KRIPTOGRAFIJA

Zadaća 1.212 X

Rok za podizanje zadaće je od 14.03.2007. do (uključivo) 21.03.2007. Rok za predaju ove zadaće je 28.03.2007.

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

   ```
   YTKTM BKBYK DMQTJ DBNPE PQTOT VCLFH TVFLW PCIDE
   QTVTC LAEDH TEPEP HDHTI OCMBO KDMBN BCWLI BQLFI
   DQELF CPMBI BDNPC BJHBW CTILC DIQBF IBIJD HBDHT
   VDWPQ IDVTQ BHDMF DVCDM B
   ```

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

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

2. Dekriptirajte šifrat

   ```
   OYQCA YZLYQ SPLYL DLXKL ZVWXJ YSZXW CTLPL XSCQD
   XZXIK LOACA DYSPC AISDV SLDLO TKLCJ XZACV XKYLC
   VXLZA YQSCQ OQPLD YQSLK JLDLY ASJLJ YXWAC AISLS
   PLJZV BTASD QJANX ASPLD XUASP XSVMV NJABT APQSP
   XTLDX BANQD AYQMA IMLTO XTLJY QLTUV IQJPX IL
   ```

   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.