RAČUNALNIŠKE KOMUNIKACIJE 2018/19

Ime in priimek: _____

2. kolokvij, 23. 5. 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):

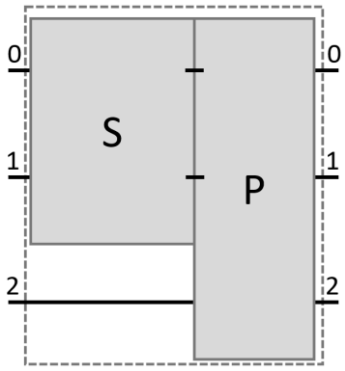
Pošiljatelj uporablja protokol TCP, ki samodejno nastavlja dolžino čakalnega intervala za čakanje na potrditve. Pri tem uporablja nastavitvi $\alpha = 0{,}1$ in $\beta = 0$.

Prvi izmerjeni RTT (IzmerjeniRTT[1]) in začetni čakalni interval znašata 20 ms.

a.) Na koliko se poveča čakalni interval, če naslednja meritev znaša 30 ms?

b.) Najmanj koliko mora biti vrednost naslednjega (drugega) izmerjenega RTT, da se čakalni interval poveča na več kot 28 ms?

2. NALOGA (5t):



Podan je bločni kriptosistem za bloke 3 bitov, ki je sestavljen iz S-škatle (dela na blokih 2 bitov) in P-škatle (dela na blokih 3 bitov), kot je prikazano na sliki. Prva dva bita kriptosistema vstopata samo v S-škatlo, tretji pa samo v P-škatlo. Pri tem velja:

- ključ dekoderja substitucijske škatle S je:
  00 → 0, 01 → 3, 10 → 2, 11 → 1
- ključ permutacije v substitucijski škatli S je (3102)
- ključ koderja substitucijske škatle S je:
  0 → 01, 1 → 10, 2 → 00, 3 → 11

Razvozlaj/ugotovi/določi ključ permutacijske škatle P, če z opazovanjem čistopisov in kriptogramov ugotoviš, da celotni kriptosistem izvaja preslikave, ki so prikazane v tabeli.

čistopis	kriptogram
000	000
001	010
010	100
011	110
100	101
101	111
110	001
111	011

Rešitev:

3. NALOGA (5t):

Pošiljatelj uporablja protokol TCP. Nariši shemo komunikacije med pošiljateljem in prejemnikom, če pošiljatelj uporablja okno velikosti 6, poslati pa želi 8 segmentov. Od teh se pri prvem pošiljanju 2. in 3. segment izgubita. Pošiljatelj naj ne uporablja zakasnjenega potrjevanja (delayed acknowledgement), uporablja pa naj hitro ponovno pošiljanje (fast retransmit) povsod, kjer je to možno. Prejemnik ima medpomnilnik, v katerem lahko začasno hrani do 10 segmentov.

4. NALOGA (5t):

Za prenos izbrane datoteke, ki je sestavljena iz treh kosov (chunks) K1, K2, K3, uporabimo protokol BitTorrent. S seznama odjemalcev, ki ga prenesemo s sledilnega strežnika, izberemo seznam petih sosedov S1, S2, ..., S5. Razpoložljivost kosov datoteke pri sosedih je naslednja (1 pomeni razpoložljivo, 0 nerazpoložljivo): S1=[1,0,1], S2=[0,0,0], S3=[1,0,1], S4=[0,0,0], S5=[1,1,0]. Vsak odjemalec pošilja podatke drugemu odjemalcu s hitrostjo, ki znaša 10+3*n Kbps (kilobitov na sekundo), pri čemer je n enako številu manjkajočih koščkov, ki jih pošiljatelj še nima, prejemnik pa ima. Podaj argumentiran odgovor na naslednja vprašanja:

a) V kakšnem vrstnem redu bo naš BitTorrent odjemalec prenesel koščke (predpostavi, da lahko vzporedno prenaša največ en košček naenkrat)?

b) S kakšno hitrostjo bo S3 prejemal podatke od preostalih odjemalcev? Lahko predpostaviš, da je ves čas razpoložljivost koščkov pri odjemalcih S1 – S5 enaka in da je množica sosedov za vse odjemalce ves čas enaka.