KRIPTOGRAFIJA

zadaća 3.34

1. Dekriptirajte šifrat

   ```
   JLLTR VJZES OIALO LEEZS ZEIAE IIUAA
   EAIPB IAUOI RVAOI CRREO RPAUU FNAJH
   ZJCIG IRTKK MIVOK CPDPC
   ```

   ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku, te da je broj stupaca veći od 4, a manji od 16.

2. Dekriptirajte sljedeća dva šifrata

   ```
   SXFITSH
   VRZSKUM
   ```

   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`.

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

   $$E_1 = 001010, \quad E_1^* = 111110, \quad C_1' = 1111,$$

   $$E_2 = 001000, \quad E_2^* = 111100, \quad C_2' = 1101.$$