Ispit iz zaštite podataka (SI4ZP, IR4ZP) 13.09.2015.

1. (**20p**) Koja je suštinska razlika između *Vernamove* šifre i *One time pad* šifre primenjene na binarne podatke. Ako je na dve poruke iste dužine primenjen isti ključ kod *One time pad* algoritma i dođe se do originalnog teksta jedne od te dve poruke, da li je moguće otkriti drugu poruku i kako?

2. (**20p**) Objasnite uloge autentikacionog i *ticket granting* servera u *Kerberos* sistemu. Kako se postiže da lozinka ne putuje kroz mrežu? Kako se postiže jedinstvenost lozinke za sve servise pomoću *Kerberos*-a?

3. (**20p**) 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)?

4. (**25p**) Nacrtati i objasniti postupak prilikom generisanja i prilikom prijema PGP (*Pretty Good Privacy*) poruke uz ostvarivanje tajnosti i autentikacije i uz korišćenje prstenova ključeva. Zanemariti kompresiju i konverziju. Koja je uloga prstenova ključeva kod PGP protokola? Koji mehanizam se koristi za upravljanje ključevima kod PGP protokola i na koji način se koriste prstenovi ključeva, kao podrška za taj mehanizam? Kako se izračunava legitimitet ključa?

Trajanje ispita 3 sata