RAČUNALNIŠKE KOMUNIKACIJE 2018/19

Ime in priimek: _____

1. izpit, 19. 6. 2019

Vpisna številka: _____

Dovoljen je 1 A4 list z lastnimi zapiski. Druga literatura (npr. prosojnice, knjige) in elektronski pripomočki niso dovoljeni.
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 80 minut.

izpolni ocenjevalec

1	
2	
3	
4	
SKUPAJ	

1. NALOGA (5t):

Uporabljamo verižno kriptiranje blokov po 2 bita, v komunikacijo pa se vrine prisluškovalec, ki opazuje promet. Skozi čas prisluškovalec ugotovi naslednje:

- da pošiljatelj in prejemnik uporabljata inicializacijski vektor, ki je enak 10,
- da pošiljatelj ves čas pošilja isti čistopis, ki je 11,
- da je zaporedje kriptogramov, ki jih je poslal pošiljatelj, enako: c(1)=01, c(2)=00, c(3)=10, c(4)=c(1)=01, c(5)=c(2)=00, c(6)=c(3)=10 itd. (zaporedje kriptogramov c(1), c(2) in c(3) se ponavlja).

Naloga:

a.) Opravi kriptoanalizo in določi ključ (substitucijsko tabelo) bločnega sistema. Rešitev vnesi v tabelo.

čistopis	kriptogram
00	
01	
10	
11	

b.) Najmanj koliko prejetih kriptogramov v nalogi a) potrebujemo, da lahko uspešno opravimo kriptoanalizo?

c.) Koliko prejetih kriptogramov bi potrebovali, če napadalec v nalogi a) ne bi poznal inicializacijskega vektorja? Ali je v tem primeru kriptoanaliza sploh možna?

2. NALOGA (5t):

Komunikacijski kanal s kapaciteto 48 Mbps uporabljajo trije pošiljatelji (A, B in C), pri čemer vsak uporablja drugačno različico protokola TCP, in sicer takšno, da ob zasičenju:

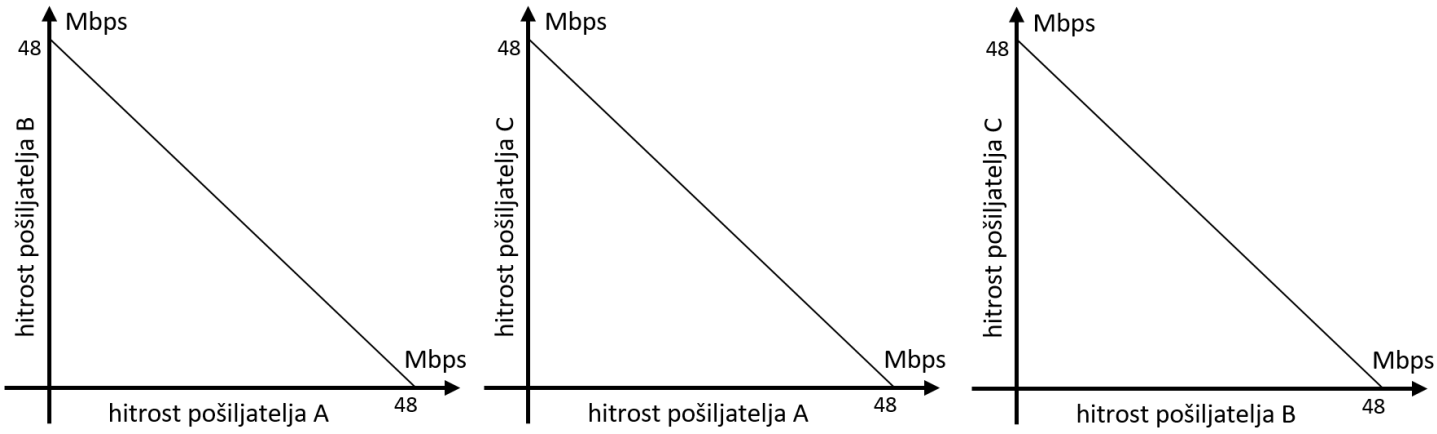
- A svojo hitrost pošiljanja prepolovi,
- B svojo hitrost pošiljanja nastavi na 1 Mbps,
- C svojo hitrost pošiljanja zmanjša za 1 Mbps.

Pošiljatelji A, B in C na začetku oddajajo s hitrostmi 3 Mbps, 9 Mbps in 3 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					
1. povečanje					
1. znižanje					
2. povečanje					
2. znižanje					
3. povečanje					
3. znižanje					
4. povečanje					

b.) V spodnje grafe pravične delitve hitrosti vriši podatke za tri pare pošiljateljev: A-B, A-C in B-C.



c.) Kaj opaziš glede pravične delitve hitrosti iz zgornjih grafov?

3. NALOGA (5t):

Odgovori na spodnja vprašanja o napadu DDOS Smurf (odgovarjaj kratko!):

a.) Katero šibkost v konfiguraciji usmerjevalnika izkorišča ta napad?

---

b.) Zakaj napad označujemo s kratico DDOS? Kakšen je pomen prve črke v tej kratici (D) – razloži, kakšno lastnost opisuje?

---

c.) Katero šibkost pri zasnovi paketa IP izkorišča ta napad?

---

d.) Na kakšen način bi se lahko zlorabljeno omrežje (poleg spremembe konfiguracije usmerjevalnika) ubranilo sodelovanja v takšnem napadu?

---

e.) Na kakšen način bi se lahko žrtev ubranila napada?

---

4. NALOGA (5t):

Denimo, da uporabljamo lokalni strežnik DNS, ki za nas izvaja rekurzivne poizvedbe. Strežnik izvaja tudi predpomnjenje zapisov o strežnikih DNS (ne pa tudi zapisov o drugih končnih sistemih), pri čemer ima pomnilnik omejen samo na pomnjenje podatkov o zadnjih dveh strežnikih DNS, katerih imena/naslove je pridobil. Vsak novi shranjeni podatek nadomesti starejšega (predpomnilnik torej deluje kot vrsta FIFO). Predpostavimo še, da predpomnjenja zapisov ne izvajamo tudi sami (lokalno) in da tako naš operacijski sistem kot tudi lokalni strežnik poznata naslove korenskih strežnikov (ti se ne hranijo v predpomnilniku).

a.) Zapiši, kako se spreminja vsebina predpomnilnika ob naslednjem zaporedju poizvedb, ki jih pošljemo lokalnemu strežniku, in koliko zapisov iz predpomnilnika lahko lokalni strežnik uporabi pri vsaki poizvedbi.

poizvedba	**vsebina predpomnilnika**	**število uporabljenih zapisov v predpomnilniku**
a.domena1.com		
b.domena1.org		
b.x.domena1.org		
b.domena1.com		

b.) Zamenjaj vrstni red zgornjih štirih poizvedb tako, da lahko lokalni strežnik uporabi čim več zapisov iz svojega predpomnilnika. Ponovno zapiši, kako se spreminja vsebina predpomnilnika in koliko predpomnjenih zapisov lahko lokalni strežnik uporabi pri vsaki poizvedbi.

poizvedba	**vsebina predpomnilnika**	**število uporabljenih zapisov v predpomnilniku**

c.) Na kratko (največ v 1 povedi) pojasni, kaj je to komercializacija domen in podaj dva primera.