

KRIPTOGRAFIJA

zadaca 4.35

1. Odredite produkt polinoma

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

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

2. Izračunajte:

$$(D9x^3 + B2x^2 + 1Dx + 36) \otimes (37x^3 + 02x^2 + CBx + F6).$$

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 .