

I.

A - 4

B - 2

C - 5

D - 1

E - 6

F - 3

II

1 - confidentialitate

2 - disponibilitate

3- integritate

4- confidentialitate

5- integritate

III

1- fals

2- adevarat, fiind probabilistic

3 - fals (are polinomiali)

IV

1, 2, 3, 4, 5

V

Securitatea perfecta este imposibil de atins in practica. Securitatea computationala este alternativa cea mai buna, bazandu-se pe faptul ca niciun sistem nu este indeajuns de puternic pentru a descifra cheia intr-un timp rezonabil.

VI.

- 2^{512}

- $2^{512} / 2^{30}$

- nu (prea multe secunde)