RAČUNALNIŠKE KOMUNIKACIJE 2021/22

Ime in priimek: _____

3. izpit, 8. 9. 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 je med usmerjevalnikoma A in B vzpostavljen tunel kot prehodni mehanizem med IPv4 in IPv6. Do usmerjevalnika A in za usmerjevalnikom B teče promet s protokolom IPv6. Kakšna je velikost paketa v tunelu med A in B, če je njegova velikost pred vstopom v tunel enaka 1500 B in se na omrežni plasti dodatno uporabljajo tudi opcije v glavi paketov, ki zasedejo 4 B?

2. Kakšen je Vigenèrjev kriptogram čistopisa »banana« s ključem »bcd«? Uporabljamo angleško abecedo: ABCDEFGHIJKLMNOPQRSTUVWXYZ.

3. Za koliko zmanjšamo število potrebnih preslikav med podatkovnimi tipi 7 različnih sistemov, če na predstavitveni plasti uporabimo standard ASN.1 za predstavitev podatkov?

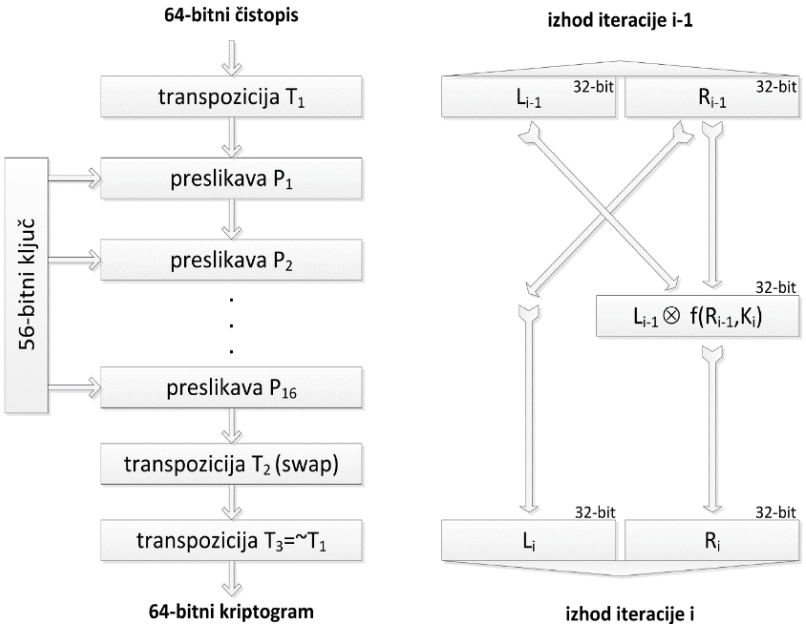
4. Prenesti moramo 1 HTML stran in 12 slik s spletne strani. Vsakega od naštetih objektov lahko prenesemo v enem samem TCP segmentu, MSS znaša 1460 B, uporabljamo IPv6, RTT pa znaša 200 ms. Koliko časa bo trajal prenos po nevztrajni in vztrajni http povezavi? Čas za rušenje povezave zanemari.

5. Pošiljatelj in prejemnik uporabljata protokol CSMA/CD z eksponentnim povečevanjem časa čakanja ob trkih (exponential backoff time). Predpostavimo, da pri tem ne uporabljata zgornje meje za dolžino čakalnega intervala. Kakšna je verjetnost ponovnega trka po 7. ponovitvi trka pri pošiljanju istega okvirja?

2. NALOGA (25t):

Denimo, da si izmislimo novi algoritem DESeasy, ki pri svojem delovanju uporablja samo 1 preslikavo namesto 16, kot to velja za pravi DES (skica delovanja originalnega algoritma DES je v pomoč prikazana na spodnji sliki). Za DESeasy velja tudi, da:

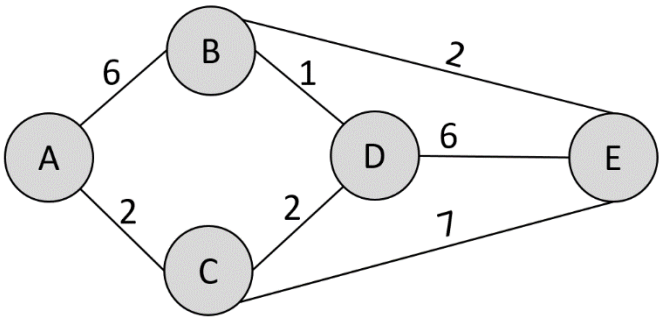
- deluje na 8-bitnih blokih,
- ključ transpozicije T1 je (74215036),
- transpoziciji T2 (swap) in T3 (inverz T1) delujeta enako kot pri DES,
- preslikava v svojem jedru računa $L_{i-1} \otimes f(R_{i-1}, K_i)$, pri čemer velja:
    - $\otimes$ = XOR
    - $K_i = 1110$
    - $f(x, y) = x + y$, pri čemer morebitni prenos prištejemo k rezultatu (kot to naredimo pri internetni kontrolni vsoti)



Naloga: Izračunaj kriptogram čistopisa 11011010 z algoritmom DESeasy. Jasno zapiši rezultat vsakega posameznega koraka algoritma.

3. NALOGA (25t):

V omrežju imamo 5 usmerjevalnikov (A, B, C, D in E), ki uporabljajo usmerjanje na podlagi cen, ki so podane na grafu na desni sliki. Na začetku so vse posredovalne tabele prazne. Odgovori na spodnja vprašanja.



a.) Denimo, da usmerjevalniki uporabljajo usmerjanje na podlagi stanja povezav in da so vsi v isti avtonomni coni. Navedi, komu ob vsaki iteraciji pošljeta podatke o stanju povezav usmerjevalnika A in D, če uporabljamo

- usmerjanje na podlagi stanja povezav: _____
- usmerjanje na podlagi vektorjev razdalj: _____

b.) Denimo, da usmerjevalniki uporabljajo usmerjanje na podlagi stanja povezav. Zapiši usmerjevalne tabele vseh petih usmerjevalnikov, ki jih izračunajo po prvi izmenjavi podatkov o stanju povezav. V tabele zapiši **izhodna vrata** (oznako sosednjega usmerjevalnika, ki mu posredujejo pakete za podani cilj) in skupno **ceno poti** do cilja (torej zapišite npr. »A/3«). V primeru, da je na razpolago več poti z isto ceno, izberite pot preko usmerjevalnika, katerega oznaka je prej po abecednem vrstnem redu.

A

cilj	vrata/cena
A	
B	
C	
D	
E	

D

cilj	vrata/cena
A	
B	
C	
D	
E	

E

cilj	vrata/cena
A	
B	
C	
D	
E	

c.) Denimo, da usmerjevalniki uporabljajo usmerjanje na podlagi vektorjev razdalj. Ob prvi izmenjavi vektorjev razdalj si usmerjevalniki med seboj izmenjajo vektorje, ki so se jih naučili prejšnji podnalogi (b), cene na vseh povezavah na sliki pa zrastejo za 1 (npr. cena A-B se poveča na 7, cena A-C na 3 itd.). Izračunaj posredovalni tabeli usmerjevalnikov B in C. Odgovore računsko utemelji za vsaj tri primere izračuna!

B

cilj	vrata/cena
A	
B	
C	
D	
E	

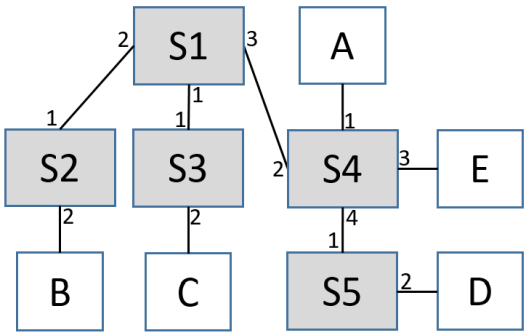
C

cilj	vrata/cena
A	
B	
C	
D	
E	

4. 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. Na začetku so stikalne tabele prazne. 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
D → C					
v stikalih S2 in S4 poteče TTL vsem zapisom					
A → D					
B → A					
B → D					
v stikalu S1 poteče TTL vsem zapisom					
C → B					