1. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 5. julij 2010

1. (25 točk) Dokažite ali poiščite protiprimer. Če ima kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ z dano verjetnostno porazdelitvijo na množici $\mathcal{B} \times \mathcal{K}$ (pri kateri je verjetnost vsakega besedila in vsakega ključa večja od 0) lastnost popolne tajnosti, potem so vsi ključi enako verjetni.

2. (20 točk) Prestregli smo kriptogram

$$0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1,$$

   ki je dobljen s seštevanje besedila (v dvojiškem zapisu) in izhoda LFSR po modulu 2. Uganemo, da se besedilo začne z nizom

$$1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0.$$

   Odkodirajte še preostanek besedila (pri predpostavki, da ima LFSR, ki vrne ustrezno zaporedje ključev, najmanjšo možno stopnjo).

3. (30 točk) Naj bo (n, e) javni ključ za sistem RSA, kjer je $n = 31 \cdot 43 = 1333$ in $e = 17$.

   (a) Poiščite dekodirni eksponent d.

   (b) Z javnim ključem $(1333, 17)$ zašifrirajte sporočilo $b = 10$.

   (c) Ali v grupi $\mathbb{Z}_n^*$ obstajajo elementi reda 1, 2, 4, 8, 16? (ustrezna besedila pri šifriranju s ključem $(1333, 17)$ ostanejo enaka!) Za vsakega od navedenih redov poščite po en element oziroma utemeljite, zakaj takšen element ne obstaja.

4. (25 točk) Naj bo $\mathcal{C}$ trojiški linearen kod z generatorsko matriko

$$G = \begin{bmatrix} 2 & 0 & 1 & 2 \\ 1 & 2 & 1 & 0 \end{bmatrix}.$$

   Poiščite generatorsko matriko za $\mathcal{C}$ v standardni obliki. Poiščite nadzorno matriko za kod $\mathcal{C}$. Kolikšna je razdalja koda $\mathcal{C}$? Koliko napak lahko popravi? Dekodirajte prejeto besedo 1111.

Vse odgovore je potrebno ustrezno utemeljiti!