1. (5)Protokol Ricart-Agrawal.

U sustavu se nalaze tri čvora i na svakom čvotu po jedan proces P1, P2 i P3 koji imaju u svojim lokalnim logičkim satovima vrijednosti c1 = 10, C2 = 8 i C3 =8 gdje je Ci lokalni log. Sat proces Pi. Sinkronizacija proces odvija se prema pravilima protokola Ricart-Agrawal. Svi procesi žele ući u KO.

a)(1.5) Skicirati protokol.

b)(0.5)Kojim redoslijedom su procesi ulazili u KO?

c)(3)Koje su sve moguće vrijednosti lokalnih log. Satova na kraju?

P1:_____

P2:_____

P3:_____

2. (5) Međusodno isključivanje u raspodijeljenim sustavima.

Neki sustav sastoji se od 6 čvorova i u svakom čvoru nalazi se po jedan proces. Niti jedan od proces P1,...;P6 do trenutka t1 nije želio ući u KO. Sinkronizacija procesa odvija se prema pravilima **raspodijeljenog Lamportovog protokola**. Između t1 i t2 svaki od proces Pi uđe i izađe iz KO i puta (P1 jednom,...,P6 šest puta)

a)(1) Koliko je ukupno poruka razaslano u intervalu (t1,t2)?

b)(4) Za svaki proces navesti broj poruka koje su razaslali te broj poruka koje su primili u intervalu (t1,t2)

P1 primio:_____ P1 poslao:_____ i tako za svaki

3. (5) Neka se višediskovni sustav sastoji od N istovrsnih diskovva. Koliko može biti najveći N ako srednje vrijeme do pojave kvara u sustavu mora biti barem 5 godina? Za svaki disk zadano je srednje vrijeme do pojave kvara MTTF = 20 godina i srednje vrijeme popravka MTTR = 5 godina. Pretpostavimo da je sustav neispravan ako se dogodi: (obavezano navesti postupak na košuljicu)

a)(4) Dvostruki kvar: N= _____

b)(1) Jednostruki kvar: N= ____

4. (10) Višediskovni zalihosni spremnici.

Za ostvarenje višediskovno zalihosnog sustava RAID na raspolaganju je 6 istovrsnih diskova svaki po 2TB.

a)(1) RAID 6 sustav ulazi u kvarno stanje ako se dogodi kvar(zaokruži jedan ili više):

a)jednog diska

b) 2 diska

c) 3 diska

d) 4 diska

e) svih raspoloživih diskova

b)(1) Skicirati RAID 6 sustav s raspoloživim diskovima te istaknuti redundantne dijelove pojasa.

c)(1) Ukupan kapacitet raspoloživih diskova sastavljenih u RAID 6 sustav iznosi _____ TB, od koji _____ TB otpada na korisne podatke, a _____ TB na redundantne podatke.

d)(3) Skicirati Markovljev lanac za takav višediskovni RAID 6 sustav. Svi diskovi imaju konstantne brzine kvarenja i popravljanja. Markovljev lanac neka se sastoji od potrebnog broja stanja gdje oznaka stanja odgovara broju neispravnih komponenti npr. (0) sve komponente ispravne (1) jedna neispravna do (K) što označava kvarno stanje. Naznačiti vjerojatnosti da se u nekom trenutku odjednom pokvare ili poprave dvije ili više komponenti.

e)(3) Postaviti sustav diferencijalnih jdž. Za navedeni sustav i navesti početne vjerojatnosti

$p'_0(t)$ = _____ $p_0(0)$ = _____

....

$p'_4(t)$ = _____ $p_4(0)$ = _____

f)(1) Navesti izraze za raspoloživost As(t) i neraspoloživost Qs(t) navedenost sustava.

As(t) = ____ Qs(t) = _____

5. (6) Kriptosustavi i sigurnosni protokoli

a) (1) Ukratko objasniti problem diskretnog logaritma u Diffie_Hellmanovom postupku.

b)(1) Vrijednost Eulerove f-je za N = 16

c)(1) Navesti dva načina kriptiranja vlokova kod kojih se pogreška u kriptiranom tekstu ne propagira na sljedeći blok čistog teksta.

d)(1) U AES f-ji „Zamijeni znakove“ substitucijska tablica ne ovisi(jedan ili više zaokruži):

a) veličini ključa

b) ključu

c) jasnom tekstu

d) ključu i jasnom tekstu

e)(2) Razmatramo raspodjelu ključeva u zatvorenom asimetričnom kriptosustavu

a) Navedi sadržaj zadnje dvije poruke

b) Koje sigurnosno svojstvo bi bilo narušeno ako bismo zadnje dvije poruke zanemarili.Obrazloži.

6.(4) Skicirajte komunikacijski dijagram protokola Kerberos s označenim porukama(npr. M1) bez navođenja saržaja poruka (ne treba pisati M1 =...) Koje od označenih poruka sadrže ulaznicu, a koje dozvolu?

7.(5) Pretpostavimo da je riječ o kriptosustavu RSA(bez nadopunjavanja i sažetka) s javnim ključem pk =(7, 77) i privatnim ključem sk = (43, 77).

a)(1) φ(N) = _____

b)(1) Pokažite da je par (sk,pk) javnog i priv. Ključa korektan.

c) (1) odredite enkripciju poruke (broja) „3“

d) (2) Dekripcija poruke (broja) „6“ koristeći algoritam uzastopnog kvadriranja. OBAVEZAN postupak.

8.(4)

a)(1) Ako napadnemo sustave AES128 i AES256 napadom grube sile, koliko će puta biti sporiji napad na AES256 od napada na AES128?

b)(2) Objasnite barem dva razloga zbog kojih kombiniramo sustave enkripcije javnim ključem i simetričnu enkruipciju.

c)(1) F-ja sažimanja SHA-1 izvorni tekst dijeli na blokove koje duljine?

9. (6) Pretpostavimo da su rezultati ovog ispita kriptirani RSA kriptosustavom na sljedeći način:

Odabrani su slučajni prosti brojevi p i q veličine 1024 bita te je odabran javni ključ pk =( N= p*q, e = 3). Za studenta A je njegov rezultat predstavljen kao rezA = rbrA*100+bodA, gdje je rbrA {1, ..., 313} njegov redni broj u grupi, a bodA {0, ..., 100} broj bodova na ispitu. Broj rezA je kriptiran RSA sustavom te je dobiven broj Ca = RS(rezA, pk). Prikazati i obrazložiti djelotvoran postupak koji samo na temelju javnog ključa pk i broja CA određuje redni broj i br. Bodova studenta A.