3. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 3. september 2012

Vse odgovore je treba ustrezno utemeljiti!

1. Naj bo $\mathcal{S} = (\mathbb{Z}_2^{128}, \mathbb{Z}_2^{128}, \mathbb{Z}_2^{128}, \mathcal{R}, \mathcal{D})$ nek "dober" simetričen kriptosistem. Z E_k označimo kodirno funkcijo, ki uporablja ključ k. Sedaj definiramo zgoščevalno funkcijo, ki poljubnemu besedilu $b = (b_1, \ldots b_n)$ priredi izvleček $h = E_{b_1}(IV) \oplus \ldots \oplus E_{b_n}(IV)$, kjer je IV nek vnaprej izbrani element $\mathbb{Z}_2^{128}$.

   Katere od lastnosti naslednjih ima takšna zgoščevalna funkcija: odpornost praslik, odpornost drugih praslik, odpornost na trke?

2. Naj bo $GF(32)$ končni obseg, konstruiran z nerazcepnim polinomom $f(x) = x^5+x^4+x^3+x+1$. Simetrični kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ definiramo takole:

$$\mathcal{B} = \mathcal{C} = \mathrm{GF}(32) \text{ in } \mathcal{K} = \mathrm{GF}(32)^* \times \mathrm{GF}(32),$$

   za ključ (p, q) je kodirna funkcija definirana kot

$$E_{(p,q)}(b) = b \cdot p + q \pmod{f}.$$

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

   (b) Za dani kodirni ključ ($p(x) = x^2+1, q(x) = x^4+1$) dekodirajte kriptogram $c(x) = x^3+x+1$.

3. Naj bo p veliko praštevilo in g generator grupe $\mathbb{Z}_p^*$.

   (a) Pokažite, da velja $g^{(p-1)/2} = p - 1$.

   (b) Dano je število $y = g^x \bmod p$. Pokažite, kako lahko z izračunom $y^{(p-1)/2}$ ugotovimo parnost števila x.

   (c) Kakšna je parnost števila x za primer $p = 1009$, $g = 11$ in $y = 26$?

4. Naj bo $\mathcal{C}$ linearen $[n, k, d]$-kod nad abecedo Σ in H ena od njegovih nadzornih matrik. Naj ima beseda $x \in \Sigma^n$ težo manjšo ali enako $\lfloor (d-1)/2 \rfloor$. Označimo s $s = Hx^T$ sindrom besede x.

   (a) Naj bo $y \in \Sigma^n$ beseda, za katero velja $Hy^T = s$. Pokažite, da je potem $x - y$ kodna beseda.

   (b) Pokažite, da ima x najmanjšo težo med vsemi besedami, ki imajo sindrom s.

   (c) Dana je nadzorna matrika

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

   Poiščite besedo z najmanjšo težo, ki ima sindrom $(10000)^T$. Ali je beseda z najmanjšo težo in sindromom $(11111)^T$ enolično določena?