RAČUNALNIŠKE KOMUNIKACIJE 2022/23

Ime in priimek: _____

1. izpit, 2. 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. 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 12 B?

2. Brezžični terminali A, B, C in D so postavljeni tako, da so si A, B in C v medsebojnih dosegih (vsak vidi preostala dva), D pa je samo v dosegu s terminalom C. Če A v nekem trenutku pošilja okvir prejemniku B, ali lahko D uspešno pošlje okvir terminalu C?

3. V kakšni kodni tabeli mora biti predstavljeno aplikacijsko sporočilo protokola SMTP? Zakaj?

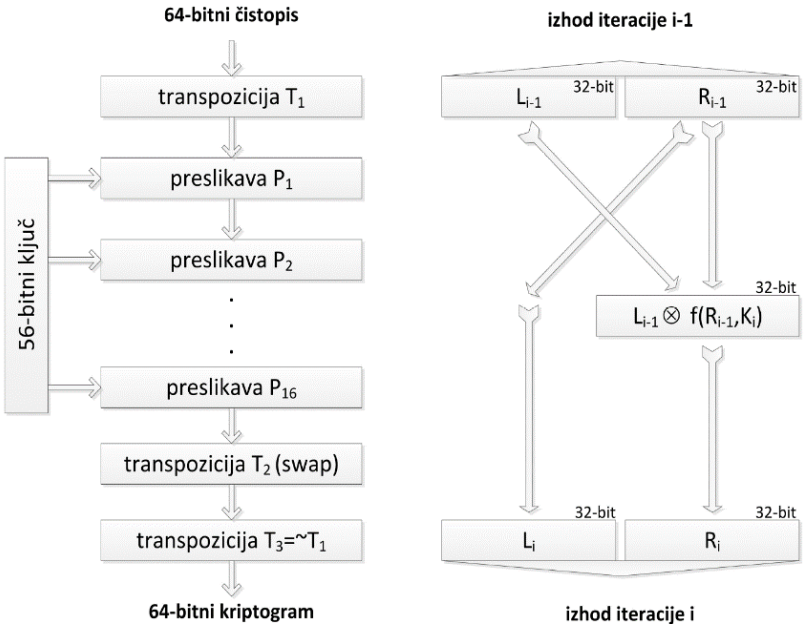
4. Prenesti moramo 1 HTML stran in 12 slik s spletne strani. Vsakega od naštetih objektov lahko prenesemo v enem samem TCP segmentu, MSS znaša 1460 B, uporabljamo IPv6, RTT pa znaša 200 ms. Koliko časa bo trajal prenos po nevztrajni in vztrajni http povezavi? Čas za rušenje povezave zanemari.

5. Kateri tip sistema IDS ima večje težave s spregledanimi napadi zaradi performančnih omejitev? Zakaj (utemeljitev v 1 kratki povedi)?

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:

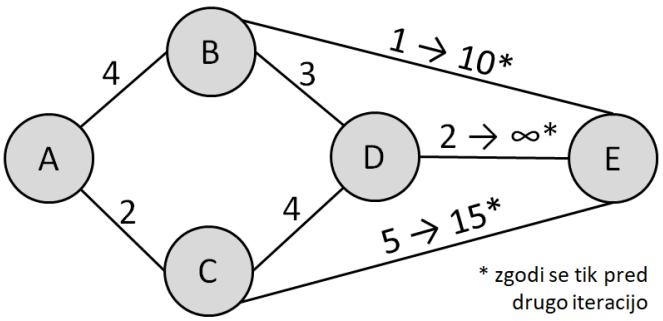
- deluje na 8-bitnih blokih,
- ključ transpozicije T1 je (41602753),
- transpoziciji T2 (swap) in T3 (inverz T1) delujeta enako kot pri DES,
- preslikava v svojem jedru računa $L_{i-1} \otimes f(R_{i-1}, K_i)$, pri čemer velja:
    - $\otimes$ = XOR
    - $K_i = 1010$
    - $f(x, y) = x + y$, pri čemer 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 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	2/C	1/A	4/D	4/B
1. iteracija				
2. iteracija (upoštevajoč predhodno spremembo cen BE, CE in DE)				
3. iteracija				

4. NALOGA (25t):

Komunikacijski kanal s kapaciteto 60 Mbps uporabljajo trije pošiljatelji (A, B in C), pri čemer vsak uporablja drugačno različico protokola TCP, in sicer takšno, da ob zasičenju:

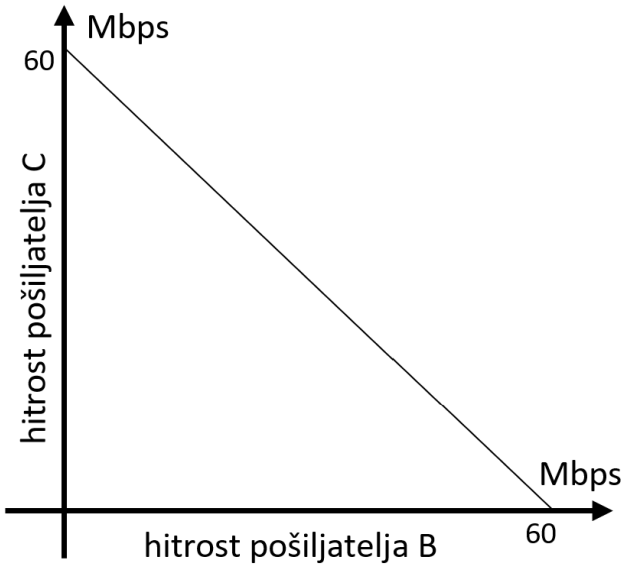
- A svojo hitrost pošiljanja zmanjša za 2 Mbps,
- B svojo hitrost pošiljanja zmanjša za 12 Mbps,
- C svojo hitrost pošiljanja zmanjša za 7 Mbps.

Pošiljatelji A, B in C na začetku oddajajo s hitrostmi 3 Mbps, 12 Mbps in 6 Mbps. Hitrost pošiljateljev A, B in C vedno narašča tako, da od prestale razpoložljive hitrosti A in B vzameta po 1/3 zaokroženo navzdol, pošiljatelj C pa preostanek (npr. 11 Mbps bi se razdelilo na A: $\lfloor 11/3 \rfloor = 3$ Mbps, B: $\lfloor 11/3 \rfloor = 3$ Mbps, C: $11 - 2 \cdot \lfloor 11/3 \rfloor = 11 - 6 = 5$ Mbps).
Naloge:

a.) Izračunaj, kakšne so hitrosti pošiljateljev A, B in C po štirih iteracijah povečevanja hitrosti.

	A	B	C
začetek	3	12	6
1. povečanje			
1. znižanje			
2. povečanje			
2. znižanje			
3. povečanje			
3. znižanje			
4. povečanje			

b.) V spodnji graf pravične delitve hitrosti vriši podatke za par pošiljateljev: B-C.



Kaj opaziš na zgornjem grafu glede pravične delitve hitrosti iz zgornjih grafov?