Drugi kolokvijum iz Zaštite podataka (SI4ZP, IR4ZP, MS1ZP) 20.04.2011.

1. (**10 p**) Objasnite kako se u komunikaciji između *Kerberos realm*-ova obezbeđuje pristup klijenta iz jednog *realm*-a servisu iz drugog *realm*-a. Navedite svaki korak u autentikaciji i autorizaciji. Ako je u toku rada potrebno prići servisu iz nekog trećeg *realm*-a, da li je potrebno ponovo se ulogovati?

2. (**10 p**) Objasniti *RSA* algoritam za šifrovanje pomoću javnog ključa. Opisati način formiranja privatnog i javnog ključa, kao i postupak prilikom šifrovanja, odnosno dešifrovanja ovim algoritmom. Koji uslovi moraju biti ispunjeni da bi *RSA* algoritam zadovoljio uslove šifrovanja pomoću javnog ključa?

3. (**10 p**) Koje funkcije se koriste u S/MIME za obezbeđivanje tajnosti, autentikacije (razmatrati obe varijante autentikacije) i tajnosti i autentikacije? Objasniti na koji način se vrši osiguravanje MIME entiteta u slučaju da želimo da postignemo tajnost. Objasniti na koji način se vrši osiguravanje MIME entiteta u slučaju da želimo da postignemo autentikaciju (razmatrati obe varijante autentikacije).

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