KRIPTOGRAFIJA

Zadaća 4.79 *Prezime Ime*

Rok za podizanje zadaće je od 07.05.2004. do (uključivo) 14.05.2004. Rok za predaju ove zadaće je 21.05.2004

1. Odredite produkt polinoma

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

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

2. Izračunajte:

   $$(\texttt{0x12}, \texttt{0x4a}, \texttt{0x1a}, \texttt{0x2b}) \otimes (\texttt{0x56}, \texttt{0x78}, \texttt{0x37}, \texttt{0x26}).$$

   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 GF(2^8) zapisani heksadecimalno. Npr. $\texttt{0x85} = 1000\,0101_2 \mapsto x^0 + x^2 + x^7 = 1 + x^2 + x^7$.