RAČUNALNIŠKE KOMUNIKACIJE 2018/19

Ime in priimek: _____

2. izpit, 4. 7. 2019

Vpisna številka: _____

Dovoljen je 1 A4 list z lastnimi zapiski. Druga literatura (npr. prosojnice, knjige) in elektronski pripomočki niso dovoljeni.
Nalogo rešujte v za to predviden prostor. Podpišite se na vse liste, ki jih oddate.
Na vprašanja odgovarjajte kratko (največ 2 povedi), daljši odgovori štejejo 0 točk.
Čas pisanja je 80 minut.

izpolni ocenjevalec

1	
2	
3	
4	
SKUPAJ	

1. NALOGA (5t):

Na skupni medij so priključena tri vozlišča (A, B in C), ki uporabljajo protokol razsekana ALOHA za dostop do medija. Vsako vozlišče želi oddati natanko en okvir, pri dogajanju pa se lahko zgodijo trki. V primeru trka vsako od treh vozlišč uporablja drugačen pristop k čakanju na ponovno oddajanje, in sicer:

- vozlišče A vedno odda v **prvem** naslednjem časovnem intervalu (intervalu, ki takoj sledi koliziji),
- vozlišče B odda v **prvem** ali **drugem** naslednjem časovnem intervalu z verjetnostima 40%:60%,
- vozlišče C odda v **drugem** ali **tretjem** naslednjem časovnem intervalu z verjetnostima 90%:10%.

Oddajanje se začne tako, da v 1. časovnem intervalu vsa vozlišča oddajo hkrati in povzročijo trk.

Naloge:

a.) Nariši najkrajše možno zaporedje oddajanj, v katerem se vsi okviri po prvem trku uspešno prenesejo.

b.) Kakšna je verjetnost scenarija iz naloge a?

c.) Nariši vse možne scenarije oddajanj, ki se lahko odvijejo v prvem in drugem naslednjem časovnem intervalu, ki sledi trku. Koliko različnih scenarijev obstaja?

2. NALOGA (5t):

Ana pošilja Branetu kriptograme, ki jih je izračunala z algoritmom RSA. Njen namen kriptiranja je zagotavljanje avtentikacije pošiljatelja.

a.) S kakšnim postopkom se bo Ana avtenticirala Branetu pri pošiljanju sporočila? Kolikokrat bo uporabila kriptiranje z metodo RSA za izračun enega kriptograma?

b.) V komunikacijo se vrine napadalec, ki si želi polastiti Aninega zasebnega ključa. Po dolgem opazovanju komunikacije med Ano in Branetom, javnih ključev obeh udeležencev in programa za izračun ključev, je napadalec uspel ugotoviti, da sta Anina ključa tvorjena s parametri: n=21, z=12, e=5 in da se čistopis 11 kriptira v kriptogram 2. Ravno tako je ugotovil, da je vrednost parametra d Aninega ključa med 15 in 20.

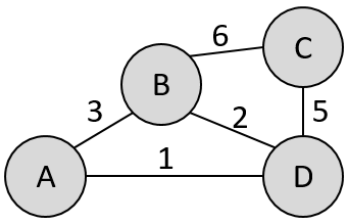
Določi najnižjo vrednost obeh komponent Aninega zasebnega ključa.

c.) Kateremu matematičnemu pogoju morata zadoščati javni in zasebni ključ? Preveri njegovo izpolnjenost in jo zapiši.

d.) Ali matematičnim pogojem za RSA ustreza tudi parameter d=5? Kakšno obliko kriptografije dobimo v primeru izbire tega parametra?

3. NALOGA (5t):

V prikazanem omrežju usmerjevalnikov se uporablja centralizirano usmerjanje glede na stanje povezav. V spodnjih tabelah so prikazane začetne posredovalne tabele vseh štirih usmerjevalnikov (A, B, C in D). Zapis D/7 npr. v drugem stolpcu pomeni, da A promet za usmerjevalnik C usmerja preko D po ceni 7).



usm. A	
B	B/2
C	D/7
D	D/2

usm. B	
A	A/2
C	D/7
D	D/2

usm. C	
A	D/7
B	D/7
D	D/5

usm.D	
A	A/2
B	B/2
C	C/5

Naloge:

a.) Usmerjevalniki si izmenjajo nove podatke o stanju povezav, ki so takšni, kot je prikazano na grafu na zgornji sliki. Izračunaj nove posredovalne tabele. V primeru več možnih poti z enako ceno, izberi tisto, ki gre preko usmerjevalnika, katerega črka je prej po abecedi.

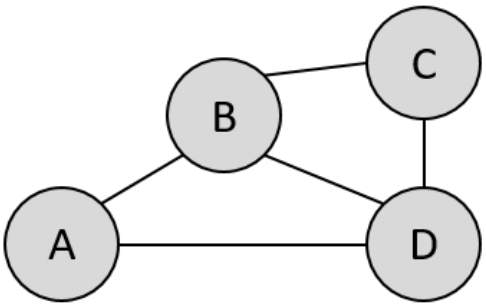
usm. A	
B	
C	
D	

usm. B	
A	
C	
D	

usm. C	
A	
B	
D	

usm.D	
A	
B	
C	

b.) Na spremembe katerih cen povezav lahko sklepaš s primerjavo začetnih in novih posredovalnih tabel? Zapiši njihove prejšnje vrednosti v spodnji graf.



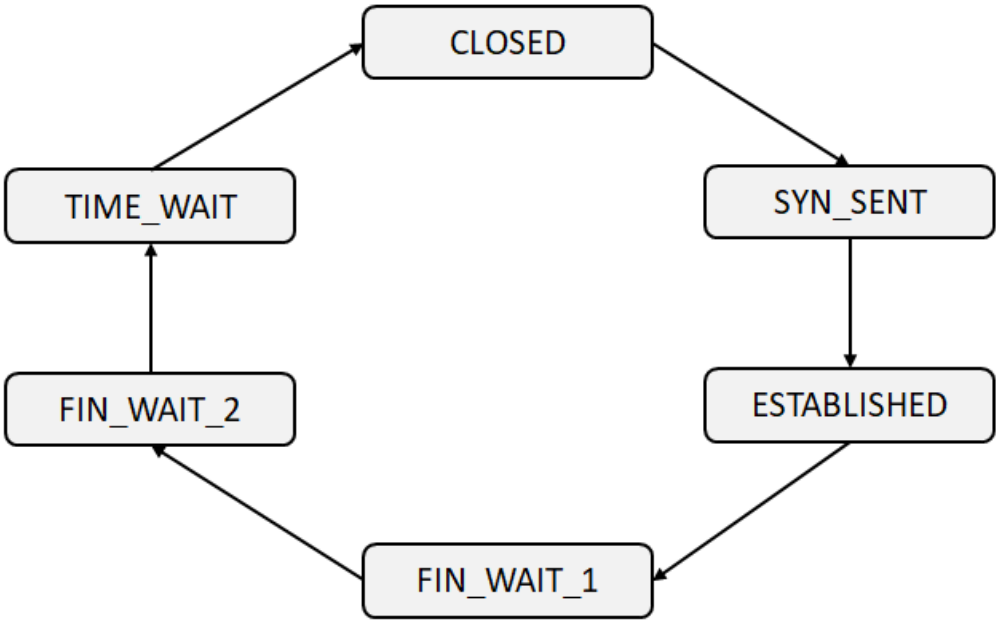
c.) Ali lahko katero koli od sprememb (iz naloge b) kategoriziramo v tipa "good news travel fast" ali "bad news travel slow"? Če da, katero? Če ne, zakaj ne?

4. NALOGA (5t):

Na sliki je prikazan končni avtomat pošiljatelja, ki prikazuje njegov življenjski cikel v kontekstu vzpostavljanja in rušenje povezave TCP.

Naloge:

a.) Dopolni končni avtomat z zapisom dejanj, ki povzročijo prehod med posameznimi stanji.



b.) Denimo, da želimo ustvariti novo različico protokola TCP, pri kateri se lahko pošiljatelj po začetku rušenja povezave še premisli in vrne nazaj v fazo pošiljanja. Premisli se lahko le do točke, preden začne tudi prejemnik rušiti povezavo. Predpostavimo, da o svoji vrnitvi v fazo vzpostavljene povezave, obvesti prejemnika s posebno novo zastavico, ki jo poimenujmo UNDO_FIN.
Dopolni diagram (na spodnji kopiji slike, označi samo dejanja na novih prehodih), da vsebuje zahtevano novo funkcionalnost.