

KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaca 4.30

1. Odredite produkt polinoma

$$x^7 + x^5 + x^4 + x^3 + x + 1 \quad \text{ i } \quad x^6 + x^5 + x^4 + 1$$

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

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

$$x = 123430$$

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