KRIPTOGRAFIJA

Zadaća 4.146 X

Rok za podizanje zadaće je od 06.05.2005. do (uključivo) 13.05.2005. Rok za predaju ove zadaće je 20.05.2005.

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

$$E_1 = 011111, \quad E_1^* = 111101, \quad C_1' = 1100$$
$$E_2 = 011110, \quad E_2^* = 110101, \quad C_2' = 1110$$

2. Odredite produkt polinoma

$$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \quad \text{i} \quad x^7 + x^4 + x^3$$

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

3. Izračunajte:

$$(\texttt{0x13}, \texttt{0x1a}, \texttt{0x4a}, \texttt{0x7b}) \otimes (\texttt{0x26}, \texttt{0x98}, \texttt{0x37}, \texttt{0x4a}).$$

Ove vektore pretvaramo u polinome kao na sljedećem primjeru

$$(\texttt{0x33}, \texttt{0x22}, \texttt{0x11}, \texttt{0x00}) \mapsto \texttt{0x33}x^3 + \texttt{0x22}x^2 + \texttt{0x11}x + \texttt{0x00}.$$

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