile criptografiei
- ▶ cunoașterea primitivelor criptografice
- ▶ definirea unor modele de securitate

Cursul își propune:

- ▶ familiarizarea cu conceptele de bază și principiile criptografiei
- ▶ cunoașterea primitivelor criptografice
- ▶ definirea unor modele de securitate
- ▶ utilizarea corectă a primitivelor și sistemelor criptografice

Cursul își propune:

- ▶ familiarizarea cu conceptele de bază și principiile criptografiei
- ▶ cunoașterea primitivelor criptografice
- ▶ definirea unor modele de securitate
- ▶ utilizarea corectă a primitivelor și sistemelor criptografice
- ▶ analiza securității unor sisteme (gandește ca un atacator!)

Cursul își propune:

- ▶ familiarizarea cu conceptele de bază și principiile criptografiei
- ▶ cunoașterea primitivelor criptografice
- ▶ definirea unor modele de securitate
- ▶ utilizarea corectă a primitivelor și sistemelor criptografice
- ▶ analiza securității unor sisteme (gandește ca un atacator!)
- ▶ studiul unor sisteme criptografice folosite în practică : AES, RSA, ...

Cursul NU îşi propune:

- conceperea unor sisteme sigure:

NU există un sistem informațional 100% sigur!

Cursul NU îşi propune:

- conceperea unor sisteme sigure:

NU există un sistem informațional 100% sigur!

"...the mathematics is impeccable, the computers are vincible, the networks are lousy, and the people are abysmal."

(Bruce Schneier, Secrets and Lies: Digital Security in a Networked World)

Cursul NU îşi propune:

- conceperea unor sisteme sigure:

NU există un sistem informațional 100% sigur!

"...the mathematics is impeccable, the computers are vincible, the networks are lousy, and the people are abysmal."

(Bruce Schneier, Secrets and Lies: Digital Security in a Networked World)

- spargerea sistemelor informaționale (hacking)

Cursul NU îşi propune:

- ▶ conceperea unor sisteme sigure:

NU există un sistem informațional 100% sigur!

"...the mathematics is impeccable, the computers are vincible, the networks are lousy, and the people are abysmal."

(Bruce Schneier, Secrets and Lies: Digital Security in a Networked World)

- ▶ spargerea sistemelor informaționale (hacking)
- ▶ studiul malware (MALicious softWARE): viruși, troieni, ...

Cursul NU îşi propune:

- ▶ conceperea unor sisteme sigure:

NU există un sistem informațional 100% sigur!

"...the mathematics is impeccable, the computers are vincible, the networks are lousy, and the people are abysmal."

(Bruce Schneier, Secrets and Lies: Digital Security in a Networked World)

- ▶ spargerea sistemelor informaționale (hacking)
- ▶ studiul malware (MALicious softWARE): viruși, troieni, ...
- ▶ studiul unor atacuri practice (side channel attacks)

Important de reținut!

- ▶ Terminologia (criptografie, criptanaliză, mesaj clar, mesaj criptat, criptare, decriptare, ...)
- ▶ Personajele (Alice, Bob, Oscar / Eve)
- ▶ Principiul lui Kerckhoffs
- ▶ Definiția sistemelor de criptare (simetrice)