3. izpit iz KRIPTOGRAFIJE IN TEORIJE KODIRANJA 1

Ljubljana, 27. avgust 2013

1. (25 točk) Za kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ je $\mathcal{B} = \{x, y, z, w\}$, $\mathcal{C} = \{X, Y, Z, W\}$ in $\mathcal{K} = \{k_1, k_2, k_3\}$, družina kodirnih funkcij pa je podana s spodnjo tabelo:

	x	y	z	w
k_1	Z	W	Y	X
k_2	Z	X	W	Y
k_3	W	Z	X	Y

.

Kriptosistem $\mathcal{S}$ opremimo še z verjetnostnimi porazdelitvami B, C in K na množicah $\mathcal{B}$, $\mathcal{C}$ in $\mathcal{K}$: $P[B = x] = 0.25$, $P[B = y] = 0.3$, $P[B = z] = 0.15$, $P[B = w] = 0.3$, $P[K = k_1] = P[K = k_3] = 0.25$, $P[K = k_2] = 0.5$. Predpostavimo, da sta B in K neodvisni.

   (a) Poiščite družino dekodirnih funkcij.

   (b) Izračunajte $P[C = X]$ in $P[C = Z]$.

   (c) Ali ima kriptosistem $\mathcal{S}$ lastnost popolne tajnosti?

2. (20 točk) Naj bodo elementi končnega obsega $GF(2^5)$ podani kot polinomi stopnje 4, računamo pa po modulu nerazcepnega polinoma $f(x) = x^5 + x^2 + 1$. V obsegu $GF(2^5)$ rešite enačbo

$$a \cdot t = b,$$

   kjer je a predstavljen s polinomom $a(x) = x^4 + x^2 + x$ in b s polinomom $b(x) = x^3 + x + 1$. Vse korake utemeljite!

3. (30 točk) Alenka ima javni ključ $N = p\,q$, kjer sta p in q veliki praštevili, kongruentni 3 po modulu 4; števili p in q predstavljata Alenkin zasebni ključ. Boris najprej izbere naključno število $s < N$ in nato šifrira sporočilo m dolžine n za Alenko 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. Boris pošlje Alenki (x_n, c).

   (a) Recimo, da Alenka 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 $N = 133$ in $n = 8$.

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

   (c) Kako Alenka dešifrira prejeti kriptogram?

4. (25 točk) Poiščite največji dvojiški linearni kod z dolžino besede $n = 8$ in razmaknjenostjo $d = 4$. Poiščite še največji trojiški linearni kod z dolžino besede $n = 8$ in razmaknjenostjo $d = 4$. Vsakega od kodov podajte z generatorsko matriko.

Vse odgovore je potrebno ustrezno utemeljiti!