KRIPTOGRAFIJA

zadaća 1.35

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

   ```
   VZWMD ZWUNO CIWIO WLWYF MUCIP WOAHZ AIOYF JYFIU
   WIJYF WGHYI RAHOY GTCZF MICJC PFMHY XWCXV CLMRI
   OWNSW VCZCZ WFMSW YFMHZ YLXMG OYFWF MOZWH RYCPC
   XWRWU CZMGA UWYJW IMYDR ZWIRY EYDWP C
   ```

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

2. Dekriptirajte šifrat

   ```
   SZPEO WFJZW PGFGB RWUWQ VBHSW RUPKV NHNWG RBCOB
   TRWAP FGWVN HAVBU WFGEB UNPFV XEVEP RUWKB UVUWK
   BEVFG VBTIP POXPQ WGPEP NOVSV GVZTH OUVRP FIBUC
   EBRPO PNPKU WVNOB NVBRP FIUWG FKBUV NOBNQ VHCPE VNH
   ```

   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.

3. Šifrirajte otvoreni tekst

   ```
   LYON PLAYFAIR
   ```

   pomoću Vigenèreove šifre s ključnom riječi PET.