Teorija kodiranja in kriptografija - vaje 2, 4. marec 2014

Klasične šifre

1. Razbijanje Vigenerjeve šifre s pomočjo testa Kasiskega in frekvenčne analize (kazalec na spletni učilnici).

2. Šifrirni stroj Enigma je sestavljen iz tipkovnice, stikalne ploščice, treh rotorjev, reflektorja, rotorja in plošče z lučkami. Za poenostavljeno Enigmo (6 črk, stikalna ploščica, ki zamenja po dva para črk, trije rotorji, reflektor) šifrirajte besedilo BBB.

3. Izračunajte število ključev za Enigmo s 26 črkami. Ključ je sestavljen iz

   (i) nastavitve stikalne ploščice (zamenja 6-krat po dve črki),

   (ii) izbire treh rotorjev izmed petih,

   (iii) permutacije treh rotorjev in

   (iv) začetne postavitve vsakega izmed treh rotorjev.

4. Pokažite, da je odšifriranja pri Enigmi enako šifriranju. Nasvet: predstavite šifrirnje kot produkt ustreznih permutacij.

5. Zašifrirajte in potem spet odšifrirajte sporočilo *MIŠ* z afino šifro s ključem $(7, 3)$ (delamo v kolobarju $\mathbb{Z}_{25}$).

6. Izračunajte število ključev za Hillovo šifro z dolžino bloka n nad $\mathbb{Z}_p$, kjer je p praštevilo. Nasvet: determinanta matrike je različna od nič natanko tedaj, ko so njene vrstice linearno neodvisne.

7. Ali je Hillova šifra odporna na napad z znanim besedilom? Če je ključ matrika dimenzije $n \times n$, koliko najmanj parov besedilo/kriptogram potrebujemo, da lahko izračunamo ključ? Prestregli smo kriptogram *KMHBTJ* in uganili, da pripada besedilu *KRIPTO*. Predpostavimo, da je besedilo zašifrirano s Hillovo šifro z dolžino bloka 2. Izračunajte ključ.

8. V $\mathbb{Z}_{25}$ rešite sistem enačb

$$\begin{aligned} 3x_1 + 9x_2 + 15x_3 &= 2 \\ 2x_1 + 6x_2 + 10x_3 &= 18 \\ 5x_1 + 8x_2 + 11x_3 &= 5 \end{aligned}$$