Drugi kolokvijum iz Zaštite podataka (SI4ZP, IR4ZP) *05.05.2012.*

1. Navedite poruke u *Kerberos* verziji 4. Pokušajte da objasnite zašto je potrebno da postoji puno *timestamp*-ova (5) i *lifetime*-a (2)?
2. Objasniti *RSA* algoritam za šifrovanje pomoću javnog ključa. Opisati način formiranja privatnog i javnog ključa, kao i postupak prilikom šifrovanja, odnosno dešifrovanja ovim algoritmom. Šifrovati poruku M=3, koristeći javni ključ PU={17, 77}. Za izračunavanje šifrovane vrednosti koristiti algoritam za brzu eksponentizaciju.
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.