Drugi kolokvijum iz Zaštite podataka (SI4ZP, IR4ZP) *27.04.2013.*

1. 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. Objasniti čemu služi i kako se koristi *Diffie-Hellman* algoritam. Napisati dokaz da algoritam funkcioniše. Dati konkretan predlog na koji način se može sprečiti *man-in-the-middle* napad na *Diffie-Hellman* protokol (poželjno koristiti postojeće elemente iz *Diffie-Hellman* algoritma koliko god je moguće)?
3. Koji su koraci za pripremu obmotanih podataka, a koji za pripremu potpisanih podataka kod S/MIME zaštite elektronske pošte? Šta sadrže i čemu služe blokovi informacije o primaocu (RecepientInfo) i informacije o potpisivaču (SignerInfo)?

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