Ispit iz Zaštite podataka (MS1ZP) 11.06.2013.

1. (K)(**10p**) Objasniti *One time pad* algoritam. Ako se ključ generiše pseudoslučajnim generatorom, da li i dalje važi da je nemoguće dekriptovati poruku. Obrazložiti.

2. (K)(**10p**) Kada i kako se radi distribucija tajnih sesijskih ključeva pomoću javnih ključeva?

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

5. (K)(**10p**) Objasniti čemu služi i kako se koristi *Diffie-Hellman* algoritam. Napisati dokaz da algoritam funkcioniše. Dati konkretan predlog na koji način se može sprečiti *man-in-the-middle* napad na *Diffie-Hellman* protokol (poželjno koristiti postojeće elemente iz *Diffie-Hellman* algoritma koliko god je moguće)?

---

1. (I)(**10p**) Objasniti *Three Way* autentikaciju kod *X.509* autentikacionog servisa. Razlozi za postojanje i poređenje sa jednostavnijim *X.509* autentikacionim servisima.

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

3. (I)(**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.

4. (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.

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.