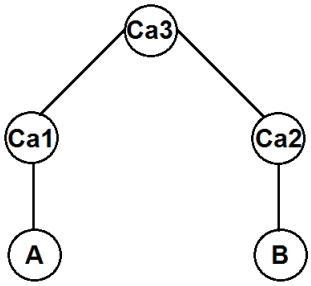
Ispit iz Zaštite podataka (SI4ZP, IR4ZP, 13E113ZP, 13S114ZP) 12.06.2016.

1. (**10p**) Objasnite kako jedan učesnik u komunikaciji (A) koji ima sertifikat izdat od jednog sertifikacionog autoriteta (Ca1) dobija pouzdan javni ključ drugog učesnika u komunikaciji (B), kada je drugi učesnik u komunikaciji (B) dobio sertifikat od drugog sertifikacionog autoriteta (Ca2), korišćenjem hijerarhije sertifikacionih autoriteta za primer sa slike 1.



Slika 1. Primer hijerarhije sertifikacionih autoriteta

2. (**10p**) Nacrtati i objasniti postupak prilikom generisanja i prilikom prijema *PGP* poruke uz ostvarivanje tajnosti i autentikacije i uz korišćenje prstenova ključeva. Zanemariti kompresiju i konverziju.

3. (**10p**) Skicirati i objasniti direktni i reflektovani DDoS napad.

Napomena: *Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Ispit traje 120 minuta.*