Criptografie și Securitate

- Prelegerea 3 -
Principiile de baza ale criptografiei moderne

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

Criptografia modernă

- reprezintă o trecere de la criptografia (istorică) ca *artă* (până in anii '75) la criptografia ca *știință* (după anii '75)
- trei principii importartante pe care se bazează criptografia modernă spre deosebire de criptografia clasică (istorică)

Criptografia modernă

- reprezintă o trecere de la criptografia (istorică) ca *artă* (până in anii '75) la criptografia ca *știință* (după anii '75)
- trei principii importartante pe care se bazează criptografia modernă spre deosebire de criptografia clasică (istorică)
  - **Principiul 1** - orice problemă criptografică necesită o definiție clară și riguroasă

Criptografia modernă

- reprezintă o trecere de la criptografia (istorică) ca *artă* (până in anii '75) la criptografia ca *știință* (după anii '75)
- trei principii importartante pe care se bazează criptografia modernă spre deosebire de criptografia clasică (istorică)
  - **Principiul 1** - orice problemă criptografică necesită o definiție clară și riguroasă
  - **Principiul 2** - securitatea primitivelor criptografice se bazează pe prezumpții clare de securitate (de regulă, probleme dificile)

Criptografia modernă

- reprezintă o trecere de la criptografia (istorică) ca *artă* (până in anii '75) la criptografia ca *știință* (după anii '75)
- trei principii importartante pe care se bazează criptografia modernă spre deosebire de criptografia clasică (istorică)
  - **Principiul 1** - orice problemă criptografică necesită o definiție clară și riguroasă
  - **Principiul 2** - securitatea primitivelor criptografice se bazează pe prezumpții clare de securitate (de regulă, probleme dificile)
  - **Principiul 3** - orice construcție criptografică trebuie să fie insoțită de o demonstrație de securitate conform principiilor anterioare

Principiul 1 - Formularea riguroasă a definițiilor de securitate

Necesitatea definițiilor exacte:

Principiul 1 - Formularea riguroasă a definițiilor de securitate

Necesitatea definițiilor exacte:

- vrem să construim un sistem de criptare sigur; dacă nu știm exact ce vrem sa obținem, cum ne putem da seama dacă sau când ne-am atins scopul?

Principiul 1 - Formularea riguroasă a definițiilor de securitate

Necesitatea definițiilor exacte:

- vrem să construim un sistem de criptare sigur; dacă nu știm exact ce vrem sa obținem, cum ne putem da seama dacă sau când ne-am atins scopul?
- vrem să folosim o schema de criptare într-un sistem mai mare; cum știm ce schema să alegem sau care ni se potrivește?

Principiul 1 - Formularea riguroasă a definițiilor de securitate

Necesitatea definițiilor exacte:

- vrem să construim un sistem de criptare sigur; dacă nu știm exact ce vrem sa obținem, cum ne putem da seama dacă sau când ne-am atins scopul?
- vrem să folosim o schema de criptare într-un sistem mai mare; cum știm ce schema să alegem sau care ni se potrivește?
- fiind date doua scheme, cum le putem compara? eficiența nu este un criteriu suficient;

Principiul 1 - Formularea riguroasă a definițiilor de securitate

Necesitatea definițiilor exacte:

- vrem să construim un sistem de criptare sigur; dacă nu știm exact ce vrem sa obținem, cum ne putem da seama dacă sau când ne-am atins scopul?
- vrem să folosim o schema de criptare într-un sistem mai mare; cum știm ce schema să alegem sau care ni se potrivește?
- fiind date doua scheme, cum le putem compara? eficiența nu este un criteriu suficient;
- NU ne putem baza pe o idee intuitivă a ceea ce înseamna securitatea;

Principiul 1 - Formularea riguroasă a definițiilor de securitate

Necesitatea definițiilor exacte:

- vrem să construim un sistem de criptare sigur; dacă nu știm exact ce vrem sa obținem, cum ne putem da seama dacă sau când ne-am atins scopul?
- vrem să folosim o schema de criptare într-un sistem mai mare; cum știm ce schema să alegem sau care ni se potrivește?
- fiind date doua scheme, cum le putem compara? eficiența nu este un criteriu suficient;
- NU ne putem baza pe o idee intuitivă a ceea ce înseamna securitatea;
- Atenție! Formalizarea definițiilor **NU** este o sarcină trivială.

Un exemplu: criptarea sigură

- Cum ați defini noțiunea de schemă de criptare sigură?
  Posibile răspunsuri:(sunt corecte?)

Un exemplu: criptarea sigură

- Cum ați defini noțiunea de schemă de criptare sigură?
  Posibile răspunsuri:(sunt corecte?)
  1. Nici un adversar nu poate găsi cheia secretă fiind dat un text criptat.

Un exemplu: criptarea sigură

- Cum ați defini noțiunea de schemă de criptare sigură?
  Posibile răspunsuri:(sunt corecte?)
  1. Nici un adversar nu poate găsi cheia secretă fiind dat un text criptat.
  2. Nici un adversar nu poate găsi textul clar corespunzător unui text criptat.

Un exemplu: criptarea sigură

- Cum ați defini noțiunea de schemă de criptare sigură?
  Posibile răspunsuri:(sunt corecte?)
  1. Nici un adversar nu poate găsi cheia secretă fiind dat un text criptat.
  2. Nici un adversar nu poate găsi textul clar corespunzător unui text criptat.
  3. Nici un adversar nu poate determina nici măcar un caracter (o literă) din textul clar corespunzător unui text criptat.

Un exemplu: criptarea sigură

- Cum ați defini noțiunea de schemă de criptare sigură?
  Posibile răspunsuri:(sunt corecte?)
  1. Nici un adversar nu poate găsi cheia secretă fiind dat un text criptat.
  2. Nici un adversar nu poate găsi textul clar corespunzător unui text criptat.
  3. Nici un adversar nu poate determina nici măcar un caracter (o literă) din textul clar corespunzător unui text criptat.
  4. Nici un adversar nu poate determina informații cu sens din textul clar corespunzător unui text criptat.

Un exemplu: criptarea sigură

- Cum ați defini noțiunea de schemă de criptare sigură?
  Posibile răspunsuri:(sunt corecte?)
  1. Nici un adversar nu poate găsi cheia secretă fiind dat un text criptat.
  2. Nici un adversar nu poate găsi textul clar corespunzător unui text criptat.
  3. Nici un adversar nu poate determina nici măcar un caracter (o literă) din textul clar corespunzător unui text criptat.
  4. Nici un adversar nu poate determina informații cu sens din textul clar corespunzător unui text criptat.

  Răspuns corect:
- Nici un adversar nu poate calcula nici o funcție de textul clar pornind de la textul criptat.

- Definiția corectă de securitate $\rightarrow$ prezentare matematică și formală
- Trebuie să cuprindă:
  (a) ce inseamnă a sparge o schemă de criptare - vezi slide-ul anterior
  (b) de ce putere dispune adversarul:
  ce acțiuni are voie să intreprindă + putere computațională

Definitie

O schemă de criptare este sigură dacă nici un adversar având puterea specificată nu poate sparge schema în modul specificat.

Principiul 2 - prezumpții de securitate și Principiul 3 - demonstrații de securitate

- majoritatea construcțiilor criptografice moderne nu pot fi demonstrate ca fiind sigure necondiționat
- fară o demonstrație riguroasă, intuiția că o schemă este corectă poate avea consecințe dezastruoase
- majoritatea demonstrațiilor folosesc o abordare reductionistă

Teorema

Constructia Y este sigură conform definiției dacă prezumpția X este adevarată.

- demonstrația va arăta cum un adversar care sparge schema Y poate încalca prezumpția X.

Important de reținut!

- Criptografia clasică $\rightarrow$ abordare ad-hoc
- Criptografia modernă $\rightarrow$ abordare riguroasă