RAČUNALNIŠKE KOMUNIKACIJE 2021/22

Ime in priimek: _____

1. izpit, 30. 5. 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.
Čas pisanja je 90 minut.

izpolni ocenjevalec

1	
2	
3	
4	
SKUPAJ	

1. NALOGA (25t):

Odgovori na naslednja vprašanja:

1. Prejemnik prejme zaporedje bitov, ki je opremljeno s Hammingovo kodo in ima vrednost 1101101. Kakšna je vrednost prejetega sporočila?

2. Paket IPv4, ki ne uporablja opcij in je velikosti 1300B, želimo poslati po povezavi, ki ima MTU=400B. Kakšne so vrednosti odmikov (offset) poslanih fragmentov?

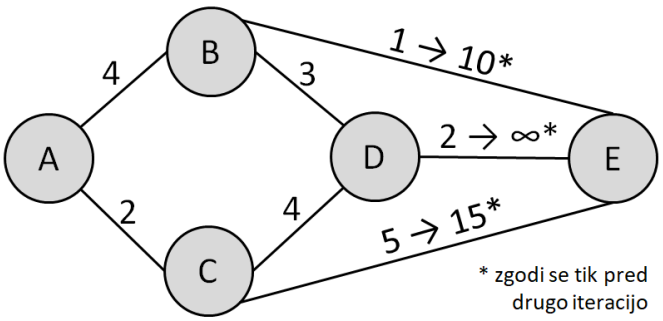
3. Kolikšna je vrednost parametra MSS, če velja in MTU=1000B, na 3. in 4. plasti pa se uporabljata protokol IPv4 in TCP, ki v glavah ne uporabljata opcij?

4. Pošiljatelju, ki uporablja TCP Reno, v nekem trenutku postane cwnd=12, vrednost praga pa znaša 16. Kolikšna je nova vrednost cwnd po prejemu 30 (različnih) potrditev segmentov?

5. Kakšen je ključ P-škatle, ki je inverzna P-škatli s ključem (50134276)?

2. NALOGA (25t):

V omrežju imamo 5 usmerjevalnikov (A, B, C, D in E), ki uporabljajo usmerjanje z vektorji razdalj na podlagi cen, ki so podane na grafu na desni sliki. Usmerjevalniki imajo ob začetku opazovanja v posredovalnih tabelah naučene takšne ocene razdalj do **usmerjevalnika E**, kot je to zapisano v prvi vrstici tabele. Zapiši, kako se v naslednjih treh iteracijah spreminja ocenjena cena poti do usmerjevalnika E znotraj posredovalnih tabel vsakega izmed preostalih usmerjevalnikov. Pri tem upoštevaj, da se tik pred računanjem druge iteracije posredovalnih tabel spremenijo cene povezav BE z 1 na 10, CE s 5 na 15, povezava DE pa se prekine (kot je prikazano na sliki). V primeru, če je na razpolago več poti z isto ceno, izberite pot preko usmerjevalnika, katerega oznaka je prej po abecednem vrstnem redu.



Odgovor podaj v strukturi prikazane tabele (lahko jo prerišeš tudi na list). Pri tem naj bodo zapisi v celicah tabele jasno podprti z računskimi postopki.

	ocenjene cene do usmerjevalnika E			
iteracija \ usmerjevalnik	**A**	**B**	**C**	**D**
začetno stanje	6/C	5/D	6/D	2/E
1. iteracija				
2. iteracija (upoštevajoč predhodno spremembo cen BE, CE in DE)				
3. iteracija				

3. NALOGA (25t):

Pošiljatelj uporablja protokol TCP. Poslati želi 8 segmentov, pri tem pa uporablja okno velikosti 5. Pri prvem pošiljanju se 7 segment izgubi. Nariši diagram komunikacije med pošiljateljem in prejemnikom, pri tem pa upoštevaj, da:

- prejemnik uporablja zakasnjeno potrjevanje (delayed acknowledgment) s privzetim intervalom 500 ms,
- kadar okno ni polno, pošiljatelj pošilja pakete z veliko hitrostjo, ki je << 500 ms (vedno takoj pošlje vse pakete, ki jih lahko),
- RTT je tolikšen, da potrditve pridejo po tem, ko se pošljejo vsi paketi do zapolnitve okna,
- dolžina čakalnega intervala je veliko večja od časa RTT (npr. 10×RTT).

Rešitev:

4. NALOGA (25t):

Ana in Brane se dogovorita, da imata v prihodnji medsebojni komunikaciji na razpolago naslednji nabor kriptografskih algoritmov, parametrov in ključev. Pri tem pa bosta uporabila samo tiste od naslednjih, ki so zahtevani za posamezen namen (nalogo spodaj) in ne vseh:

- **algoritem za simetrično bločno kriptografijo**, ki deluje na naslednji način:
  - algoritem deluje na blokih dolžine k=8,
  - tvorjen je iz dveh zaporednih P-škatel s ključem (30124756),
  - uporablja verižno kriptiranje blokov z IV=01100001,
- **tajni ključ** za zgoščanje z vrednostjo 11,
- **žeton** (nonce, sol) za zgoščanje z vrednostjo 10,
- **algoritem RSA:**
  - pred kriptiranjem se čistopis v binarni obliki pretvori v desetiško vrednost,
  - rezultat kriptiranja ohranimo v desetiškem zapisu,
  - Anina ključa: E_A=(n=77,e=43), D_A=(n=77,d=7),
  - Branetova ključa: E_B=(n=15,e=3), D_B=(n=15,d=27),
- **zgoščevalno funkcijo**, ki deluje na naslednji način:
  - algoritem najprej iz čistopisa izračuna kontrolno vsoto po enakem algoritmu, kot računamo internetno kontrolno vsoto, le da dogovorjen algoritem deluje na 4-bitnih in ne 16-bitnih besedah,
  - na dobljeni 4-bitni kontrolni vsoti v naslednjem koraku uporabimo P-škatlo s ključem (3012).

Pri vsaki nalogi izberi najmanjši potreben nabor zgornjih metod, ki zadoščajo zahtevam nalog. Naloge:

a.) Ob neki priložnosti se Ana odloči *digitalno podpisati* svoje sporočilo m=01101100 in poslati digitalni podpis Branetu. Izračunaj vrednost digitalnega podpisa.

b.) (neodvisno vprašanje od prejšnje naloge) Ana ugotovi, da je napadalec izvedel kriptoanalizo njune simetrične kriptografske metode, zato jo želi popolnoma spremeniti. Z Branetom mora zato varno izmenjati ključ nove simetrične metode, ki ima vrednost 00001000. Zapiši Anino sporočilo, namenjeno Branetu, ki zagotavlja varno izmenjavo simetričnega ključa.

c.) Ali odgovor iz naloge b) zagotavlja tudi integriteto sporočila? Če DA, obrazloži, kako (brez računanja, v 1 povedi). Če NE, obrazloži, kako bi zagotovil tudi to (brez računanja, v 1 povedi).