# KRIPTOGRAFIJA

## Zadaća 3.1

Rok za podizanje zadaće je od 11.04.2003. do (uključivo) 18.04.2003. Rok za predaju ove zadaće je 02.05.2003.

1. Dekriptirajte šifrat:

   ```
   IVNDS EKCOM UPONC IKDAD SJUGM SANCH CAENS USIJL
   TLOAS DKSUS EUIIM CAAEU JOIOA JIITA RI
   ```

   ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku, te da je broj stupaca između 4 i 9.

2. Dekriptirajte sljedeća dva šifrata:

   ```
   CODHVBZS
   ZCEDPBNU
   ```

   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`.