Tudorache Alexandru-Theodor

Grupa 342

Laborator 2

Securitatea Sistemelor Informatice

1.

A -> 4

B -> 2

C -> 5

D -> 1

E -> 6

F -> 3

2.

*1.* Confidentiality

*2.* Availability

*3.* Integrity

*4.* Confidentiality

*5.* Integrity

Exemple de primitive criptografice:

- Confidentialitate -> Symmetric key cryptography

- Integritate -> Digital signatures

3.

*1.* Fals

*2.* Adevarat

*3.* Fals

4.

*1.* ne-neglijabila -> pentru ca este functie constanta

*2.* ne-neglijabila -> pentru ca este functie constanta

*3.* ne-neglijabila -> pentru ca este functie polinomiala

*4.* neglijabila -> pentru ca este functie exponentiala

*5.* neglijabila -> pentru ca doua numere foarte mici (functii neglijabile) adunate dau un numar foarte mic

*6.* ne-neglijabila -> pentru ca un numar foarte mic (functie neglijabila) adunat cu un numar mare (functie ne-neglijabila) este tot un numar mare (functie ne-neglijabila).

5.

Securitate perfecta nu este scopul nostru deoarece aceasta nu poate fi atinsa din cauza limitarilor practice. De-obicei, se face un compromis de securitate pentru a se ajunge la constructii practice.

6.

- Numar de chei posibile distinte -> 2512

- Timp de gasire al cheii: 2512 – 30 = 2482 sec

- Nu este un atac eficient pentru ca 2482 sec inseamna 3.9569742 \* 10137 ani, care este un timp mult prea mare de calculare.