1). Kako se zove mehanizam unutar jednog računala koji broji događaje?

Prema pravilima globlanog logičkog sata na koju vrijednost proces Pi postavlja lokalni logički sat kada primi poruku zahtjev(j,T(j))? Ci = \_\_\_\_\_\_\_\_\_\_

Navesti broj poruka koji se treba razmjeniti u sustavu s 10 računala gdje u svakom računalu se nalazi po jedan proces koji se natječe za ulazak u kritični odsječak ako se koristi raspodijeljeni Lamportov protokol?

Običan cjevovod je opisan s \_\_\_\_\_ opisnika a imenovani cjevovod s \_\_\_\_\_\_ opisnika.

2.) Pronaći prvi broj p veći od 7700 koji prolazi ispitivanje radi li se o prostom broju Fermatovim teoremom. U postupku ispitivanje umjesto proizvoljnog broja nasumično odabranih brojeva a€Zp\* koristite samo dva broja i to 2 i 7. (ako se za prvi broj 2 utvrdi složenost ne treba provjeravati za drugi broj 7. Napomena. U svim zadacima u ovom ispitu gdje treba izračunati izraz abmod n treba koristiti modularno potenciranje.

3). Veličina ulaznog bloka podataka u DES kriptosustav iznosi \_\_\_\_ bajtova a u AES kriptosustav \_\_\_ bajtova.

Broj koraka u kriptosustavu AES ovisi o \_\_\_\_\_\_ .

Koliko iznosi Eulerova phi funkcija ᵨ(77) = \_\_\_\_\_\_\_ .

Kolika j maksimalna veličina simetričnog ključa k u bitovima koji može kriptirati RSA kriptosustav u koje je n= 2049? Odgovor: \_\_\_\_\_

Ako se uz pomoć kriptosustava AES kriptira datoteka veličine 100 bajtova. Koliko će velika biti kriptirana datoteka?

4) Ana i Branko su ustanovili zajednički ključ Diffie- Hellmanovim postupkom. Pritom su koristili sljedeće parametre sustava n=179, g=19. Nadalje Ana je u postupku generirala nasumični broj x=11, a Branko y=97.

(1) koji od brojeva x,y,n i g u navedenom postupku moraju biti prosti?

Dogovoreni zajednički ključ je: \_\_\_\_\_\_\_\_\_ .

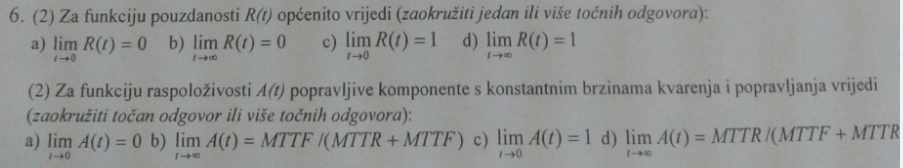
5) (1) Navesti dva načina kriptiranja koji su pogodni za kriptiranje toka podataka. \_\_\_\_\_\_\_\_\_\_\_

Skicirati CFB način kriptiranja.

6) a) Za funkciju R(t)

b) Za funkciju raspoloživosti A(t)

isti zadatak kao prosle godine.



7) Neka je zadan kriptosustav RSA sa javnim ključem P=(N,e) i privatnim ključem S=(N,d) gdje je N=pq za velike proste brojeve p i q.

a) (1)Za brojeve e i d mora vrijediti: \_\_\_\_\_\_\_\_\_\_\_,

b) (0.5)C=RSA(M,P): \_\_\_\_\_\_ ,

c) (0.5) M'=RSA-1(C,S)=\_\_\_\_\_\_\_\_,

d) (1) Dokazati da je M'=M \_\_\_\_\_\_\_\_.

e)(1) Prethodni korak vrijedi samo za brojeve M manje od N koji su relativno prosti sa N. Obrzloži zašto je vrlo teško da se dogodi da slučajno odabrani broj M nije relativno prost za N. \_\_\_\_\_\_\_.

f)Pretpostavimo da se datoteka enkriptira javnim ključem tako da se datoteka podijeli na bajtove B1, B2, ... Bk, svaki bajt se interpretira kao broj između 0 i 255 te se enkriptira pomoću RSA kriptosustava, točnije izračunavaju se brojevi Ci= RSA(Bi, P). Obrazloži efikasan postupak kojim se na temelju javnog ključa i niza C1, C2,..Ck može odrediti sadržaj originalne datoteke.

8)(2) Ana i Branko dijele tajni AES ključ KAB, Ana i Branko dijele tajni AES ključ KAD. Ana želi kriptirati poruku M tako da je mogu dekriptirati Branko, Danko i nitko drugi. Opišite jedan takav mehanizam kriptiranja.

9) (3) Skicirati postupak jednostavne autentifikacije u zatvorenom asimetričnom kriptosustavu. Naznačiti sadržaj svake poruke (elemente poruke nije potrebno opisivati)

10) Skicirati Markovljev lanac sa N popravljivih komponenti s konstantnim brzinama λ i popravljanja µ. Dozvoljen je dvostruki kvar(sustav prelazi u kronostanje ako se tri komponente pokvare). Markovljev lanac neka se sastoji od sljedeća četri stranja (0) sve komponente su ispravne, (1) jedna neispravna, (2) dvije neispravne i (3) kronostanje. Naznačiti vjerojatnosti prijelaska iz stanja u stanje kao i vjerojatnost ostanka u istom stanju. Zanemariti vjerojatnosti da se u nekom trenutku odjednom pokvare ili poprave dvije ili više komponenti.

(3boda) Postaviti sustav diferencijalnih jednadžbi za naveden sustav i navesti početne vjerojatnosti

P'0(t)= \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ P0(0)=

P'1(t)= \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ P1(0)=

P'2(t)= \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ P2(0)=

P'3(t)= \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ P3(0)=

(1bod) Navesti izraze za raspoloživost As(t) i neraspoloživost Qs(t)

11) (2boda) Za neki radi 5 sustav na raspolaganju su šest diskova, svaki po 1TB i tri diska po 2TB. Diskove rasporediti u jedan RAID 5 sustav tako da taj višediskovni sustav ima maksimalni kapacitet. Koliki je maksimalni kapacitet podataka koji se mogu pohraniti u takav RAID 5 sustav? Odg: \_\_\_\_\_\_\_\_

(2b) Skicirati takav RAID 5 sustav

13) (rješavati na košuljici) Neka se višediskovni sustav sastoji od N istovrsnih diskova. Koliko može biti najveći N ako srednje vrijeme do pojave kvara u sustavu mora biti barem 4 godine? Za sveki disk zadano je srednje vrijeme do pojave kvara MTTF = 12 godina i srednje vrijeme popravka MTTR= 10 dana. Pretpostavimo da je sustav neispravan ako se dogodi

a) (4b) dvostruki kvar Rješenje N=\_\_\_\_\_\_\_\_

b)(1b) jednostruki kvar Rješenje N = \_\_\_\_\_\_\_\_\_