Ispit iz Zaštite podataka (SI4ZP, IR4ZP) 12.06.2012.

1. (K1)(**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. (K1)(**10p**) Nacrtati strukturnu šemu *AES* algoritma za veličinu ključa od 128 bita i objasniti način funkcionisanja algoritma prilikom šifrovanja. Objasniti strukturu jedne iteracije *AES* algoritma. Objasniti svaku od faza iteracije. Objasniti algoritam koji se koristi za ekspanziju ključa kod *AES* algoritma.

3. (K1)(**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?

---

1. (K2)(**10p**) Šta su *replay* napadi i kako izbegavamo te napade? Navedite elementarni primer lažnog predstavljanja korišćenjem *replay* napada.

2. (K2)(**10p**) Objasniti čemu služi i kako se koristi *Diffie-Hellman* algoritam. Napisati dokaz da algoritam funkcioniše. Kako se izvodi *man-in-the-middle* napad i kako ga je moguće sprečiti kod *Diffie-Hellman* algoritma?

3. (K2)(**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).

---

1. (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.

2. (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.

3. (I)(**5p**) Objasniti proaktivnu proveru šifara kao jednu od strategija za izbor šifara. Koje sve varijante proaktivne provere šifara postoje?

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 K1. Potrebno je na svesci naznačiti ukoliko želite da Vam se poeni sa drugog kolokvijuma računaju umesto zadataka označenih sa K2. Ispit traje 180 minuta.