KRIPTOGRAFIJA

zadaća 3.03

1. Dekriptirajte sljedeća dva šifrata

   `XEMEDDH`

   `VQTRKGX`

   ako je poznato da su dobiveni istim ključem po pravilu

   $$y_i \equiv x_i + k_i \pmod{26}.$$

   Također je poznato da su oba otvorena teksta riječi na hrvatskom jeziku koje počinju jednim od slova `S, P, N, D`.

2. Otvoreni tekst

   `A36BA9B8CA5B178A`

   zapisan heksadecimalno šifrirajte pomoću DES kriptosustava s ključem

   `2693B6A236943784`

   koji je zapisan heksadecimalno (ignorirajte svaki osmi bit ključa).

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

   $$E_1 = 001001, \quad E_1^* = 111101, \quad C_1' = 0001,$$

   $$E_2 = 000010, \quad E_2^* = 110110, \quad C_2' = 0100.$$