KRIPTOGRAFIJA

Zadaća 4.213 X

Rok za podizanje zadaće je od 02.05.2007. do (uključivo) 09.05.2007.
Rok za predaju ove zadaće je 16.05.2007.

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

$$E_1 = 011101, \quad E_1^* = 101101, \quad C_1' = 1011$$
$$E_2 = 001111, \quad E_2^* = 100001, \quad C_2' = 1010$$

2. Izračunajte:

$$(\texttt{0xa2}, \texttt{0x34}, \texttt{0x26}, \texttt{0xbf}) \otimes (\texttt{0x4a}, \texttt{0x7b}, \texttt{0x3a}, \texttt{0x4d}).$$

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. $\texttt{0x85} = 1000\,0101_2 \mapsto x^0 + x^2 + x^7 = 1 + x^2 + x^7$.