Ispit iz Zaštite podataka (13E113ZP, 13S114ZP) 26.01.2020.

1. (**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?
2. (**15p**) Skicirati strukturu *PKI* i objasniti osnovne elemente. Šta se sve mora uraditi ako je kompromitovan privatni ključ izdavaoca *X.509* sertifikata, da bi se ponovo uspostavio sistem sigurnosti zasnovan na *X.509*?
3. (**15p**) Opisati dva načina zaštite fajlova sa šiframa – zaštita jednostranim (*one-way*) funkcijama i zaštita kontrolom pristupa. Navesti mane zaštite kontrolom pristupa.
4. (**15p**) Data je poruka PER ANGUSTA AD AUGUSTA.
   a. Šifrovati datu poruku *Playfair* algoritmom. Za šifrovanje izabrati ključ DISLEKSIJA.
   b. Šifrovati datu poruku *Rail Fence* algoritmom u tri reda.

   Poruka se sastoji isključivo od slova engleskog alfabeta. Uzeti da se I i J mapiraju kao jedno slovo. Prikazati postupke šifrovanja.

Napomena: *Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Ispit traje 150 minuta.*