KRIPTOGRAFIJA

Zadaća 3.85 *X*

Rok za podizanje zadaće je od 16.04.2004. do (uključivo) 30.04.2004. Rok za predaju ove zadaće je 07.05.2004

1. Dekriptirajte šifrat:

   ```
   TDMOT JBODI TVSEI GJIOI IAJZP IAEAJ EALLM REJSZ
   KNIIO IKEAK KEDSL EOAPT ZLEAO VDZSE OMAAO SKTLI
   GJJSM EGATX PLAAT KJAJE IECKI OEPEL AZMKK JASVU
   AAIVN IOMNN
   ```

   ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku, te da je broj stupaca između 4 i 16.

2. Dekriptirajte sljedeća dva šifrata:

   ```
   TLRIEYXR
   JSKKRDYV
   ```

   ako je poznato da su dobiveni istim ključem po pravilu

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

   Oba teksta počinju jednim od slova `s, p, n, d, i`.

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

   $$E_1 = 101111, \quad E_1^* = 010010, \quad C_1' = 1000$$

   $$E_2 = 101001, \quad E_2^* = 011110, \quad C_2' = 1001$$