RAČUNALNIŠKE KOMUNIKACIJE 2017/18

Ime in priimek: _____

1. izpit, 21. 6. 2018

Vpisna številka: _____

Literatura (prosojnice, knjige, zapiski, elektronski pripomočki) ni dovoljena.
Dovoljen je 1 A4 list s poljubno vsebino.
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	
5	
SKUPAJ	

1. NALOGA (20t):

V omrežju, ki je prikazano na desni, se uporablja usmerjevalni protokol iz iste družine protokolov, kot je protokol OSPF. Pri usmerjanju uporablja ceno, ki jo izračuna kot uteženo vsoto finančnega stroška in obremenitve povezave, pri čemer vsakega od teh kriterijev upošteva z utežjo 50%. Cene na povezavah so podane v obliki F/O, kjer F predstavlja finančni strošek najema povezave, O pa njeno obremenjenost. Vrednosti posredovalnih tabel ob nekem času so podane v spodnjih tabelah (podatek v prvem stolpcu predstavlja cilj, v drugem pa <cena poti>/<izhodna vrata-naslednji hop>).

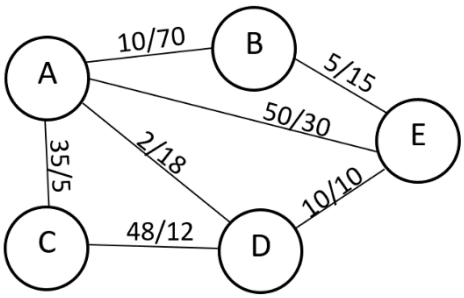
usm. A	
B	50/E
C	40/D
D	10/D
E	50/B

usm. B	
A	70/E
C	60/A
D	50/A
E	10/E

usm. C	
A	40/D
B	80/D
D	30/A
E	60/A

usm. D	
A	50/E
B	50/A
C	30/A
E	50/E

usm. E	
A	50/B
B	80/A
C	60/A
D	50/A



Izračunaj posredovalni tabeli usmerjevalnikov A in E v naslednji časovni enoti.

2. NALOGA (20t):

Konstruirati želimo novi protokol, ki deluje na predstavitveni plasti, in se imenuje *Compress*. Protokol mora ustrezati naslednjim zahtevam:

- Struktura datagrama se bo morda v prihodnosti kdaj spremenila z dodajanjem novih funkcionalnosti glede predstavitve podatkov. Zato mora datagram vsebovati polje, ki definira, kako brati strukturo datagrama. Polje naj bo poimenovano skladno s poimenovanjem tega polja pri ostalih protokolih, ki smo jih spoznali, in naj bo dolgo 3 bite.
- Uporabljamo lahko 5 različnih kompresijskih algoritmov, od katerih vsak uporablja tudi parameter, ki je dolg 8 bitov.
- Struktura datagrama naj odraža možnost, da se lahko v datagram *Compress* enkapsulirajo natanko 4 različni protokoli višje plasti (po modelu ISO/OSI). Polje ustrezno poimenuj (skladno kot je poimenovano pri drugih protokolih). Podaj šifrant za to polje, ki prikazuje primer pomena njegovih vrednosti glede na možen enkapsuliran protokol višje plasti (šifrant si izmisli, uporabi protokole, omenjene na predavanjih).
- Datagram naj uporablja CRC-16.

Naloge:

a) Skiciraj datagram protokola, ki ustreza zgornjim specifikacijam. Dolžine polj smiselno določi sam/a.

b) Če ne uporabljamo sejne plasti, ampak se zgornji datagram neposredno enkapsulira v protokol TCP in če velja MSS=1024 B, kolikšna je največja velikost enkapsuliranih podatkov v datagramu protokola *Compress*?

c) Denimo, da se znotraj enkapsulirane vsebine lahko pojavi poseben bajt (zaporedje 8 bitov), ki imajo za kompresijski algoritem poseben kontrolni pomen (podobno kot zastavici za začetek in konec okvirja pri PPP). Zato moramo uporabljati metodo vrivanja, kot ga uporabljamo pri protokolu PPP. Če je v enkapsulirani vsebini v povprečju 25% takšnih posebnih bajtov, kolikšna je v povprečju velikost (v bajtih) koristne enkapsulirane vsebine, ki jo lahko protokol *Compress* prenaša? Pri izračunu izhajaj iz odgovora na nalogo b).

3. NALOGA (20t):

Ana in Borut uporabljata varovanje komunkacije, ki je podobno protokolu SSL. Med rokovanjem določita glavni ključ (master key), ki ima vrednost 011111101011. Ključ razbijeta na 6 enako dolgih delov, ki določajo (v tem vrstnem redu): Anin tajni kjuč za zgoščanje, Branetov tajni ključ za zgoščanje, Anin enkripcijski ključ, Branetov enkripcijski ključ, Anin inicializacijski vektor in Branetov inicializacijski vektor. Ana želi v nadaljevanju Branetu poslati sporočilo 01010101, za kar bo uporabila bločno kriptografijo z verižnim kriptiranjem blokov.

Bločni kriptosistem obeh udeležencev deluje po funkciji $f(čistopis, ključ) = čistopis + ključ$ (pri čemer se prenos pri seštevanju prišteje k najnižjemu bitu). Zgoščanje oba izvajata samo z uporabo tajnega ključa tako, da seštejeta vse vhodne bite skupaj in po potrebi seštevanje večkrat ponovita do zgostitve v 1 sam bit.

Naloga: Zapiši zaporedje kriptogramov in pripadajočih zgoščenih vrednosti, ki jih Ana pošlje Branetu.

4. NALOGA (20t):

Brane uporablja lokalni DNS strežnik, ki uporablja predpomnjenje zapisov.

a) Koliko iterativnih in rekurzivnih poizvedb se bo izvedlo, če bo Brane izvedel naslednje poizvedbe (v tem vrstnem redu): pop.mail.yahoo.com, smtp.mail.yahoo.com, www.uni-lj.si, www.yahoo.com, www.fri.uni-lj.si. Predpostavi, da Brane ne uporablja lastnega predpomnjenja in da imajo zapisi na strežniku dovolj velik TTL, da se ohranijo med časom vseh petih poizvedb. Upoštevaj tudi, da Brane in medstrežnik poznata naslove korenskih strežnikov.

b) Kako se število zgornjih iterativnih in rekurzivnih poizvedb spremeni, če si lahko strežnik v medpomnilniku zapomni največ štiri najbolj sveže zapise (po principu vrste FIFO)?

c) Ali bi se število poizvedb lahko spremenilo, če bi Brane izvedel poizvedbe v drugačnem vrstnem redu? Če da, podaj primer takšnega vrstnega reda in število poizvedb pri njem.

5. NALOGA (20t):

S programom Wireshark smo zajeli spodnja dva paketa, levo paket a in desno paket b:

Ethernet II
  Destination: 6c:62:6d:60:00:a8
  Source: 00:12:43:3b:23:ff
  Type: IPv6 (0x86dd)
Internet Protocol Version 6
  Version: 6
  Traffic class: 0x000000e0
  Flowlabel: 0x00000000
  Payload length: 32
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source: 2001:1470:fffd::1
  Destination: 2001:1470:fffd::155
Internet Control Message Protocol v6
  Type: 136 (Neighbor advertisement)
  Code: 0
  Checksum: 0x8fb2 [correct]
  Flags: 0xe0000000
  Target: 2001:1470:fffd::1
ICMPv6 Option (Target link-layer address)
  Type: Target link-layer address (2)
  Length: 8
  Link-layer address: 00:12:43:3b:23:ff
	Ethernet II
	  Destination: 33:33:ff:00:00:01
	  Source: 6c:62:6d:60:00:a8
	  Type: IPv6 (0x86dd)
	Internet Protocol Version 6
	  Version: 6
	  Traffic class: 0x00000000
	  Flowlabel: 0x00000000
	  Payload length: 32
	  Next header: ICMPv6 (0x3a)
	  Hop limit: 255
	  Source: 2001:1470:fffd::155
	  Destination: ff02::1:ff00:1
	Internet Control Message Protocol v6
	  Type: 135 (Neighbor solicitation)
	  Code: 0
	  Checksum: 0x34ff [correct]
	  Reserved: 0 (Should always be zero)
	  Target: 2001:1470:fffd::1
	ICMPv6 Option (Source link-layer address)
	  Type: Source link-layer address (1)
	  Length: 8
	  Link-layer address: 6c:62:6d:60:00:a8

1. Napiši vse protokole, ki so del paketov, in za vsakega povej, na katero plast je umeščen.

2. Kakšen tip sporočila je v paketu a in kakšen tip sporočila je v paketu b (za protokol, ki je najbližje aplikacijski plasti)? Kateri paket je zahteva, kateri pa odgovor? Za kaj se ta protokol uporablja?

3. Koliko usmerjevalnikov je med računalnikoma, ki sta poslala ta dva paketa? Razloži, kako si prišel do odgovora.

4. Kaj veš o ponornem omrežnem naslovu paketa b? Zakaj se uporablja, kako se tvori?

5. Kaj veš o ponornem naslovu povezavne plasti paketa b? Zakaj se uporablja, kako se tvori?

6. Kakšen bi bil ponorni naslov povezavne plasti, če bi uporabljali IPv4? Zakaj?

7. Kako je z varnostjo protokola, ki je v teh dveh paketih najglobje enkapsuliran? Opiši v največ dveh stavkih vsaj en napad na ta protokol.