KRIPTOGRAFIJA

Zadaća 2.212 *X*

Rok za podizanje zadaće je od 28.03.2007. do (uključivo) 04.04.2007. Rok za predaju ove zadaće je 11.04.2007.

1. Vigenèreovom šifrom iz otvorenog teksta na hrvatskom jeziku dobiven je šifrat:

   ```
   CVDFN RCFCA VZACW WIJXW ZVGGD DMOWD DUIKS TTJBP
   RFJJX KSJCZ POOGP UINSK DUWNC UPSZB BZDKD PFVCZ
   BFYJI UWMOQ XCWAP FVEMT DITKV PGKXU QQZFB RBBYF
   YZAVI IJTMO SZBUQ QZFBR BTYVC FBFIU DJTPJ EDDWC
   ZZZLL FGZUI QSOCX
   ```

   Odredite najprije duljinu ključne riječi, potom samu ključnu riječ, te dekriptirajte šifrat.

2. Dešifrirajte šifrat:

   ```
   FKFSP TBDZI NUXKA VCMYO DFIMD KJLAY XUCMD BKZLO
   MNZBQ PYFKT ZFMEU QQKDM CMZBF CQJBU KMJZU TRAEL
   RLFDS PPNAD DI
   ```

   šifriran Playfairovom šifrom[1] s ključnom riječi "KUBIZAM".

3. Odredite ključ K u Hillovoj šifri ako je poznato da je $m = 2$, te da otvorenom tekstu

   ```
   nagla skomn anedj eljuc rkven i-- --- ---
   --- --- --- --- --- --- --- ---
   --- --
   ```

   odgovara šifrat

   ```
   ANZQC YUSXU NAVCA DVNOK QHKXY PDWAY BIVMT EFSCV
   EXOVQ ZRQSE PIQXA USXRI NYCSO JGMCL USXHG UZYAD
   MBXRT EAD
   ```

   Dešifrirajte ostatak poruke.

[1] koristite konvenciju "spajanja" `V` i `W` s ključnom riječi te ignorirajte razmake, interpunkciju; hrvatska slova zamijenite kao kod afine šifre