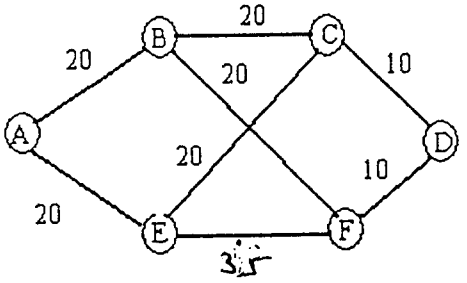
RAČUNALNIŠKE KOMUNIKACIJE

pisni izpit 18.6.1999

1. 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!

2. Naloga: Podano je omrežje, kapacitete povezav med vozlišči, prometna matrika ter usmerjanje paketov po omrežju. Povprečna velikost paketa je 800 bitov, kapacitete so podane v kbit/sek in so v obe smeri enake. Izračunajte povprečni odzivni čas omrežja T, odzivni čas prazne mreže T_o, povprečno št. skokov na eno povezavo točka-točka n, točko zasičenja k. Ponovite izračun po spremembi usmerjanja ABFD ABCD. Kaj opazite?



	A	B	C	D	E	F
A		9 AB	4 ABC	4 ABFD	7 AE	4 AEF
B			8 BC	3 BFD	2 BFE	4 BF
C				3 CD	3 CE	2 CEF
D					3 DCE	4 DF
E						5 EF
F						

3. Naloga: Sekvenco petih podatkovnih paketov prenašamo med oddajnikom in sprejemnikom z uporabo posrednega sprotnega potrjevanja in tekočega posrednega selektivnega potrjevanja. Pri prenosu se izgubita 2. in 4. paket ter 3. potrditev(slednje le za prvi primer). Simulirajte na časovni osi zaporedje dogodkov in sproti pojasnjujte.

4. Naloga: Ugotovite pravilnost/ nepravilnost delovanja sledečega protokola. Če najdete napake jih popravite oz. podajte predlog izboljšave, da bo protokol deloval brez napak. Naredite analizo za primer ko čakalna vrsta lahko sprejme enega oz. dva paketa, kanal je dvosmeren.