4. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 11. september 2012

Vse odgovore je treba ustrezno utemeljiti!

1. Obseg $\mathrm{GF}(2^4)$ je konstruiran z nerazcepnim polinomom $f(x) = x^4 + x + 1$. Ali je element $\alpha = x$ generator grupe $\mathrm{GF}(2^4)^*$? Poiščite rede elementov α, $\beta = 1 + x$, $\gamma = x + x^2$ in $\delta = x^2 + x^3$. Poiščite še γ^{-1}.

2. Anita ima javni ključ $N = p\,q$, kjer sta p in q veliki praštevili, kongruentni 3 po modulu 4. Števili p in q predstavljata Anitin zasebni ključ. Bojan najprej izbere naključno število $s < N$ in nato šifrira sporočilo m dolžine n za Anito takole.

$$\begin{aligned} x_0 &= s \\ x_{k+1} &\equiv x_k^2 \bmod N; \quad k = 0, \ldots, n. \end{aligned}$$

   Naj bo b_i zadnji bit števila x_i. Potem je $c = m \oplus b_2 b_3 \ldots b_{n+1}$ kriptogram, ki ustreza sporočilu m. Bojan pošlje Aniti (x_n, c).

   (a) Recimo, da Anita dobi (x, c). Pokažite, da lahko vedno iz enačbe $d \cdot 2^n \equiv 4 \pmod{\varphi(N)}$ izračuna d, kjer je n dolžina c. Izračunajte d za primer, ko je $N = 77$ in $n = 10$.

   (b) Pokažite, da je $x_n^d \equiv x_2 \pmod N$.

   (c) Kako Anita dešifrira prejeti kriptogram?

3. Sporočilo oblike $a_1a_2a_3a_4 \in \mathbb{Z}_{11}^4$ kodiramo v kodno besedo $c_1c_2c_3c_4c_5c_6c_7 \in \mathbb{Z}_{11}^7$ na naslednji način: $c_i = a_i$ za $i = 1, \ldots, 4$, c_5, c_6 in c_7 pa določimo tako, da je

$$\sum_{i=1}^{7} c_i \equiv 0 \pmod{11}, \quad \sum_{i=1}^{7} i\, c_i \equiv 0 \pmod{11} \quad \text{in} \quad \sum_{i=1}^{7} i^2\, c_i \equiv 0 \pmod{11}.$$

   Pokažite, da je dobljeni kod linearen. Določite generatorsko in nadzorno matriko za ta kod. Kolikšna je razmaknjenost dobljenega koda in koliko napak popravi?

4. Naj bo $h : \{0,1\}^* \to \{0,1\}^n$ zgoščevalna funkcija, ki je odporna na trke. Katera od naslednjih zgoščevalnih funkcij $H_i : \{0,1\}^* \to \{0,1\}^n$ je odporna na trke?

   (a) $H_1(m) = H(|m|)$ (torej povzetek dolžine besedila m),

   (b) $H_2(m) = H(m)[0, \ldots, 31]$ (torej samo prvih 32 bitov povzetka),

   (c) $H_3(m) = H(m)||H(m)$,

   (d) $H_4(m) = H(m||m)$,

   (e) $H_5(m) = H(m) \oplus H(m \oplus 1^{|m|})$,

   (f) $H_6(m) = H(H(H(m)))$.