Kriptografija in teorija kodiranja – 4. domača naloga
(do torka 21. aprila 2009)

---

1. Naj bo zgoščevalna funkcija $H_1 : \{0,1\}^{2\ell} \longrightarrow \{0,1\}^{\ell}$, krepko brez trčenj (collision resistant), tj. ni moč v doglednem času najti različna $x, x' \in \{0,1\}^{2\ell}$, za katera je $H_1(x) = H_1(x')$.
   Naj bo $H_2 : \{0,1\}^{4\ell} \longrightarrow \{0,1\}^{\ell}$, $x \in \{0,1\}^{4\ell}$ in $x = x_1||x_2$, kjer sta $x_1, x_2 \in \{0,1\}^{2\ell}$ in $||$ simbol za spoj/spetje (konkatenacijo) dveh zaporedij bitov.
   Dokaži, da je funkcija $H_2(x) = H_1(H_1(x_1)||H_1(x_2))$ tudi krepko brez trčenj.

2. Dokaži, da je trinom $x^n + x^m + 1$ nerazcepen natanko tedaj, ko je nerazcepen trinom $x^n + x^{n-m} + 1$.

3. Naj bo $T = (t_{mk})$ $n \times n$-razsežna matrika definirana z i
   $$\beta\beta^{p^m} = \sum_{k=0}^{n-1} \beta^{p^k} t_{mk}.$$
   Dokaži, da je kompleksnost matrike T za množenje v normalne bazi
   $$\{\beta, \beta^p, \ldots, \beta^{p^{n-1}}\}$$
   vsaj $2n - 1$ (tj. število neničelnih elementov).

4. Z matriko T iz prejšnje naloge izračunaj $\beta^{p^h}\beta^{p^m}$.

5.

6.

7.

9.

10.