

KRIPTOGRAFIJA

zadaca 5.05

1. 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

$$x = 123645$$

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

2. Nađite dva pseudoprosta broja u bazi $b = 29$.