Domača naloga 2 iz Teorije kodiranja in kriptografije

Domačo nalogo rešujte samostojno. Oddati je potrebno dokument s kodo preko spletne učilnice. Poročilo lahko podate kot komentarje v kodi ali pa kot ločen dokument. Priporočeno in zaželeno je, da za programski jezik uporabite Python. V kolikor želite uporabiti kak drug jezik, najprej pišite asistentu za potrditev. Rok za oddajo je 17.4.2019. Datoteke pred oddajo združite v eno datoteko (zip, rar,...) z vašim imenom in vpisno v imenu, recimo *tilen_marc_23424123745.zip*.

Geffejev generator

Geffejev generator je sestavljen iz treh pomičnih registrov s povratno zanko: LFSR1, LFSR2 in LFSR3. Označimo izhodne bite posameznih registrov z x_1, x_2 oziroma x_3. Potem je izhodni bit generatorja enak $z = x_1x_2 + x_2x_3 + x_3 \pmod 2$.

Naj bodo karakteristični polinomi LFSR-jev za dani Geffejev generator enaki

$$p_1(x) = x^5 + x^2 + 1$$
$$p_2(x) = x^7 + x + 1$$
$$p_3(x) = x^{11} + x^2 + 1.$$

Prestregli ste besedilo v datoteki geffe.txt (datoteka na spletni učilnici). Poiščite začetni ključ (to je začetna stanja za LFSR1, LFSR2 in LFSR3) ter dešifrirajte besedilo. Besedilo je v angleškem jeziku, brez presledkov in ločil. Posamezni črki priredimo število med 0 in 25 (A->0, B->1,..., Z->25), vsakemu od teh števil pa priredimo dvojiško zaporedje dolžine 5 (na primer, D -> 3 -> 00011). Zakodirano besedilo (zaporedje ničel in enk) potem šifriramo tako, da mu prištejemo ključ z ustrezne dolžine, ki ga vrne Geffejev generator, (seštevamo po komponentah po modulu 2).

Opomba 1: Za manjši odbitek točk lahko predpostavite, da ste uganili, da se besedilo začne s *CRYPTOGRAPHY*.

Opomba 2: Zaradi relativno majhnega ključa bi bil izvedljiv tudi napad z izčrpnim pregledom vseh kombinacij treh ključev. Za uspešno opravljeno nalogo ta napad ni veljaven, saj so ključi kratki z namenom, da vaši programi ne bi tekli preveč časa. Ločen pregled ključev za vsak LFSR je dovoljen.