RAČUNALNIŠKE KOMUNIKACIJE 2021/22

Ime in priimek: _____

2. izpit, 20. 6. 2022

Vpisna številka: _____

Dovoljen je 1 A4 list z lastnimi zapiski. Druga literatura (npr. prosojnice, knjige) ni dovoljena. Dovoljen je preprost kalkulator.
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.
Odgovori na vprašanja morajo biti utemeljeni. Čas pisanja je 90 minut.

izpolni ocenjevalec

1	
2	
3	
4	
SKUPAJ	

1. NALOGA (25t):

Odgovori na naslednja vprašanja, odgovore utemelji:

1. Denimo, da uporabljamo kvadratno modulacijo z 12 faznimi koti. Koliko nivojev amplitude najmanj potrebujemo, če želimo kodirati zaporedja 6 bitov?

2. Za niz 000000000 oblikujemo 2D paritetno shemo dimenzij 3x3. Kakšna je vrednost meta-paritetnega bita, če se za vrstice, stolpce in meta-pariteto uporablja liha paritetna shema?

3. Ana in Borut sta povezana s 100 m dolgim vodilom, na katerem je propagacijska hitrost signala 2000 m/s. Ob nekem času začne Ana z oddajanjem svojega okvirja velikosti 1000 B, 40 ms kasneje pa še Borut z oddajanjem svojega okvirja velikosti 500 B. Ana pošilja s hitrostjo 100 Kbit/s, Borut pa s hitrostjo 80 KBit/s. Kako dolgo po začetku Aninega pošiljanja pride do trka na mediju?

4. Na katera od vrat bo usmerjevalnik posredoval paket za naslov 212.235.188.15, upoštevajoč spodnjo posredovalno tabelo? Odgovor utemelji.

   212.235.176.0/20 -> vrata1
   212.235.144.0/20 -> vrata2
   212.235.176.0/21 -> vrata3
   212.235.190.0/23 -> vrata4

5. Pošiljatelju, ki uporablja TCP Reno, v nekem trenutku postane cwnd=9, vrednost praga pa znaša 16. Kolikšna je nova vrednost cwnd in praga po prejemu 30 (različnih) potrditev segmentov, katerim sledijo 3 kopije iste ponovljene potrditve? Decimalke zaokrožuj na najbližje celo število.

2. NALOGA (25t):

Komunikacijski kanal s kapaciteto 40 Mbps uporabljajo štirje vmesniki (A, B, C in D). Vmesniki A, B in C uporabljajo protokol TCP, vmesnik D pa uporablja protokol UDP. Začetne hitrosti pošiljanja so podane v spodnji tabeli. Hitrost A, B in C nato narašča tako, da si preostalo razpoložljivo hitrost med seboj enakomerno razdelijo, pri tem pa upoštevajo trenutno hitrost vmesnika D (podana v tabeli); v tem času se hitrost vmesnika D ne spreminja. Vsakič, ko pride do zasičenja omrežja, se hitrost spremeni v skladu s poenostavljenimi pravili o pravičnosti, ki smo jih obravnavali na predavanjih. Izračunaj, kakšne so hitrosti vmesnikov. Izračunaj toliko iteracij, dokler hitrosti vmesnikov A, B, C ne dosežejo pravične delitve kanala – v našem primeru se to zgodi, ko je največja medsebojna dovoljena razlika v njihovih hitrostih največ 1 Mbps.

Vsaj eno iteracijo postopka računsko utemelji.

	A	**B**	**C**	**D**
začetne hitrosti [Mbps]	12	4	8	4
1. iteracija – povečanje hitrosti				4
1. iteracija – zmanjšanje hitrosti				4
2. iteracija – povečanje hitrosti				7
2. iteracija – zmanjšanje hitrosti				7
3. iteracija – povečanje hitrosti				10
3. iteracija – zmanjšanje hitrosti				10
4. iteracija – povečanje hitrosti				13
4. iteracija – zmanjšanje hitrosti				13
5. iteracija – povečanje hitrosti				1
5. iteracija – zmanjšanje hitrosti				1

3. NALOGA (25t):

Podan je bločni kriptosistem, ki je tvorjen iz ene same S-škatle. Ta je sestavljena iz dekoderja 3/8, P-škatle in koderja 8/3. Ključa dekoderja in koderja sta podana v tabelah na desni strani, ključ P-škatle pa je (31257604).

dekoder	
000	2
001	4
010	5
011	1
100	0
101	6
110	7
111	3

koder	
0	011
1	101
2	110
3	000
4	111
5	001
6	010
7	100

Odgovori na naslednja vprašanja, razviden naj bo postopek reševanja:

a.) Kakšen je ključ celotnega kriptosistema? Odgovor podaj v spodnji tabeli.

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

b.) Nekega dne se dekoder pokvari in zamenjati ga moramo z novim. Žal pa imamo na zalogi samo drugačne dekoderje (dekoder2), ki imajo ključ, kot je prikazan na desni. Da bo celoten kriptosistem deloval ekvivalentno (z enakim ključem celotnega kriptosistema), moramo posledično zamenjati tudi P-škatlo s škatlo P2, ki bo zagotovila pravilno delovanje.
Določi ključ nove škatle P2.

dekoder2	
000	1
001	3
010	5
011	7
100	0
101	2
110	4
111	6

c.) Skupaj s kriptosistemom iz naloge a) se odločimo uporabiti verižno kriptiranje blokov z IV=111. Izračunaj prve tri kriptograme čistopisa 010.

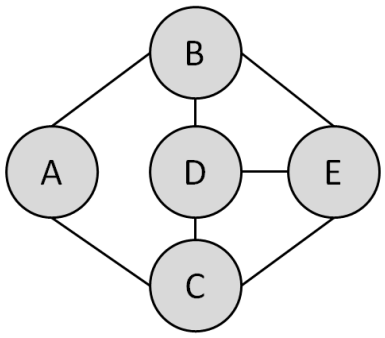
1. kriptogram:

2. kriptogram:

3. kriptogram:

4. NALOGA (25t):

V omrežju imamo brezžične terminale A, B, C, D in E, ki so medsebojno dosegljivi tako, kot prikazuje slika na desni. Terminali za komunikacijo uporabljajo protokol CSMA/CA.



a.) Katere od spodnjih izmenjav okvirjev so uspešne ob pogoju, da je predhodno že vzpostavljena izmenjava podatkov (uspešno je bila odvita sekvenca RTS/CTS in trenutno že teče pošiljanje podatkovnih okvirjev)? Za vsakega od spodnjih primerov podaj odgovor in utemeljitev. Legenda: X→ Y označuje smer prenosa okvirja.

Obstoječa komunikacija (povezava predhodno vzpostavljena z RTS/CTS + teče izmenjava podatkov)	**Ali je med obstoječo komunikacijo možna tudi izmenjava okvirja med naslednjimi terminali?**	**Odgovor, izberi izmed (zapiši številko):** **(1) komunikacija je možna** **(2) komunikacija ni možna, ker jo preprečujeta RTS/CTS** **(3) komunikacija ni možna, ker jo preprečuje trk okvirjev**	**Utemeljitev:**
A → C	B → E		
C → A	E → D		
E → C	A → B		
E → D	A → B		
D → B	C → A		

b.) Zapiši vse postavitve skritih terminalov, v katerih kot pošiljatelj nastopa terminal A.