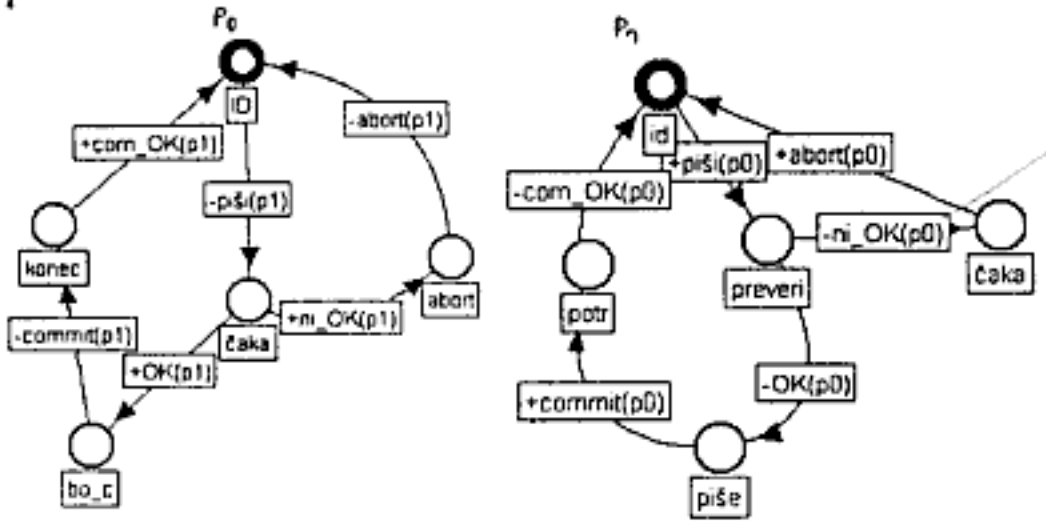
KOMUNICIRANJE V PORAZDELJENIH SISTEMIH
RAČUNALNIŠKE KOMUNIKACIJE

pisni izpit 20. 4. 2001

1) Od vozlišča A do B imamo tri enosmerne povezave. Prva in druga imata kapaciteto 10^6 bit/s, tretja pa $5*10^5$ bit/s. Po prvi pošljemo 400 paketov/s, po drugi 450 paketov, po tretji pa 250 paketov. Paket je velik 1000 bitov.
   a) Izračunajte povprečno zakasnitev paketa v takem omrežju.
   b) Denimo, da so povezave izmenično dvosmerne in imajo enako kapaciteto kot zgoraj. Posebno stikalo zagotavlja, da promet poteka v vsako smer enako število časovnih intervalov. Kakšna je v tem primeru povprečna zakasnitev?

   Kakšna pa je zakasnitev, če gre za popolnoma dvosmerne povezave, kjer je kapaciteta v vsako smer enaka zgoraj navedeni?

2) Analizirajte protokol pri dolžini vrste 1. Ali je kaka bistvena razlika, če vrsto povečamo na 2?



3) MIT-RSA:
   a. Ali števili d = 21 in e = 221 ustrezata pravilom za enkripcijski in dekripcijski ključ pri izbiri 11 in 17 za p in q?
   b. Ali menite, da bi bila glede na velik n dolžina bloka 4 bolj smiselna kot dolžina bloka 2?
   c. Kriptirajte niz 017, če uporabljamo dložino bloka 3 mesta.

4) Za kakšno potrjevanje gre? Naštejte vse lastnosti, ki jih opazite.