KRIPTOGRAFIJA

Zadaća 4.15

Rok za podizanje zadaće je od 09.05.2003. do (uključivo) 16.05.2003. Rok za predaju ove zadaće je 23.05.2003.

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

$$E_1 = 000001 \quad E_1^* = 110011, \quad C_1' = 0101,$$

$$E_2 = 111010, \quad E_2^* = 000011, \quad C_2' = 1101.$$

2. Odredite produkt polinoma

$$x^7 + x^5 + x^3 + x^2 + x + 1 \quad \text{i} \quad 1 + x^2 + x^3 + x^5$$

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

3. Izračunajte:

$$(\texttt{0x33}\,x^3 + \texttt{0x1}\,x^2 + \texttt{0x3}) \otimes (\texttt{0xB}\,x^3 + \texttt{0x2D}\,x^2 + \texttt{0x39}\,x + \texttt{0xE}).$$

Koeficijenti ovih polinoma su elementi ranije spomenutog polja GF(2^8) zapisani heksadecimalno. Npr. $\texttt{0x85} = 1000\,0101_2 \mapsto x^0 + x^2 + x^7 = 1 + x^2 + x^7$.