2. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 8. julij 2013

1. 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. Tokovna šifra je definirana na naslednji način. Ključ je sestavljen iz permutacije $\pi \in S(\mathbb{Z}_n)$ in števila $a \in \mathbb{Z}_n$. Kodirna funkcija $E_{(\pi,a)}$ besedilu b_i, $i \in \{1, 2, \ldots\}$ priredi

$$E_{(\pi,a)}(b_i) = \pi(b_i) + a + i - 1 \bmod n.$$

   (a) Izračunajte število vseh možnih ključev.

   (b) Poiščite ustrezno dekodirno funkcijo.

   (c) Za $n = 5$, $\pi = (0)(14)(23)$ in $a = 2$ dešifrirajte zaporedje besedil $(1, 1, 2, 2)$.

   (d) Poiščite zaporedje besedil $(b_1, b_2, b_3, b_4, b_5)$, ki se po šifriranju s ključem iz točke (c) ne spremeni.

   (e) Analizirajte varnost gornjega kriptosistema glede na napad z znanim besedilom oziroma golim kriptogramom.

3. Avtoriteta ima javni ključ za RSA (n, e) in zasebni ključ d. Radi bi, da nam podpiše sporočilo m, a sporočila ne želimo razkriti. Zato podtaknemo v podpis neko drugo sporočilo $m' \equiv k \cdot m \pmod{n}$. Privzamemo lahko, da je sporočilo m tuje z n (sicer znamo n razcepiti in lahko sami podpišemo karkoli).

   (a) Kako moramo izbrati k, da bomo iz podpisa sporočila m' ($s' \equiv m'^d \pmod{n}$) lahko izračunali podpis sporočila m ($s \equiv m^d \pmod{n}$), ne da bi uporabili zasebni ključ d?

   (b) Naj bo $n = 85$, $e = 11$ in $m = 42$. Poiščite k in sporočilo m' kot v točki (a).

   (c) Kaj pa če so veljavna le sporočila, ki so soda števila (drugačnih avtoriteta ne podpisuje)? Kako težko je sedaj poiskati primerno število k?

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

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

   generatorska matrika za kod $\mathcal{C}$. Poiščite generatorsko in nadzorno matriko za kod $\mathcal{C}'$. Koliko napak popravi kod $\mathcal{C}$? Kaj pa kod $\mathcal{C}'$

   (c) S pomočjo nadzorne matrike iz točke (b) dekodirajte prejeto besedo 1110000.

Vse odgovore je potrebno ustrezno utemeljiti!