Dima Oana-Teodora 341

Securitatea Sistemelor Informatice – Laborator 2

1.

A - 4

B - 2

C - 5

D - 1

E - 6

F – 3

2.

1. confidentialitate

2. integritate, disponibilitate

3. integritate

4.confidentialitate

5.integritate

Condentialitatea: Sisteme de criptare

Integritatea: Constructii MAC

3.

1. Fals

2. Adevarat

3. Fals

4.

1. neneglijabila
2. neneglijabila
3. neneglijabila
4. neglijabila
5. neglijabila
6. neneglijabila

5. De ce preferam securitatea computationala in practica?

Securitatea computationala: puterea atacatorului este marginita(algoritm polinomial in timp).

In timp ce, securitatea perfecta se bazeaza pe ipotezele matematice sau primitivele de criptografie. De asemenea, costul material pentru un sistem cu securitate perfecta ar fi mult prea mare, nefezabil, deci inaccesibil pentru clienti(customeri).

6.

cheie de criptare pe 512 biti

chei posibile distincte: 2^{512}

2^{30} chei pe secunda => timp $2^{512-30}=2^{482}$

Nu este un atac eficient datorita timpului.