Drugi kolokvijum iz Zaštite podataka (SI4ZP, IR4ZP) *09.05.2015.*

1. *Three Way* autentikacija kod *X.509* autentikacionog servisa. Razlozi za postojanje i poređenje sa jednostavnijim *X.509* autentikacionim servisima.
2. Kod *Diffie-Hellman* algoritma objasniti po kom pravilu se biraju globalni javni elementi, a zatim za dva učesnika u komunikaciji objasniti na koji način svaki od njih formira par ključeva i kako dobijaju zajedničku tajnu vrednost. Dokazati da učesnici u komunikaciji dobijaju istu vrednost iako koriste različite proračune da do nje dođu.
3. 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.

Napomene: Na kolokvijumu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Kolokvijum traje 90 minuta.