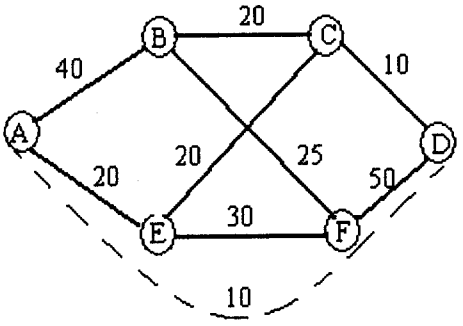
RAČUNALNIŠKE KOMUNIKACIJE

pisni izpit 24.6.1999

1. Naloga: Odločimo se za uporabo uporabo kriptografskega sistema z javnim ključem RSA. Izbrali smo si praštevili 3 in 17. Tvorite parametre javnega in privatnega ključa (za lažje nadaljevanje si izberite ustrezno majhne vrednosti) ter zakodirajte z dobljenim javnim ključem geslo DENAR(5,6,15,1,18).

2. Naloga: Podanemu omrežju želimo izboljšati parametre (povprečni odzivni čas omrežja **T**, odzivni čas prazne mreže $\mathbf{T_o}$, povprečno št. skokov na eno povezavo točka-točka **n**, točko zasičenja **k**). Ali je izboljšava naznačena z črtkano črto in sprememba usmerjanja iz ABFD v AD uspešna? Dolžina paketa je 1kbit/s, kapacitete so podane v kbit/s. Matrika je simetrična. Svoj odgovor utemeljite!



	A	B	C	D	E	F
A		12 AB	3 ABC	5 ABFD	10 AE	2 AEF
B			7 BC	2 BFD	1 BFE	1 BF
C				3 CD	2 CE	5 CEF
D					3 DCE	3 DF
E						2 EF
F						

3. Naloga: Sekvenco petih podatkovnih paketov prenašamo med oddajnikom in sprejemnikom z uporabo tekočega posrednega potrjevanja: Pri prenosu se izgubi 2. potrditev in 3. paket, 4. potrditev pride na cilj popačena. Simulirajte na časovni osi zaporedje dogodkov in sproti pojasnjujte.

4. Naloga: Ugotovite lastnosti podanega protokola. Ali obstaja kombinacija robnih pogojev, ko protokol deluje brez napak? Odgovor utemeljite!