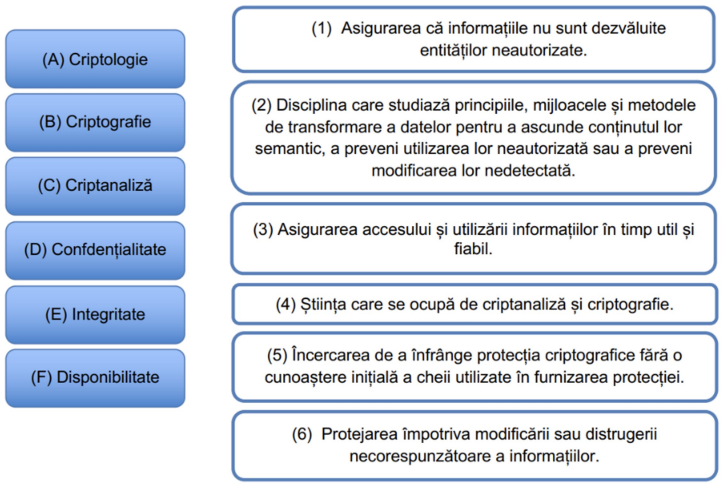
Lab2

vineri, 13 octombrie 2023 14:15

ex.1



A - 4
B - 2
C - 5
D - 1
E - 6
F - 3

ex.2

1. Salariile angajaților nu trebuie făcute publice.
2. Biroul casierie trebuie să aibă acces la salariile angajaților (pentru a realiza plățile).
3. Un angajat nu își poate modifica singur suma primită ca salariu pe luna în curs.
4. Un angajat nu ar trebui să afle cât câștiga un coleg fără acordul acestuia (ex. să îi spună direct).
5. Biroul casierie trebuie să aibă certitudinea că suma pe care o înmânează angajatului de plată este cea corectă.

1 - Confidentialitate
2 - Disponibilitate
3 - Integritate
4 - Confidentialitate
5 - Integritate

ex.3

1. Un adversar care are la dispoziție un timp infinit pentru criptanaliza unui sistem este un adversar PPT.
2. Un adversar PPT are dreptul de a „ghici” cheia.
3. Un adversar PPT are la dispoziție algoritmi exponențiali în timp.

1. fals
2. adevarat
3. fals (alg sunt polinomiali, nu exponentiali)

ex.4

def: O fct f: N -> R+ este PPT neglijabila daca pentru orice c natural, exista un rang n natural a.i. pentru orice x > n sa avem ca f(x) < 1/x^c.

1. $f(x) = 2$
2. $f(x) = 1/2000$
3. $f(x) = 1/n^{2000}$
4. $f(x) = 1/2^n$
5. $f(x) = f1(x) + f2(x)$, unde $f1(x)$ și $f2(x)$ sunt neglijabile
6. $f(x) = f1(x) + f2(x)$, unde $f1(x)$ este neglijabilă și $f2(x)$ este ne-neglijabilă

1 – not neglijabila (constanta)
2 – not negrlijabila (constanta)
3 – not neglijabila (exponentiala creste mai rpd decat polinomiala)
4 – neglijabila (exponentiala)
5 – neglijabila (suma fct negl e o fct negl)

~~f1(x) < 1/x^c + 1~~
~~f2(x) < 1/x^c +1 => f1+f2< 2/x^c +2 <1/x^c~~

|f1+f2|<= |f1|+|f2|
|f1| < 1/x^c
|f2| < 1/x^c
+
|f1+f2|<= 1/x^c+1/x^c
|f1+f2| <= 2/x^c < 2* 1/x^c
2/x^c neglijabila => f1+f2 negl

6 – not neglijabila (negl + not negl e tot not negl)

valoarea abs din cele doua functii, deci functia notneglijabila.
Inseamna deci ca si suma e notneglijabila
|f1(x)|<1/x^c
|f2(x)|>=1/x^c
Deci |f1(x)|+|f2(x)|>=1/x^c

ex.5

preferam securitatea computationala in loc de cea perfecta pt ca aceasta ar necesita un nr mai mare de resurse, lucru adesea inutil.
se folosesc resurse de securitate pe un timp finit, deoarece practic niciun atacator nu are timp infinit la dispozitie pentru spargere. (asteptam sa moara atacatorul daca e nevoie)

ex.6
exista 2^512 chei (suma combinarilor de 512 luate cate …)

timp 2^512 / 2^30 = 2^482 secunde

atacul nu ar fi prea eficient (are nevoie de muult timp pentru a incerca toate variantele posibile, e mai mult timp decat anii de la big bang)