Napadi na bločne šifre, linearne rekurzivne šifre

1. Naj bo P^* slučajna spremenljivka, ki zavzame vrednosti iz množice permutacij $\{0,1\}^n \to \{0,1\}^n$, vsako z enako verjetnostjo. Naj bosta $b, c \in \{0,1\}^n$. Kolikšna je verjetnost dogodka $P^*(b) = c$?

2. Naj bo $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ kriptosistem, za katerega velja $\mathcal{B} = \mathcal{C} = \{0,1\}^n$ in $\mathcal{K} = \{0,1\}^k$. Naj bo $b \in \mathcal{B}$, $c \in \mathcal{C}$.

   (a) Koliko je ključev $k \in \mathcal{K}$, za katere velja $E_k(b) = c$? Z drugimi besedami, koliko ključev dobimo pri izčrpnem pregledu vseh ključev za dana b, c? Predpostavimo, da se kodirne funkcije obnašajo kot naključne permutacije.

   (b) Spremenite algoritem za izčrpni pregled vseh ključev tako, da bo vrnil samo en ključ k. Predpostavite lahko, da imate na voljo t parov (b_i, c_i), za katere je $E_k(b_i) = c_i$. Koliko najmanj mora biti t? Koliko je to za DES, 2DES in 3DES?

3. Linearni rekurzivni šifri sta podani z rekurzivnima enačbama

   (a) $z_{i+4} = z_i + z_{i+1} + z_{i+2} + z_{i+3} \bmod 2$,

   (b) $z_{i+3} = z_i + z_{i+1} + z_{i+2} \bmod 2$.

   Za vsako od šifer poiščite periode za vsakega od začetnih ključev.

4. Kako se hitro vidi, da spodnji zaporedji nista generirani z linearno rekurzivno šifro reda 4?

   a) 1011010000101

   b) $(011101110)^*$

5. Linearna rekurzivna šifra reda 4 je podana z rekurzivno enačbo

$$z_{i+4} = z_i + z_{i+3} \bmod 2.$$

   Zapišite karakterističen polinom, ki ustreza tej enačbi, in z njegovo pomočjo izračunajte periodo zaporedja. Nasvet: če je polinom nerazcepen, je perioda zaporedja kar enaka redu polinoma.

6. Geffejev generator psevdonaključnih števil je sestavljen iz treh pomičnih registrov s povratno zanko, LFSR1, LFSR2 in LFSR3, redov m_1, m_2, m_3 in s periodami $2^{m_1} - 1$, $2^{m_2} - 1$ oziroma $2^{m_3} - 1$. Označimo izhodne bite posameznih registrov z x_1, x_2 oziroma x_3. Potem je izhodni bit generatorja enak $z = x_1 \cdot x_2 + x_2 \cdot x_3 + x_3 \bmod 2$.

   (a) Kolikšna je perioda Geffejevega generatorja, če so števila $2^{m_1} - 1$, $2^{m_2} - 1$ in $2^{m_3} - 1$ paroma tuja?

   (b) Pokažite, da se izhoda LFSR1 in LFSR3 ujemata z izhodom Geffejevega generatorja v približno treh četrtinah primerov, med tem ko se izhod LFSR2 ujema z izhodom Geffejevega generatorja v približno eni polovici primerov.

   (c) S pomočjo ugotovitev iz točke (b) sestavite napad na Geffejev generator z znanim besedilom, ki najde začetne ključe vseh treh LFSR-jev v času $\mathcal{O}(2^{m_1} + 2^{m_2} + 2^{m_3})$.