KRIPTOGRAFIJA

zadaća 4.01

1. Odredite skupove $test_1\,(E_1, E_1^*, C_1')$ i $test_2\,(E_2, E_2^*, C_2')$ ako je

$$E_1 = 000011, \quad E_1^* = 110111, \quad C_1' = 0001,$$

$$E_2 = 000010, \quad E_2^* = 110110, \quad C_2' = 0010.$$

2. 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

$$x = 123456$$

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