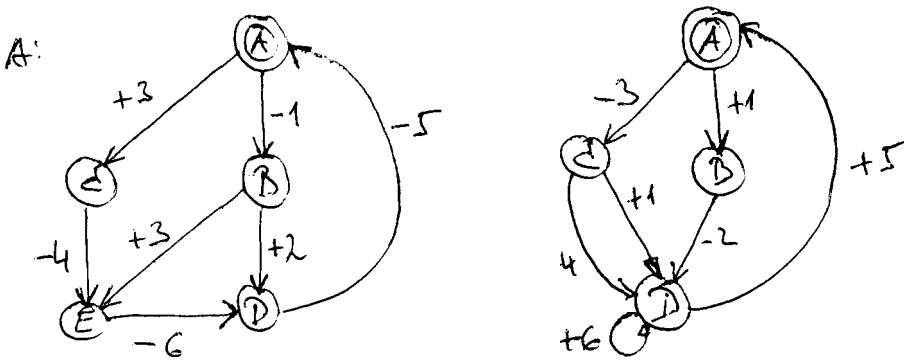
PISNI IZPIT RKO, RK 9.6.2000

1. Naloga: Na Ethernet vodilo imamo priključene štiri delovne postaje. Verjetnost dostopa do vodila v danem časovnem intervalu za posamezno postajo je po vrsti 0.2, 0.3, 0.4, 0.5. Koliko časa v povprečju je vodilo prazno? Koliko časaje vodilo v posameznem časovnem intervalu zaradi trkov neuporabno?

2.Naloga: a.) Odločimo se, da bomo pismo prijatelju podpisali z elektronskim podpisom s pomočjo algoritma MIT-RSA. Pri tem je naš javni ključ (7,33) in privatni (3,33). Prejemnik nam je dobrohotno sporočil javni (5,51) in privatni (13,51) ključ. Kot osnovo za podpis uporabimo geslo **KUNDERA** (12 ,22 ,15 ,5 ,6 ,18 ,1). Simulirajte postopek podpisovanja na zgornjem geslu in izračunajte elektronski podpis!

b.) S pomočjo prisluškovanja nam je uspelo odkriti fragmente iz kriptografskega sistema MIT-RSA in sicer smo izvedeli: n = 84773093 in z = 84754668. Ali nam ta informacija omogoča globji vpogled v vrednosti javnega oz. privatnega ključa uporabnika., odgovor utemeljite!

3. Naloga: Za protokol definirajte popolno drevo globalnih stanj. Ce je potrebno spremenite robne pogoje in protokol, da bo deloval brez napak.



4.Naloga: Podano imamo omrežje z vozlišči A, B, C, D, ki so povezana v obroč (v navedenem zaporedju); povezave so tipa 'fullduplex' kapacitete 14400 bitov/sek. Znanaje matrika končnega prometa. Povprečna velikost paketaje 128 bitov. Razdalje med vozlišči so |AB| je 6 enote, |BC| 3 enote, |CD| je 1 enota in |AD| 2 enoti. Poiščite usmerjevalno tabelo, čeje uporabljeno usmerjanje po najkrajši poti (v primeru, da sta poti enako dolgi vzamemo tisto z manj skoki)

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

Izračunajte: a.) Kaksna je povprečna zakasnitev v omrežju in kolikšen je odziv praznega omrežja?

b.) Kolikšnoje povprečno število skokov?

c.) Kakšen je faktor Kmax za to omrežje?