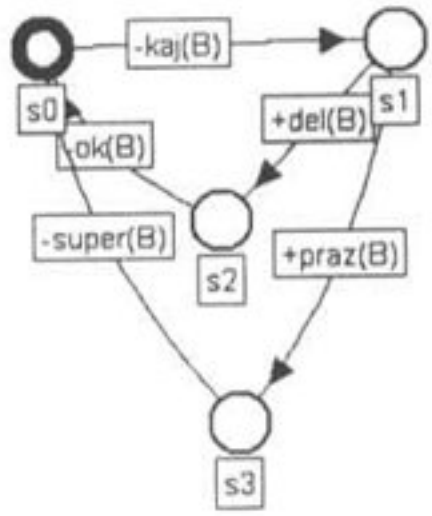
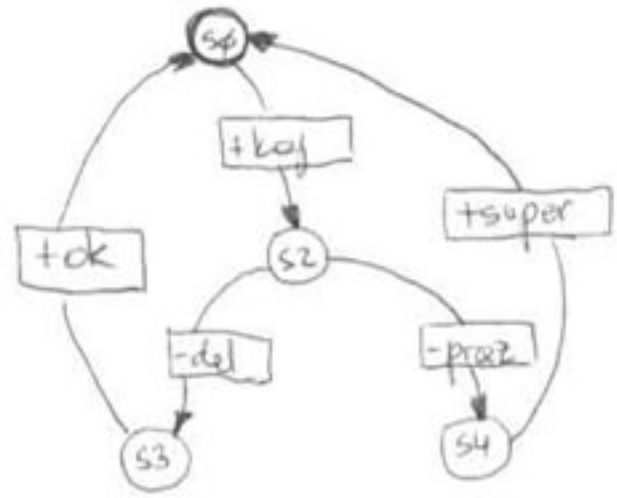
RAČUNALNIŠKE KOMUNIKACIJE
pisni izpit 2. 9. 2002

1. Podan je končni avtomat, ki prikazuje enega od komunikacijskih procesov. Proces A včasih vpraša proces B, kaj je danes. Če B odgovori "delavnik", A potrdi z OK, če pa B odgovori, da je praznik, A odgovori SUPER. Kanal med procesoma je dvosmeren, dolžina vrste je 2. Oba procesa sta enako visoka po hierarhiji, prioriteta sprejema in oddaje sta enaki. Narišite avtomat procesa B in analizirajte protokol. Če najdete napake, razložite, zakaj pride do njih.





2. Analiziramo omrežje s 5 vozlišči, kjer imamo popolnoma dvosmerne povezave AC, BC, CD in CE. Povezava CE ima kapaciteto 100 MB/s, ostale pa 10 MB/s. Povprečen paket je velik 1kbit. (Za lažje računanje vzemite 1k = 1000). Prometna matrika je podana. Ugotovite, kakšno je usmerjanje po najkrajši poti in poiščite povprečno zakasnitev, povprečno število skokov in Kmax.

	A	B	C	D	E
A	-	1000		100	500
B	1000	-		800	2000
C			-		
D	100	800		-	1000
E	500	2000		1000	-

$T_1 = 1.74$

$K_{max} = 2.94$

$\bar{T} = 77\mu s$

3. Peter bi rad Ančki pošiljal pismo, ki jih njen oče ne bi znal prebrati. Odločil se je za kriptografijo MIT-RSA, prilagojeno svojim računskim sposobnostim seveda. Za p in q je izbral 7 in 3.
   a. Pomagajte Petru poiskati števili, različni od (5,5) in (5,17), ki ustrezata pogojem za e in d.
   b. Ančka želi sporočiti Petru, naj pride k njej ob 10h. S pomočjo para (d, e) = (5,5) ji pomagajte kriptirati sporočilo "10". (Število 10 vzemite kar kot blok, ki ga kriptiramo).
   c. Kriptirajte isti niz še s pomočjo para (d, e) = (5,17).

4. Razložite razliko med posrednim in neposrednim tekočim potrjevanjem na primeru pošiljanja sekvence treh paketov, kjer se prvi paket popači, zadnji pa izgubi.