RAČUNALNIŠKE KOMUNIKACIJE 2022/23

Ime in priimek: _____

3. izpit, 8. 9. 2023

Vpisna številka: _____

Literatura (npr. zapiski, 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. Pošiljatelji A, B in C uporabljajo protokol ALOHA. Pošiljatelji v primeru trka s 30% verjetnostjo ponovno oddajo okvir v prvem naslednjem časovnem intervalu, s 70% verjetnostjo pa v drugem naslednjem. Na začetku komunikacije (T=0) želita A in B oddajati hkrati (zgodil se bo trk), C pa bo svoj okvir oddal v naslednjem časovnem intervalu (T=1). Kakšna je verjetnost trka v tem časovnem intervalu (T=1)?

2. Za preslikavo katerega IP naslova v fizični naslov uporabimo protokol ARP v primerih, če:

   - želimo nasloviti IP naslov znotraj lokalnega omrežja: _____

   - želimo nasloviti IP naslov izven lokalnega omrežja _____

3. V povezavnem tipu omrežja, v katerem se uporabljajo navidezni vodi, sta računalnika A in B zaporedno povezana preko usmerjevalnikov X in Y (v topologiji A – X – Y – B). Promet, ki je namenjen računalniku B, računalnik A oddaja na vodu št. 41, B pa ta promet sprejema na vodu št. 98. Podaj zapisa, ki morata biti prisotna v usmerjevalnikih X in Y, da je povezava med A in B uspešno vzpostavljena. Morebitne manjkajoče podatke izberi sam poljubno.

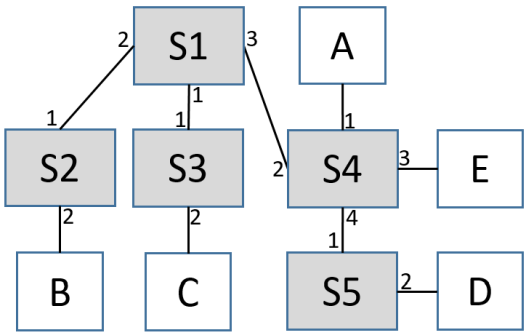
4. Kaj pomeni, da mehanizem NAT krši princip končnih sistemov (angl. end-to-end argument)?

5. Na lokalni DNS naslovimo poizvedbo naprej za ime xx.yy.zz.com, nato pa za ime xx.yy.zz.org. Predpomnilnik je na začetku prazen, sproti pa se napolni z vsemi vmesnimi poizvedbami. Naštej, katere poizvedbe bodo poslane in na kateri tip DNS strežnika.

2. NALOGA (25t):

Podan je sistem stikal (S1 – S5) in vmesnikov (A – E), kot je prikazan na sliki. Ob stikalih so podane tudi številke njihovih posameznih vrat. Začetno stanje stikalnih tabel podaja prva vrstica spodnje tabele. Med vmesniki se nato odvijejo dogodki, kot to podajajo vrstice v tabeli (X → Y pomeni, da pošiljatelj X pošlje okvir prejemniku Y). Za vsak korak navedene komunikacije zapiši:

- vsebine stikalnih tabel na podanem koraku v obliki seznama oblike **vmesnik/vrata**, npr. »B/2, C/2«),
- katero **akcijo** izvede stikalo na danem koraku.



	stikalo S1	**stikalo S2**	**stikalo S3**	**stikalo S4**	**stikalo S5**
začetno stanje	D/3, A/3, B/2	B/2	D/1	A/1, B/2	D/2, A/1, B/1
C → B					
E → D					
v vseh stikalih poteče TTL za najstarejši (prvi) zapis					
C → A					

3. NALOGA (25t):

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

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

a.) Na koliko se poveča čakalni interval, če naslednja meritev znaša 40 ms?

b.) Najmanj koliko mora biti vrednost naslednjega (drugega) izmerjenega RTT, da se čakalni interval poveča na več kot 35 ms?

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 in Branetova ključa: **glej spodnje naloge**.
- **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 <u>najmanjši potreben nabor zgornjih metod,</u> ki zadoščajo zahtevam nalog. Naloge:

a.) Napadalec želi odkriti Anin ključ za kriptografijo RSA, pri čemer se je dokopal do podatkov: p=11, q=7, e=37 in $10 \leq d < 15$. Izračunaj Anin zasebni in javni ključ.

Zasebni ključ:

Javni ključ:

a.) Branetova ključa sta RSA sta: E_B=(n=15,e=3), D_B=(n=15,d=27). Ob neki priložnosti se Brane odloči digitalno podpisati svoje sporočilo m=00101100 in poslati digitalni podpis Ani. Izračunaj vrednost digitalnega podpisa.