Ispit iz zaštite podataka (MS1ZP) 28.08.2012.

1. (**20p**) Šta se sve mora uraditi ako je kompromitovan tajni ključ izdavaoca X.509 sertifikata, da bi se ponovo uspostavio sistem sigurnosti zasnovan na X.509?

2. (**20p**) Opisati osnovne osobine, entitete i mehanizam SET (*Secure Electronic Transaction*) transakcije.

3. (**20p**) 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. (**20p**) Nacrtati i objasniti postupak prilikom generisanja i prilikom prijema PGP (*Pretty Good Privacy*) poruke uz ostvarivanje tajnosti i autentikacije i uz korišćenje prstenova ključeva. Zanemariti kompresiju i konverziju.

5. (**20p**) Šta su to zapisi osluškivanja (*audit records*) i koja je razlika između izvornih zapisa osluškivanja i zapisa osluškivanja specifičnih za detekciju? Kako funkcioniše detekcija upada u sistem zasnovana na identifikaciji penetracije (*penetration identification*)? Šta je cilj sistema za detekciju upada (šta takav sistem treba da ispuni da bi bio od koristi)?

Trajanje ispita 3 sata