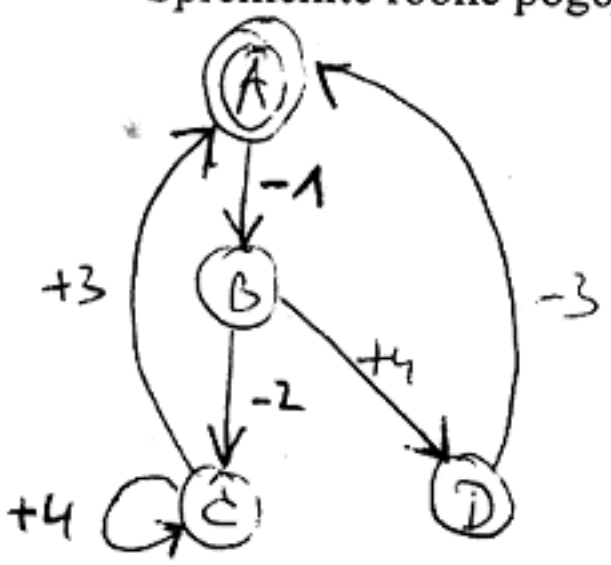
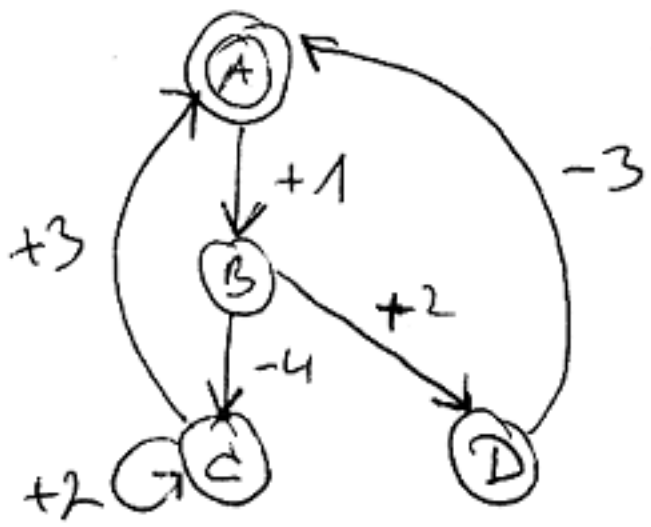
PISNI IZPIT RK, RKO 22.6.2000

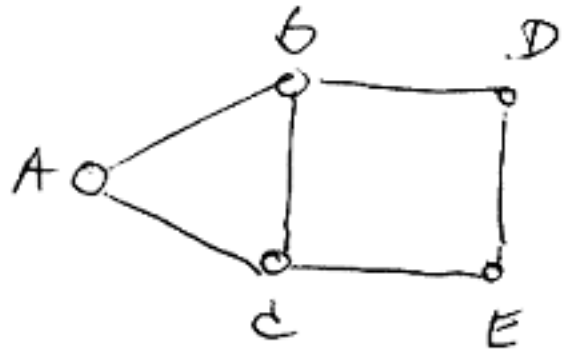
1. naloga: Namen imamo poslati sejni ključ za vzpostavitev varnega komuniciraja. Odločili smo se uporabiti algoritme RSA. Izberite ustrezni praštevili (večji od 3) ter določite javni in privatni ključ. Simulirajte prenos in posamezne korake opišite. Sejni ključ je 13, 5, 25, 41. Javni ključ partnerja je (5,119).

2. naloga: Ugotovite pravilnost sledečega protokola. Rezultate komentirajte! Spremenite robne pogoje in sam protokol, da bo deloval brez napak.

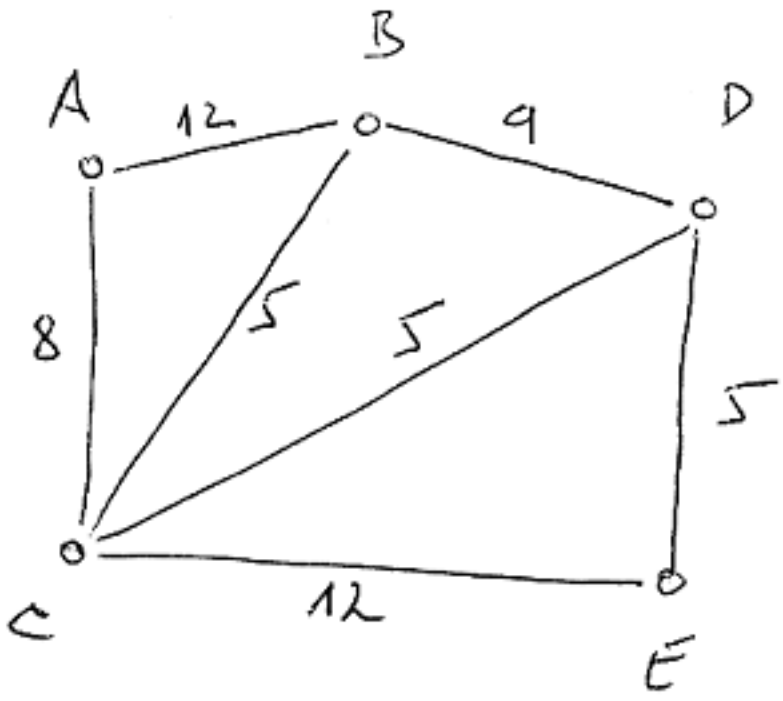




3. naloga: V omrežju na sliki uporabljamo porazdeljeno usmerjanje. Metrika zakasnitve je število skokov. Vozliče A je v začetku nedelujoče. Nato se priklopi v omrežje in deluje določeno število taktov, nakar ponovno odpove. Simulirajte izmenjavo in izračun usmerjevalnih tabel! Koliko taktov je potrebno, da se informacija o odpovedih usmerjevalnikov razširi preko celotno omrežje (glede na posamezen tip omrežja)?



4. naloga: Za podano omrežje izračunajte T, To, Kmax, n. Povezave so fullduplex. Povprečna velikost paketa je 1024 bitov. Kapacitete so v tisočih.



	A	B	C	D	E
A	-	3 AB	2 AC	6 ABD	4 ACE
B	3 BA	-	4 BC	2 BD	1 BDE
C	2 CA	4 CB	-	2 CD	4 CE
D	2 DCA	2 DB	2 DC	-	1 DE
E	4 ECA	2 ECB	4 EDC	1 ED	-