KRIPTOGRAFIJA

zadaća 4.34

1. Odredite produkt polinoma

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

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

2. Izračunajte:

$$(E4\,x^3 + 59\,x^2 + 39\,x + 75) \otimes (25\,x^3 + 2B\,x^2 + 3B\,x + 4B).$$

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

$$x = 123435$$

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