Ispit iz zaštite podataka (MS1ZP, SI4ZP, IR4ZP) 30.08.2011.

1. (**20p**) 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. (**20p**) Objasniti mehanizam duplog potpisa kod *SET* sistema za finansijske transakcije. Šta se postiže korišćenjem ovog mehanizma?

3. (**20p**) Objasniti postupak prilikom šifrovanja pomoću DES algoritma. Nacrtati i objasniti strukturu jedne iteracije.

4. (**20p**) Objasniti kako se kod RSA algortima formira par privatni/javni ključ i kako se vrši šifrovanje i dešifrovanje pomoću formiranih ključeva. Nakon objašnjenja dati konkretan primer sa proizvoljnim vrednostima.

5. (**20p**) Šta su zapisi osluškivanja (*audit records*) i na koji način se koriste u detekciji upada? Koje dve vrste ovih zapisa postoje i koje su prednosti i mane svake od njih?

Trajanje ispita 3 sata