Ispit iz Zaštite podataka (SI4ZP, IR4ZP) 11.06.2013.

1. (K1)(**10p**) Polialfabetske substitucione šifre – osobine i razlog uvođenja. Posebno analizirajte Vigenère šifru i prodiskutujte uticaj dužine ključa na sigurnost.

2. (K1)(**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.

3. (K1)(**10p**) Nacrtati i objasniti *CBC* i *CFB* modove funkcionisanja blok algoritama. Kada se koristi *CBC*, a kada *CFB*? Koja je razlika između ova dva moda?

---

1. (K2)(**10p**) Objasniti ulogu, osobine i zahteve kodova za autentikaciju poruka (*MAC* kodovi). Kojim kriptografskim mehanizmima se realizuju i po čemu se razlikuju od *hash* funkcija?

2. (K2)(**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. Šifrovati poruku M=5, koristeći javni ključ PU={17, 77}. Za izračunavanje šifrovane vrednosti koristiti algoritam za brzu eksponentizaciju.

3. (K2)(**10p**) Nacrtati i objasniti postupak prilikom generisanja i prilikom prijema *PGP* poruke uz ostvarivanje tajnosti i autentikacije i uz korišćenje prstenova ključeva. Zanemariti kompresiju i konverziju.

---

1. (I)(**10p**) Objasniti mehanizam duplog potpisa kod *SET* sistema za finansijske transakcije. Šta se postiže korišćenjem ovog mehanizma?

2. (I)(**10p**) Koje četiri tehnike je moguće koristiti da bi se korisnicima sistema omogućilo da sami biraju šifre, ali da se pritom eliminišu šifre koje su lake za pogađanje? Kratko objasniti svaku od njih.

3. (I)(**5p**) Šta predstavljaju i kako se koriste zapisi osluškivanja (*audit records*) kod sistema za detekciju upada? Koje vrste ovih zapisa postoje i koje su prednosti i mane svake od njih?

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.