KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaća 1.31

1. Dekriptirajte šifrat

   ```
   TSVIHEO
   ```

   dobiven Cezarovom šifrom.

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

   ```
   BFMXK TKVKO BFNMW EFABJ MUYUJ KNKUK YJMET PYOSI
   ZAMPS WAFMT KIMOK FDKXM IATKX UEATA PSOXA EAIKJ
   SIKJA OKFMX PSDKX KUBMV XKJEK MPSDK XMDBF NALBM
   BYTKF AVKJM FKVXK XMUJA AKYJM FBFNM WJSEU JKAVJ
   SMFAP SNPSF MPKJX MUJA
   ```

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

3. Dekriptirajte šifrat

   ```
   XAPVS FMYWN AYWCU WPVIP DVGDV QDNUW VPUGW SDBAD
   IENPV PRDED SPAFI AGNOC GUWEC BNOAP EFINC RDUWA
   PEPIN CEDYP NUWQP CVNCR NGVFI NCRNG VFBPA DUWAF
   DINCE PNIAW TCUWT VDBIP ADCBW EAYNG PSBWB NONAW
   ```

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