KRIPTOGRAFIJA

zadaća 3.05

1. Dekriptirajte šifrat

   ```
   ITTUJ PSTAL NATCN RIUSK ENJIK EIMAD
   KOATU RAANI ITIAO VPSAL VAEJI CMARA
   PRSVO COOLS JKECR
   ```

   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

   ```
   XFHJYOU
   LCJUHYS
   ```

   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. Otvoreni tekst

   ```
   3CA64DE9C1B123A7
   ```

   zapisan heksadecimalno šifrirajte pomoću DES kriptosustava s ključem

   ```
   A384558318CAF524
   ```

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