

# RAČUNALNIŠKE KOMUNIKACIJE

## pisni izpit 24.9.1999

**1. Naloga:** Namen imamo poslati sejni ključ za vzpostavitev varnega komuniciranja. Odločili smo se uporabiti algoritem RSA. Izberite ustrezni praštevili ter določite vaš javni in privatni ključ. Simulirajte prenos in posamezne korake opišite. Sejni ključ je 9,5,6,21,41. Javni ključ našega partnerja je (5,119). Partner mora biti prepričan, da ste ključ poslali vi.

**2. Naloga:** Podano imamo omrežje z vozlišči A, B, C, D, ki so povezana v obroč (v navedenem zaporedju); povezave so tipa 'fullduplex' kapacitete 30000bitov/sek. Znana je matrika končnega prometa. Povprečna velikost paketa je 130 bitov. Razdalje med vozlišči so  $|AB|$  je 6 enote,  $|BC|$  3 enote in  $|CD|$  je 1 enota in  $|AD|$  2 enoti. Poiščite usmerjevalno tabelo, če je uporabljeno usmerjanje po najkrajši poti (v primeru, da sta poti enako dolgi vzamemo tisto z manj skoki)

*36 107 21*

	A	B	C	D
A		4	3	3
B	4		2	4
C	3	2		1
D	3	4	1	

**Izračunajte:**

- Kakšna je povprečna zakasnitev v omrežju in kolikšen je odziv praznega omrežja?
- Koliko povprečno porabi paket iz C v D?
- Kolikšno je povprečno število skokov?
- Kakšen je faktor  $K_{max}$  za to omrežje?

**3. Naloga:** Prenašamo zaporedje petih podatkovnih paketov z uporabo tekočega pošiljanja z neposrednim potrjevanjem, kjer se uporablja ponavljanje sekvence in potrjevanje bloka. Pri prenosu se izgubita prvi paket in četrta potrditev. S pomočjo tekočega posrednega selektivnega potrjevanja. Pri prenosu se izgubita 2. in 4. paket ter 3. potrditev. Simulirajte na časovni osi zaporedje dogodkov in sproti pojasnajte.

**4. Naloga:** Proces komunicirata med seboj s pomočjo sporočil a, b, c ter p, ki pomeni potrditev. Ob prihodu poročil prehaja v stanja A, B, C. Graf prehajanja stanj je podan. Konstruirajte drugi avtomat, če velja:

- z oddajo sporočila x (a,c,b) preide proces v stanje X (A,B,C),
- če je v stanju A lahko odda le znak b, v stanju B lahko odda le c, v stanju C pa lahko odda le a
- če prejme p, se vrne v začetno stanje.

Narišite drevo globalnih stanj, pri čemer ima prvi proces večjo prioriteto. Dolžina vrste je 1. Označite stabilna stanja in akcije med prehodi stanj. Ali je v avtomatih mrtva koda?

