1.
    a. Criptologie = Știința care se ocupă de criptanaliză și criptografie.
    b. Criptografie = Disciplina care studiază principiile, mijloacele și metodele de transformare a datelor pentru a ascunde conținutul lor semantic, a preveni utilizarea lor neautorizată sau a preveni modificarea lor nedetectată.
    c. Criptanaliza = Încercarea de a înfrânge protecția criptografice fără o cunoaștere inițială a cheii utilizate în furnizarea protecției.
    d. Confidentialitate = Asigurarea că informațiile nu sunt dezvăluite entităților neautorizate.
    e. Integritate = Protejarea împotriva modificării sau distrugerii necorespunzătoare a informațiilor.
    f. Disponibilitate = Asigurarea accesului și utilizării informațiilor în timp util și fiabil.
2.
    a. Salariile angajaților nu trebuie făcute publice.=> Confidentialitate
    b. Biroul casierie trebuie să aibă acces la salariile angajaților (pentru a realiza plățile). => Disponibilitate
    c. Un angajat nu își poate modifica singur suma primită ca salariu pe luna în curs. => Integritate
    d. Un angajat nu ar trebui să afle cât câștiga un coleg fără acordul acestuia (ex. să îi spună direct). => Confidentialitate
    e. Biroul casierie trebuie să aibă certitudinea că suma pe care o înmânează angajatului de plată este cea corectă. => Integritate

    Confidentialitate - criptare asimetrica
    Integritate - functii hash
    Disponibilitate - server care reporneste

3.
    a. Un adversar care are la dispoziție un timp infinit pentru criptanaliza unui sistem este un adversar PPT => fals
    b. Un adversar PPT are dreptul de a „ghici” cheia => adevarat
    c. Un adversar PPT are la dispoziție algoritmi exponențiali în timp. => fals
4.
    a. $f(n)$ = 2 => ne-neglijabila
    b. $f(n)$ = 1/2000 => ne-neglijabila
    c. $f(n)$ = 1/(n^2000) => ne-neglijabila
    d. $f(n)$ = 1/(2^n) => neglijabila
    e. 5. $f(n) = f1(n) + f2(n)$, unde $f1(n)$ și $f2(n)$ sunt neglijabile => neglijabila
    f. 6. $f(n) = f1(n) + f2(n)$, unde $f1(n)$ este neglijabilă și $f2(n)$ este ne-neglijabilă => ne-neglijabila

5. Securitatea computationala spune ca un sistem este considerat sigur atunci cand probabilitatea sa de a fi spart este neglijabila. Pe de alta parte, securitatea perfecta este foarte greu de atins.
6.
    a. 2^512 chei
    b. 2^512 / 2^30 = 2^482 secunde = 1.13*2^70 ore = 1.51*2^465 zile

c. Atacul nu ar putea fi unul eficient pentru ca probabilitatea e reusita intr-un timp fiabil este foarte mica.