KRIPTOGRAFIJA

zadaća 4.42

1. Odredite produkt polinoma

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

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

2. Izračunajte:

$$(C7\,x^3 + E8\,x^2 + C0\,x + 43) \otimes (9C\,x^3 + 4E\,x^2 + 8D\,x + 90).$$

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

$$x = 123654$$

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