1. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 10. junij 2013

1. (25 točk) Naj bo končni obseg $\mathrm{GF}(2^6)$ generiran z nerazcepnim polinomom $f(x) = x^6+x+1$. Preverite, da je x generator grupe $\mathrm{GF}(2^6)^*$ in v tej grupi poiščite element reda 9 (zapišite ga kot polinom stopnje manjše od 6). Kolikšen je red elementa $x + 1$?

2. (20 točk) Prestregli smo kriptogram

$$0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1,$$

ki je dobljen s seštevanje besedila (v dvojiškem zapisu) in izhoda LFSR po modulu 2. Uganemo, da se besedilo začne z nizom

$$1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0.$$

Odkodirajte še preostanek besedila (pri predpostavki, da ima LFSR, ki vrne ustrezno zaporedje ključev, najmanjšo možno stopnjo).

3. (30 točk) Bojanov javni ključ za sistem RSA je (n, e), kjer je $n = 899$ in $e = 23$.

   (a) Poiščite dekodirni eksponent d (pri predpostavki, da poznate razcep števila n, $n = 29 \cdot 31$).

   (b) Ali bi Bojan za kodirni eksponent lahko izbral sodo število, na primer $e = 4$?

   (c) Bojan pošlje svoj javni ključ Aniti po elektronski pošti. Oskar pismo prestreže, spremeni kodirni eksponent e v $e' = 17$ in pismo posreduje Aniti. Anita zašifrira besedilo b s ključem (n, e') in ga pošlje Bojanu. Bojan sporočila seveda ne more razvozlati in zopet pošlje Aniti svoj javni ključ. Anita še enkrat zašifrira sporočilo b, tokrat s ključem (n, e) in ga pošlje Bojanu. Oskar je prestregel obe Anitini pismi. Natančno opišite, kako lahko izračuna besedilo b (pri predpostavki, da ne pozna razcepa števila n oziroma dekodirnega eksponenta d).

4. (25 točk) Naj bo $\mathcal{C}$ trojiški linearen kod z generatorsko matriko

$$G = \begin{bmatrix} 2 & 0 & 1 & 2 \\ 1 & 2 & 1 & 0 \end{bmatrix}.$$

Poiščite generatorsko matriko za $\mathcal{C}$ v standardni obliki. Poiščite nadzorno matriko za kod $\mathcal{C}$. Kolikšna je razmaknjenost koda $\mathcal{C}$? Koliko napak lahko popravi? Dekodirajte prejeto besedo 1111.

Vse odgovore je potrebno ustrezno utemeljiti!