KRIPTOGRAFIJA

zadaća 1.03

1. Afinom šifrom s ključem K je iz otvorenog teksta na hrvatskom jeziku dobiven sljedeći šifrat:

   ```
   TXEPC LCNCG TXFEO WXSTB EMQMB CFCMC QBEWL HQGKA
   RSEHK OSXEL CAEGC XVCPE ASLCP MWSLS HKGPS WSACB
   KACBS GCXEP HKVCP CMTEN PCBWC EHKVC PEVTX FSDTE
   TQLCX SNCBE XCNPC PEMBS SCQBE XTXFE OBKWM BCSNB
   KEXSH KFHKX EHCBP EMBS
   ```

   Navedite pet najfrekventnijih slova, te pet najfrekventnijih bigrama u ovom šifratu. Odredite ključ $K = (a, b)$ i otvoreni tekst (dekriptirajte šifrat).

2. Dekriptirajte šifrat

   ```
   QOPVF WTWIV YWRWE WUWHK RUVNV BTFWF GBFGE PRVSP
   BCVFP BFIWF GBFWH RUWYB IBIEV UWAWN RPOBB KEVCG
   BYEPX VUVBC VFPBU WRWKB OVKBC BOVPO XPQWG FKVZF
   HFGPI PGWEP NOVSV GWCBF GHCKW NPVNE PTHKO UHSWI
   PCBAB SHEVU WSVVO VXEPN P
   ```

   dobiven supstitucijskom šifrom, i to Cezarovom šifrom s ključnom riječi. Poznato je da je otvoreni tekst pisan na hrvatskom jeziku, te da je ključna riječ jedan grad u Hrvatskoj. Odredite ključ = (ključna riječ, broj), gdje "broj" označava poziciju u alfabetu od koje počinje ključna riječ.

3. Šifrirajte otvoreni tekst

   ```
   ROSSIGNOL
   ```

   pomoću Vigenèreove šifre s ključnom riječi OSAM.