

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. (20p) Nacrtati i objasniti postupak prilikom generisanja i prilikom prijema PGP (*Pretty Good Privacy*) poruke uz ostvarivanje tajnosti i autentikacije i uz korišćenje prstenova ključeva. Zanimariti kompresiju i konverziju.
5. (20p) Prikazati strukturu virusa koristeći pseudokod. Koje su to faze kroz koje tipičan virus prolazi i šta se dešava u svakoj od faza?

Trajanje ispita 3 sata