KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaća 4.63

1. Odredite produkt polinoma

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

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

2. Izračunajte:

$$(4B\,x^3 + 74\,x^2 + 2D\,x + F2) \otimes (24\,x^3 + E4\,x^2 + 1F\,x + 89).$$

3. Odaberite dva različita četveroznamenkasta prosta broja p i q. Neka je $n = p \cdot q$. Odaberite peteroznamenkasti broj e koji je relativno prost sa $\varphi(n)$. Šifrirajte otvoreni tekst

$$x = 123413$$

pomoću RSA kriptosustava s javnim ključem (n, e). Odredite pripadni tajni ključ d.