Ispit iz Zaštite podataka (MS1ZP) 12.06.2012.

1. (K)(**10p**) Objasnite *one-time pad* šifru i njene osobine. Za neku proizvoljnu kriptovanu poruku dužine 67 slova i blanko znakova, da li je moguće naći ključ kojim će se prilikom dekripcije dobiti poruka: "Svi studenti koji slusaju zastitu smatraju da je ispit suvise tezak"? Obrazložite odgovor.

2. (K)(**10p**) Šta su *replay* napadi i kako izbegavamo te napade? Navedite elementarni primer lažnog predstavljanja korišćenjem *replay* napada.

3. (K)(**10p**) Nacrtati strukturnu šemu *DES* algoritma i objasniti način funkcionisanja algoritma prilikom šifrovanja. Detaljno objasniti kako izgleda jedna iteracija i kako se od ključa prave ključevi iteracije.

4. (K)(**10p**) Objasniti razliku između šifrovanja na linku i šifrovanja sa kraja na kraj prilikom zaštite poverljivosti korišćenjem simetričnih algoritama. Koji od ova dva načina šifrovanja ostaje ranjiv za analizu saobraćaja i zbog čega?

5. (K)(**10p**) Objasniti *RSA* algoritam za šifrovanje pomoću javnog ključa. Opisati način formiranja privatnog i javnog ključa, kao i postupak prilikom šifrovanja, odnosno dešifrovanja ovim algoritmom. Dešifrovati šifrovanu poruku C=3, koristeći privatni ključ PR={17, 77}. Za izračunavanje originalne vrednosti koristiti algoritam za brzu eksponentizaciju.

---

1. (I)(**10p**) Nacrtajte blok dijagram koji prikazuje osnovne entitete *PKI* (*public-key infrastructure*) i njihove međusobne komunikacije, sa vrlo kratkim opisom sadržaja tipičnih poruka koje se razmenjuju. Koji su tipični zahtevi korisnika prema sertifikacionom autoritetu *PKI* (*public-key infrastructure*).

2. (I)(**10p**) Koje se sve poruke i kojim redosledom razmenjuju između klijenta i servera kod uspostavljanja *SSL* sesije (*SSL Handshake*). Pretpostavite da je potrebna samo autentikacija servera, a ne i klijenta.

3. (I)(**10p**) 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).

4. (I)(**10p**) Koje tri klase uljeza postoje? Opisati kratko svaku od njih. Za svaku klasu uljeza navesti koji pristup detekcije upada može detektovati upade iz te klase i objasniti zašto.

5. (I)(**10p**) Objasniti na koji način su virusi uspevali da ostanu nevidljivi (*stealth*) za antivirus softver prve generacije. Skicirati postupak izvršavanja programa zaraženog takvim virusom.

Napomena: Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Potrebno je na svesci naznačiti ukoliko želite da Vam se poeni sa prvog kolokvijuma računaju umesto zadataka označenih sa K. Ispit traje 180 minuta.