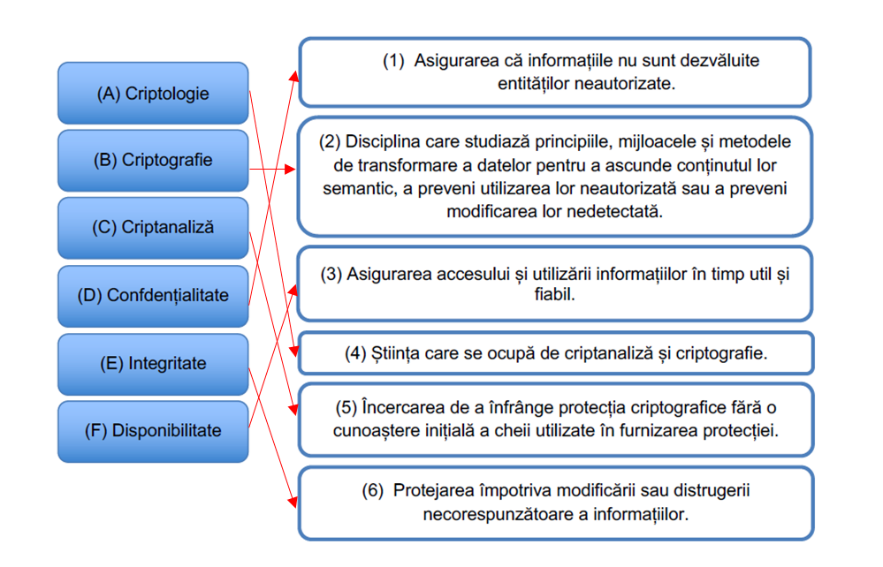
**Laborator 2**

**Notiuni generale:**

1. A – 4

B – 2

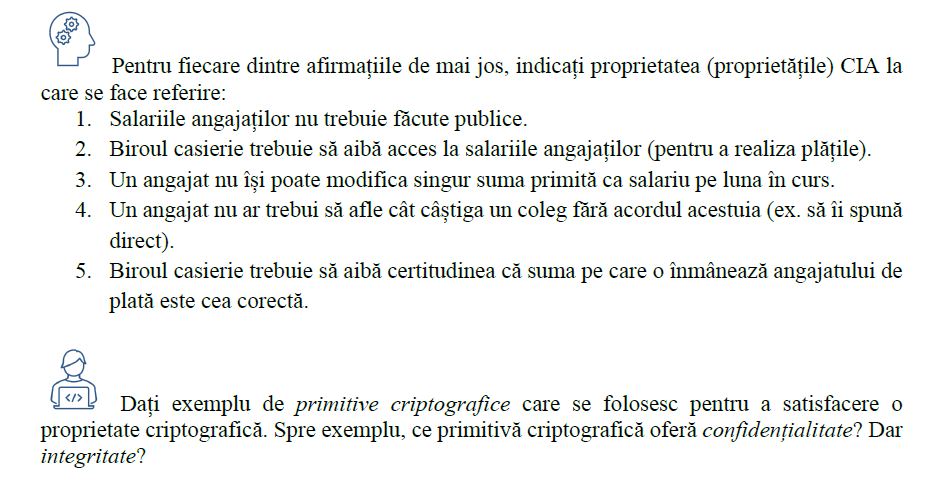
C – 5

D – 1

E – 6

F – 3

Triada Confidentiality, Integrity, Availability:



1. 1 – C

2 – A

3 – I

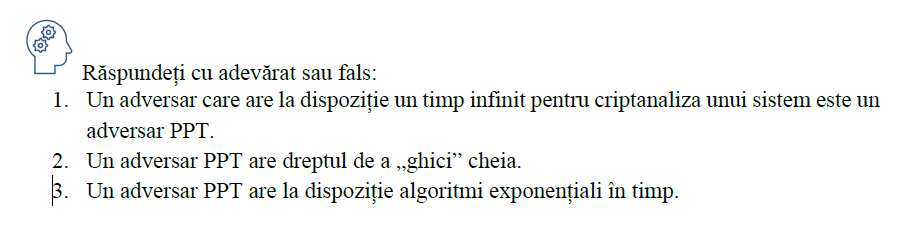
4 – C

5 – I

Confidentialitate: sisteme de criptare

Integritate: constructii MAC (Message Authentication Code)

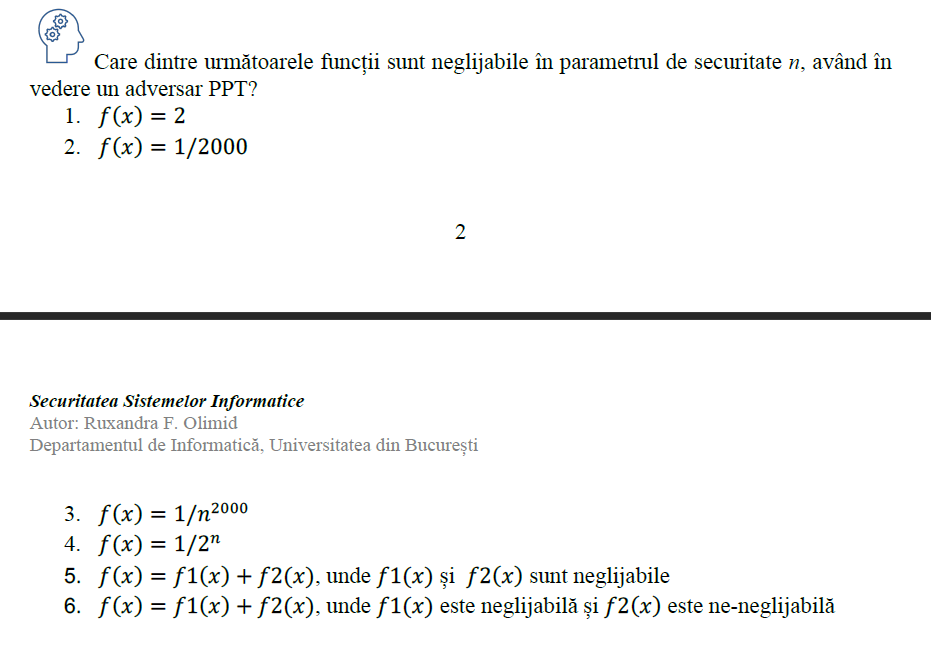
Adversar Probabilistic Polinomial in Timp (PPT):



1. 1 – F

2 – A

3 – F



Functii neglijabile:

4.

1) f(x) = 2 neneglijabila

∀ c > 0, ∃ Nc >= 0 a.i |f(x)| < 1 / x^c ∀ x > Nc

⬄

∀ c > 0, ∃ Nc >= 0 a.i. 2 < 1/x^c, ∀ x > Nc

⬄

1/2 > x^c, ∀ x > Nc

Fals, ex alegem c = 10

2) f(x) = 1/2000 neneglijabila

∀ c > 0, ∃ Nc >= 0 a.i. |f(x)| < 1 / x^c ∀ x > Nc

⬄

∀ c > 0, ∃ Nc >= 0 a.i. 1/2000 < 1/x^c, ∀ x > Nc

⬄

2000 > x^c, ∀ x > Nc

Fals, ex alegem c = 1000

3) f(x) = 1/ x^2000 neneglijabila

∀ c > 0, ∃ Nc >= 0 a.i. |f(x)| < 1 / x^c, x > Nc

⬄

∀ c > 0, ∃ Nc >=0 a.i. 1/ x^2000 < 1/x^c, ∀ x > Nc

⬄

x^2000 > x^c, ∀ x > Nc

Fals, ex alegem c = 2001

4) f(x) = 1/ 2^x neglijabila

∀ c > 0, ∃ Nc >=0 a.i. |f(x)| < 1 / x^c, x > Nc

⬄

∀ c > 0, ∃ Nc >=0 a.i. 1/ 2^x < 1/x^c, ∀ x > Nc

⬄

2^x > x^c, ∀ x > Nc

Pt c = 2, 2^x > x^2, ∀ x > Nc

5) f(x) = f1(x) + f2(2), unde f1(x) și f2(x) sunt neglijabile – neglijabila

| f1(x) + f2(x) | <= |f1(x)| +|f2(x)|

f1 neglijabila ⇔ ∀ c1 > 0, ∃ Nc1 >=0 a.i. |f1(x)| < 1 / x^c1 ∀ x > Nc1

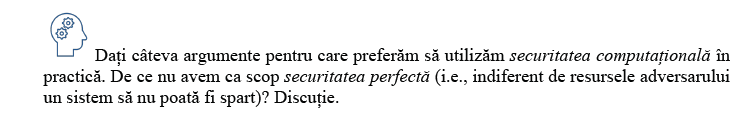
f2 neglijabila ⇔ ∀ c2 > 0, ∃ Nc2 >=0 a.i. |f2(x)| < 1 / x^c2 ∀ x > Nc2

* ∀ c3 > 0, ∃ Nc3 = max{Nc1, Nc2} a.i. |f1(x) + f2(x) | <= |f1(x)| +|f2(x)| <= 1/x^c1 + 1/x^c2 <= 1/x^c3 ∀ x > Nc3
* f neglijabila

6) f(x) = f1(x) + f2(2), unde f1(x) negliabila și f2(x) neneglijabila

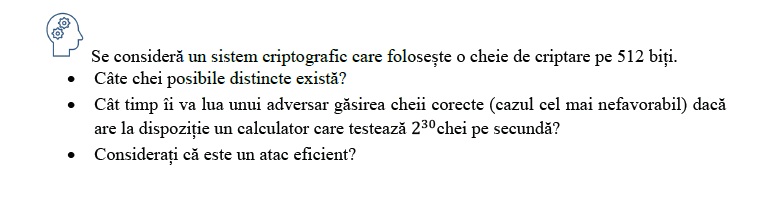
Pp ca f(x) este neglijbila => ∀ c > 0, ∃ Nc >=0 a.i. |f(x)| < 1 / x^c ∀ x > Nc

|f(x)| <= |f1(x)| + |f2(x)|

Securitate computationala:

1. Costul material pentru un sistem cu securitate perfecta fata de unul cu securitate computationala este mult mai mare si acest fapt il face sa fie inaccesibil pentru majoritatea clientilor.

Atac prin forta bruta/cautare exhaustive:



6.

a) 2^512 chei distincte

b) 2^512 : 2^30 = 2 ^(512 -30) = 2 ^482

c) Nu e un atac eficient.