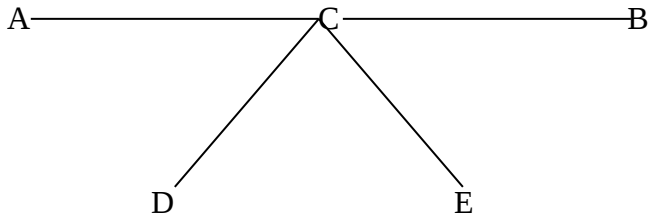
2.naloga pisni izpit 2.9.2002

Usmerjanje:

	A	B	C	D	E
A	-	ACB (1000)	AC	ACD (100)	ACE (500)
B	BCA (1000)	-	BC	BCD (800)	BCE (2000)
C	CA	CB	-	CD	CE
D	DCA (100)	DCB (800)	DCA	-	DCE (1000)
E	ECA (500)	ECB (2000)	EC	ECD	-



	λ_i	C_i [bit/s]	μC_i [bit/s]	$T_i=(1/\mu C_i * \lambda_i)$ [s]	$(\lambda_i * T_i)$	$k_i=(\mu C_i/\lambda_i)$
AC	1600	80 000 000	80 000	0,000012755	0,02041	50
BC	3800	80 000 000	80 000	0,000013123	0,04987	21,05
CD	1900	80 000 000	80 000	0,000012804	0,02433	42,1
CE	3500	800 000 000	800 000	0,000001255	0,00439	228,57
	Σ10800				Σ 0,099	

γ =5 400

Povprečna zakasnitev: $T=(1/\gamma) * \Sigma (\lambda_i * T_i)$
T=(1/5400) * 0,099 = 0,0000183 [s] ; ker je matrika simetrična je potrebno pomnožiti z 2. 0,0000367 [s] = **<u>0,0367 [ms]</u>**

Povprečno število skokov: $\overline{n} = (\lambda/\gamma) = (10\ 800 / 5400) =$ **<u>2 skoka</u>**

<u>K_{max} = 21,05</u>

3.naloga pisni izpit 2.9.2002

p = 7 , q = 3
a.) n = p * q = 7 * 3 = 21 z = (p-1) * (q-1) = 6 * 2 = 12
d = 7 (nesme imeti nobene skupne lastnosti z z-jem)
e*d mod z = 1 e * 7 mod 12 =1 => **e = 19**

b.) (d,e) = (5, 5) => 5 * 5 mod z = 1 25 mod z = 1 => z = 24
z = (p-1) * (q-1) => 24 = 6 * 4; p-1=6 => **p=5**; q-1=4 => **q=3** (p in q sta praštevili)
n=p*q=3*5=15
e=5; n=15
kriptiranje: **10^5 mod 15= 10**

dekriptiranje (za preverjanje): 10^5 mod 15 = 10

c.) (d,e) = (5, 17) => 5 * 17 mod z = 1 85 mod z = 1 => z = 84
z = (p-1) * (q-1) => 84 = 6 * 14; p-1=6 => **p=5**; q-1=14 => **q=13** (p in q sta praštevili)
n=p*q=13*5=65
e=17; n=65
kriptiranje: **10^{17} mod 65 = (10^9 * 10^8) mod 65= (25 * 35) mod 65 = 30**

dekriptiranje (za preverjanje): 30^5 mod 65 = 10