2. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 3. julij 2012

1. Naj bo $GF(2^6)$ končni obseg, konstruiran z nerazcepnim polinomom $f(x) = x^6 + x + 1$. Simetrični kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ definiramo takole:

$$\mathcal{B} = \mathcal{C} = GF(2^6) \quad \text{in} \quad \mathcal{K} = GF(2^6)^*,$$

za ključ $p \in GF(2^6)^*$ je kodirna funkcija definirana kot

$$E_p(b) = b \cdot p \pmod{f}.$$

   (a) Pokažite, da za tako definirano kodirno funkcijo vedno obstaja tudi dekodirna funkcija s potrebnimi lastnostmi, in jo opišite.

   (b) Za dani kodirni ključ $p(x) = x^3 + x + 1$ dekodirajte kriptogram $c(x) = x^3 + x$.

2. Tokovno šifro sestavimo iz dveh linearnih rekurzivnih šifer (vse računanje poteka po modulu 2):

$$z_i = x_i + y_i, \qquad \text{kjer je} \qquad x_i = x_{i-1} + x_{i-2} \qquad \text{in} \qquad y_i = y_{i-1} + y_{i-3}.$$

Začetni ključ je $(x_1, x_2, y_0, y_1, y_2)$. Dano besedilo $b_1, b_2, b_3 \ldots$(zaporedje ničel in enk) zakodiramo v kriptogram $c_1, c_2, c_3 \ldots$ takole:

$$c_i = b_i + z_{i+2} \pmod{2}.$$

   (a) Za dan začetni ključ $(1, 1, 1, 1, 1)$ izračunajte prvih nekaj členov zaporedij x_i, y_i in z_i. Kakšne so njihove periode?

   (b) Recimo, da smo prestregli kriptogram $c = 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1$ ter uganili začetni del besedila $b = 0, 0, 1, 0, 0, 1, 1, 0, 1, 0$. Dekodirajte še preostanek kriptograma!

3. Anita in Bojan bi se rada dogovorila za skupen ključ po ne-varnem kanalu s pomočjo Diffie-Hellmanovega algoritma. Izbrala sta praštevilo $p = 227$ in bazo $g = 5$.

   (a) Preverite, da je g generator grupe $\mathbb{Z}_{227}^*$.

   (b) Anita je izbrala naključno število $a = 4$ in Bojanu poslala $A = g^a$. Bojan je izbral naključno število b in Aniti poslal $B = g^b = 200$. Izračunajte skupni ključ!

4. Naj bo $\mathcal{C}$ dvojiški $[n, k, d]$-linearen kod z generatorsko matriko G in nadzorno matriko H. Iz koda $\mathcal{C}$ sestavimo nov kod $\mathcal{C}'$ tako, da na konec vsake besede dodamo parnostni bit (število enic v vsaki besedi je potem sodo število).

   (a) Pokažite, da je tudi $\mathcal{C}'$ linearen kod in poiščite njegove parametre. Koliko napak odkrije/popravi v primerjavi s kodom $\mathcal{C}$?

   (b) Naj bo

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

   generatorska matrika za kod $\mathcal{C}$. Poiščite generatorsko in nadzorno matriko za kod $\mathcal{C}'$.

Vse naloge je potrebno ustrezno utemeljiti!