Teorija kodiranja in kriptografija - vaje 1, 25. februar 2014

Uvodne naloge

1. Izračunajte največji skupni delitelj števil 899 in 812. Poiščite še celi števili s in t, da bo veljalo $899s + 812t = \gcd(899, 812)$.

2. Pokažite, da pri Evklidovem algoritmu velja $r_{i+2} < r_i/2$ za $1 \leq i \leq k-2$, kjer je k število korakov. S pomočjo tega ocenite število korakov Evklidovega algoritma.

3. Izračunajte $\varphi(360)$.

4. Sestavite tablico za množenje za grupo $\mathbb{Z}_{12}^*$.

5. Koliko elementov ima grupa $\mathbb{Z}_{25}^*$? Ali je 18 element grupe $\mathbb{Z}_{25}^*$? Če je, izračunajte njegov inverz.

6. Pri substitucijski šifri s ključno besedo je ključ podan s ključno besedo in začetno črko. Naj bo ključna beseda $KRIPTOGRAFIJA$ in začetna črka S. Poiščite ključ (permutacijo) in zašifrirajte besedilo $JUTRI$. Kolikšno je število ključev pri tej varianti substitucijske šifre, če je ključ dolg med 4 in 10 znakov, začetna črka pa je vedno A? Kolikšno je število ključev pri varianti substitucijske šifre, kjer je ključ permutacija reda dva brez fiksnih točk?

7. Razbijanje substitucijske šifre s pomočjo frekvenčne analize v računalniški učilnici (šteje tudi za 1. domačo nalogo).