RAČUNALNIŠKE KOMUNIKACIJE 2022/23

Ime in priimek: _____

1. izpit, 21. 6. 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. Napadalec želi izvesti DDoS napad Smurf. Odgovori na vprašanja:
   - Katera lastnost izbranega omrežja nevede pomaga napadalcu, da lahko izvede napad?

     _____
   - Kako napadalec pripravi paket, da izvede napad? Kaj je v njem posebnega?

     _____
   - Zakaj/kako napad škoduje izbrani žrtvi?

     _____

2. Izračunaj Vigenèrjev kriptogram čistopisa IZPIT. Kot ključ za kriptiranje uporabi besedo STOL. Za kriptiranje uporabi črke slovenske abecede (ABCČDEFGHIJKLMNOPRSŠTUVZŽ).

3. Pošiljatelju, ki uporablja TCP Reno, v nekem trenutku postane cwnd=10, vrednost praga pa znaša 16. Kolikšna je vrednost cwnd in praga po naslednjih dveh dogodkih:
   - pošiljatelj prejme 120 (različnih) potrditev segmentov,
   - nato pošiljatelj prejme 3 kopije iste potrditve.

4. Prejemnik prejme zaporedje bitov, ki je opremljeno s Hammingovo kodo in ima vrednost 1111110. Kakšna je vrednost prejetega sporočila?

5. 9 različnih računalniških sistemov uporablja sistem ASN.1 za predstavitev podatkov. Za koliko se zmanjša potrebno število različnih konverzij podatkovnih tipov pri uporabi ASN.1 v primerjavi s pristopom, ko sistemi neposredno pretvarjajo v vse ostale podatkovne tipe.

2. NALOGA (25t):

Podan je bločni kriptografski sistem za bloke dolžine 3, katerega ključ je podan v tabeli na desni strani. Skupaj s tem bločnim kriptosistemom uporabljamo tudi verižno kriptiranje blokov, pri čemer uporabimo inicializacijski vektor enak 011.

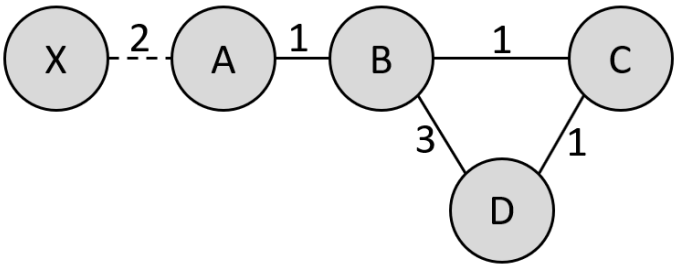
čistopis	**kriptogram**
000	100
001	101
010	011
011	110
100	001
101	111
110	000
111	010

Naloga: Izračunaj prvih 8 kriptogramov c(1) ... c(8) za čistopis 011.
Odgovore jasno zapiši v spodnjo tabelo.

c(1)	
c(2)	
c(3)	
c(4)	
c(5)	
c(6)	
c(7)	
c(8)	

Prostor za reševanje:

3. NALOGA (25t):



V omrežju imamo 5 usmerjevalnikov (A, B, C, D in X), 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 X**, kot je to zapisano v prvi vrstici tabele. Nato se povezava med A in X prekine (narisano črtkano na sliki). Zapiši, kako se v naslednjih štirih iteracijah spreminja ocenjena cena poti do usmerjevalnika X znotraj posredovalnih tabel vsakega izmed preostalih usmerjevalnikov. 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 X			
iteracija \ usmerjevalnik	**A**	**B**	**C**	**D**
začetno stanje	2/X	3/A	4/B	5/C
prekinitev povezave A-X				
1. iteracija				
2. iteracija				
3. iteracija				
4. iteracija				

4. NALOGA (25t):

Pošiljatelj in prejemnik uporabljata protokol za potrjevanje, ki uporablja velikost okna 6. Pošiljatelj pošlje prejemniku 6 segmentov, od katerih se tretji pri prvem pošiljanju izgubi. Za pošiljatelja in prejemnika veljajo tudi naslednje lastnosti:

- Pošiljatelj vedno pošilja z maksimalno hitrostjo, dokler ne zapolni okna, šele nato čaka na potrditve in morebiten potek časovnih intervalov.
- Zakasnitev na komunikacijskem mediju je majhna, zato prejemnik prejema pakete z majhnim časovnim razmikom (<500ms), kot so bili tudi poslani.

Nariši shemo komuniciranja za dva različna scenarija:

a.) Pošiljatelj in prejemnik uporabljata TCP, ki dodatno uporablja tudi mehanizem zakasnjenega potrjevanja (angl. delayed acknowledgment).

b.) Pošiljatelj in prejemnik uporabljata protokol za ponavljanje N nepotrjenih segmentov (angl. go-back-N).