

# RKVB

Ime: \_\_\_\_\_

Priimek: \_\_\_\_\_

Vpisna številka: \_\_\_\_\_

*Pozorno preberite navodila! Literatura **ni** dovoljena. Odgovarjajte kratko (z eno, največ dvema povedima)! Čas pisanja je **60** minut. Naloge so enakovredne, razen če ni označeno drugače!*

1. (15%) Analogni signal s frekvenčnim obsegom od 500 do 2500 Hz želimo digitalizirati. Po Nyquistu ga vzorčimo z dvakratnikom najvišje frekvence signala.

- a) Koliko vzorcev na sekundo vzamemo?
- b) Če vsak vzorec opišemo s 4-bitno vrednostjo: najmanj kako hiter pretok podatkov potrebujemo, da bomo lahko prenesli vse vrednosti?
- c) Koliko podatkov predstavlja 5 minut posnetka?
- d) Koliko časa bi potrebovali, da teh 5 minut posnetka prenesemo po povezavi s hitrostjo 1 Gb/s? Predpostavite, da ni nič režije.
- e) Na kateri plasti po modelu ISO/OSI se dogaja vzorčenje signala?

2. (20%) Na stikalo so na vmesnike 1 do 4 priključene naprave s strojnimi naslovi A, B, C in D.

- a) A odda okvir z naslovom cilja B. Tabela stikala je prazna. Kaj se zgodi z okvirjem na stikalu?
- b) Kaj pa se zgodi z vsebino tabele?
- c) Kaj bi moralo pisati v tabeli na stikalu, če bi želeli, da okvir iz vprašanja a) zagotovo pride samo na napravo B?
- d) Predpostavimo, da je zapis iz vašega odgovora na vprašanje b) zdaj že v tabeli. Nato D odda okvir z naslovom cilja B. Kaj se zgodi z okvirjem na stikalu?
- e) Kaj pa se zgodi z vsebino tabele?
- f) Kaj pa če bi D namesto tega oddal okvir z naslovom cilja A. Kaj se zgodi z okvirjem na stikalu?
- g) Kaj pa če D odda okvir z naslovom cilja FF:FF:FF:FF:FF:FF. Kaj se bo zgodilo na stikalu in zakaj?

3. (15%) Kdaj in zakaj se zgodi IP fragmentacija? Kaj se sploh zgodi? Pojasnite prednosti in slabosti fragmentacije. Kakšna pa je fragmentacija v IPv6?

4. (15%) Zakaj govorimo, da TCP v povprečju ne porabi več kot 75% razpoložljive hitrosti prenosa? Pojasnite mehanizem, ki stoji za to trditvijo.

5. (15%) Kako bi kriptirali naslednji niz dveh 8-bitnih blokov: 1001 1100 1001 1100

- a) Če se uporablja metoda enkratnega ključa, ki generira naslednje zaporedje: 011001110001111?
- b) Če se uporablja preprost kriptografski mehanizem, ki zamenja ničle z enicami in enice z ničlami?
- c) Če se uporablja zgornji kriptografski mehanizem (iz točke b) s CBC in se tako prvi od zgornjih dveh blokov zakriptira v »1101 0110«?
- d) Ali naslednja števila ustrezajo pogojem za kriptografijo RSA? Odgovor utemeljite.  
 $n = 221$ ,  $z = 162$ ,  $d = 133$ ,  $e = 144$ .

6. (12%) S programom Wireshark smo zajeli spodnja dva paketa (v naključnem vrstnem redu):

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

- V kateri protokol, ki je najbližje aplikacijski plasti, sodita prikazana paketa?
- Kateri je vprašanje, kateri je odgovor?
- Napišite pošiljateljev naslov IP in prejemnikov strojni naslov.
- Kako imenujemo omrežni naslov (tip naslova) na katerega je bila poslana zahteva?
- Če bi bila smer komunikacije obrnjena (torej tokrat prejemnik začne pošiljati prvo sporočilo omenjenega protokola), kakšna bi bil v tem primeru omrežni naslov iz točke d?
- Kaj se zgodi, če na povpraševanje ne dobimo odgovora?

7. (8%) IPv6 naslov je **2001:1470:ffff:fe01:b85c:865b:de86:e7de/48**. Izračunajte:

- Največji naslov naprave v tem podomrežju.
- Najmanjši naslov naprave v tem podomrežju.
- Število naprav, ki jih lahko priključimo v to podomrežje
- Kakšnega tipa je IPv6 naslov fe80::1610:9fff:fee9:c268?