KRIPTOGRAFIJA

Zadaća 1.1

Rok za podizanje zadaće je od 14.03.2003. do (uključivo) 21.03.2003. Rok za predaju ove zadaće je 28.03.2003.

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

   ```
   STOFL FWGHU NPJLF RHMTR HMFNH GWGHU NXFJS FTMTJ
   RHMGH JTXJU FSHNT RRXQT GUTHO ZTKGT KFXIT MHLXQ
   ITGFA XEUHM FLGFA MXHUH OFMFN HGLXI FJTXJ XKFMX
   FJMHL HXQTL GFAMF GHUIT RJFWG FGHUF CJAHU IXOJL
   FCAXG
   ```

   Navedite pet najfrekventnijih slova, te pet najfrekventnijih bigrama u ovom šifratu.

   Odredite ključ $K = (a, b)$ i otvoreni tekst (dekriptirajte šifrat).

2. Dekriptirajte šifrat

   ```
   AKIGZ KIYOB WMIMB IXIFS GYWME IBPHK PMBFS QFSMY
   IMQFS IDHFM NPHBF DVWKS GMWQW ESGHF CIWCA WXGNM
   BIOMI AWKWK ISGMI FSGHK FXCGD BFSIS GBKIH NFWEW
   CINIY WKGDP YIFQI MGFZN KIMNF LFZIE
   ```

   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 ime poznatog matematičara.

3. Šifrirajte otvoreni tekst

   ```
   KERCKHOFFS
   ```

   pomoću Vigenèreove šifre s ključnom riječi ZETA.