1. kolokvij iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 24. april 2012

1. Naj bo p veliko praštevilo. Simetrični kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ definiramo takole:

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_p \text{ in } \mathcal{K} = \mathbb{Z}_{p-1}^*,$$

za ključ $k \in \mathbb{Z}_{p-1}^*$ je kodirna funkcija definirana kot

$$E_k(b) = b^k \pmod{p}.$$

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

   (b) Naj bo $p = 47$. Za dani kodirni ključ $k = 5$ dekodirajte kriptogram $c = 10$.

   (c) Ali je kriptosistem $\mathcal{S}$ odporen na napad znanim besedilom?

2. Naj bo za kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ dana verjetnostna porazdelitev na množici $\mathcal{B} \times \mathcal{K}$, za katero velja, da se vsako besedilo in kriptogram pojavi z neničelno verjetnostjo. Dokažite ali poiščite protiprimer: če ima kriptosistem s takšno verjetnostno porazdelitvijo lastnost popolne tajnosti, potem so vsi ključi enako verjetni.

3. Zaporedje izhodnih znakov pri neki nelinearni dvojiški tokovni šifri je podano z rekurzivno zvezo

$$f(z_0, z_1, z_2, z_3) = z_0 + z_2 + z_0 z_2 z_3 + z_1 z_2 \pmod{2}.$$

   (a) Poiščite nekaj členov zaporedja, ki je generirano z začetnim stanjem $z_0 z_1 z_2 z_3 = 0001$. Ali je zaporedje periodično?

   (b) Poiščite linearno rekurzivno šifro najmanjšega reda, ki bo iz začetnega stanja 0001 generirala isto izhodno zaporedje kot v točki (b).

4. Naj bo p praštevilo in α, γ generatorja grupe $\mathbb{Z}_p^*$. Recimo, da znamo učinkovito izračunati logaritme v $\mathbb{Z}_p^*$ za bazo α. Pokažite, da znamo potem učinkovito izračunati tudi logaritme za bazo γ.

   Postopek ilustrirajte za primer $p = 23$, $\alpha = 5$, $\gamma = 7$, ko iščemo $\log_7 10$, torej x, pri katerem je $7^x \equiv 10 \pmod{23}$. Logaritme z osnovo α odčitajte iz spodnje tabele.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\log_5 i$	22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8	7	12	15	5	13	11

Vse naloge je potrebno ustrezno utemeljiti!