# KRIPTOGRAFIJA

zadaća 4.03

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

   $$x = 123546$$

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

2. Nađite neki pseudoprost broj $n$ u bazi $b = 19$.

3. Zadan je broj $n = 2458307$. Nađite dvije baze $b_1$ i $b_2$ takve da je $(b_i, n) = 1$, $b_i \neq \pm 1$ za $i = 1, 2$, te da je $n$ pseudoprost broj u bazi $b_1$, a da $n$ nije pseudoprost broj u bazi $b_2$.