Ispit iz Zaštite podataka (SI4ZP, IR4ZP, 13E113ZP, 13S114ZP) 28.08.2016.

1. (**20p**) Originalnu poruku „VNMCMBWKVSOTAKBINBFINOEZVJQ“ propustiti kroz rotor mašinu sa tri rotora prikazanu na slici 1 (svi rotori rotiraju udesno) i ispisati dobijenu šifrovanu poruku. Prikazati detalje šifrovanja prvog i poslednjeg slova originalne poruke. Koliko različitih algoritama zamene koristi ovakva mašina?

Slika 1. Rotor mašina sa tri rotora – početna povezivanja (svi rotori rotiraju udesno)

2. (**15p**) Prikazati osnovne elemente sistema sa javnim ključevima kod kojih se postiže tajnost i autentikacija. Pretpostavite da se autentikacija ostvaruje primenom asimetričnih algoritama nad celom porukom.

3. (**15p**) Objasnite kako se u komunikaciji između *Kerberos realm*-ova obezbeđuje pristup klijenta iz jednog *realm*-a servisu iz drugog *realm*-a. Navedite svaki korak u autentikaciji i autorizaciji. Ako je u toku rada potrebno prići servisu iz nekog trećeg *realm*-a, da li je potrebno ponovo se ulogovati?

4. (**15p**) Koje funkcije se koriste u *S/MIME* za obezbeđivanje tajnosti, autentikacije (razmatrati obe varijante autentikacije) i tajnosti i autentikacije? Objasniti na koji način se vrši osiguravanje *MIME* entiteta u slučaju da želimo da postignemo tajnost. Objasniti na koji način se vrši osiguravanje *MIME* entiteta u slučaju da želimo da postignemo autentikaciju (razmatrati obe varijante autentikacije).

Napomena: *Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Ispit traje 180 minuta.*