Ispit iz Zaštite podataka (SI4ZP, IR4ZP, MS1ZP) 14.06.2011.

1. (K1) Poruku „zastita podataka“ šifrovati *Vigenère* algoritmom sa *autokey* poboljšanjem i ključem: „kljuc“. Objasniti zašto je uvedeno *autokey* poboljšanje. Napomena: koristiti 26 slova engleske abecede.

2. (K1) Pre prelaska sa *DES* algoritma na *AES* algoritam pokušano je poboljšanje *DES* algoritma njegovom višestrukom uzastopnom primenom. Objasniti napad zbog koga nije izabran *Double-DES*. Objasniti kako izgleda *Triple-DES*, koje sve varijante postoje i zbog čega.

3. (K1) Nacrtati izgled jedne kompletne iteracije *AES* algoritma prilikom šifrovanja. Objasniti svaku operaciju koja učestvuje u iteraciji.

---

1. (K2) Objasniti čemu služe i kako se koriste autentikacioni kodovi poruka (*MAC*). U čemu su osnovne razlike i sličnosti u odnosu na digitalno potpisivanje.

2. (K2) Objasniti čemu služi i kako se koristi *Diffie-Hellman* algoritam. Napisati dokaz da algoritam funkcioniše. Koja je osnovna razlika između *Diffie-Hellman* i *RSA* algoritma?

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

---

1. (K3) Objasniti mehanizam duplog potpisa kod *SET* sistema za finansijske transakcije. Šta se postiže korišćenjem ovog mehanizma?

2. (K3) Navesti tri klase uljeza koje postoje i opisati svaku od njih.

3. (K3) Nacrtati i objasniti konsolidovani konceptualni model kontrole pristupa (zaštite) pomoću uloga. Šta se postiže uvođenjem kontrole pristupa pomoću uloga?

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.