KRIPTOGRAFIJA

zadaća 4.05

1. Odredite skupove $test_1\left(E_1, E_1^*, C_1'\right)$ i $test_2\left(E_2, E_2^*, C_2'\right)$ ako je

$$E_1 = 001100, \quad E_1^* = 111000, \quad C_1' = 0001,$$

$$E_2 = 000010, \quad E_2^* = 110110, \quad C_2' = 0111.$$

2. Odredite produkt polinoma

$$x^7 + x^6 + x^4 + x^3 + x^2 + 1 \quad \text{i} \quad x^6 + x^3 + x^2 + 1$$

u polju $\mathrm{GF}(2^8)$, definiranom kao $\mathbb{Z}_2[X]/(x^8 + x^4 + x^3 + x + 1)$.