KRIPTOGRAFIJA

Zadaća 1.90 —

Rok za podizanje zadaće je od 12.03.2004. do (uključivo) 19.03.2004. Rok za predaju ove zadaće je 26.03.2004.

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

   ```
   RGYZD APVDS HYJGJ SVDIO WGPSV IUNIX FGDUK IJAKI
   JSOAP GWGPS ZIYAR NIFIA OYRGX SDINI XFSZA YUYAK
   VGWAV GFAWN IVAKI JAKIJ SOAKG WZGTS YANAE SPIDA
   ONSRJ GWNIL SDIDA PVIGP VDSH
   ```

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

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

2. Dekriptirajte šifrat

   ```
   WCKDO CBHDJ JORCD IUBXO DFHPO FHDEB JODCW ICOLH
   OFKDI DRMEH WCYMJ LDUVW ZPOUB RDZOC BJBKD IOLDD
   XDRWK ODVWN PWIUM UMYOC WRHWZ WAWLD UBUBZ DXOPW
   DVWJP DUBZB LHOFK WVBZW UBJWR HWZOD ZPDHW YXIOV
   MFWHO VW
   ```

   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.