Ispit iz zaštite podataka (SI4ZP, IR4ZP) 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. (**25p**) 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. Koja je uloga prstenova ključeva kod PGP protokola? Koji mehanizam se koristi za upravljanje ključevima kod PGP protokola i na koji način se koriste prstenovi ključeva, kao podrška za taj mehanizam? Kako se izračunava legitimitet ključa?

Trajanje ispita 3 sata