KRIPTOGRAFIJA

Zadaća 1.176 X

Rok za podizanje zadaće je od 24.03.2006. do (uključivo) 31.03.2006. Rok za predaju ove zadaće je 07.04.2006.

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

   ```
   YHEVR DOBCL HJZYD JEHRS HYDEY ZIZVY JEOVX LHCZN
   VEBNV EHLXH MYDCN DUVHE VXDEB YDCND UBDGU DCHSH
   DGXDI XOBEI HMDQC BXVEV DIHJZ EVGVY DNDLZ EHMVY
   JEOVX EIHMY DCNDU VDQCV JIHSH ZJEOD CJEUD JUHCB
   EV
   ```

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

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

2. Dekriptirajte šifrat

   ```
   DEBRD GEDJE XEUTW IWBDW GZRTD WAWGZ YPHFY EPHXZ
   RJEGR KZSRU WBDEB WFGEP TWJEB DRBHF GZRRM JESRM
   JEYZG ZGWJT RVWTW JUWTR XDRXH THYZI VEPED WYZJW
   GRFZP ZJEPZ SWTRB DRFGZ R
   ```

   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 izraz (fraza ili riječ) na hrvatskom jeziku.