KRIPTOGRAFIJA

Zadaća 2.176 X

Rok za podizanje zadaće je od 07.04.2006. do (uključivo) 14.04.2006. Rok za predaju ove zadaće je 05.05.2006.

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

   ```
   QIKUM FKREH JZXFX EAMUG AEDUE KATCS HLVXT LAFIL
   PBRUE JIGUD ERLEV JJVCS HLVXT LAFGH LRRFN UKRBH
   EAGIE BKFCL UOKUD PBLXN DIUUG FNFMB PDAYV VIQAE
   FDRET PZZPH UIEDT VSKPT SIZTZ MEUUD BOJPB OJRVX
   ADCUD B
   ```

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

2. Dešifrirajte šifrat:

   ```
   LPSCV TAFIM OZFMX KQAZU MSDKX KQAZU MSYVO LPTKQ
   CLPYM SKALE MSNEK ZJZTK QMDUQ KTVNE OTVNQ MENTV
   SCNEE MBQQM BKMYQ KTVSC ZPFSA FTBZA JZDME MPNFM
   QKKZN EKFTV FSFA
   ```

   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

   ```
   ANTYE YKOXK NARQM PJTUC UVWZW PPSSQ ZSFON SLGSJ
   MBMFO HXSUO FWGXC WSFRE FQGUQ XGGEL KOXXM UZMMP
   YBLVN SMP
   ```

   Dešifrirajte ostatak poruke.

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