KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaća 2.28 Mihael Petrinjak

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

   ```
   YCGRC AAZHW YMPHQ EYEDG MMBAR SLITG ASROK KGWOX
   ULDUH NKDTY QMVTX FZRPE CWYEV OGIJE TAOOG XPEKD
   ZVRAB SMXGD DBHNK LDATN KKPHD HXUVS NQKTG WIITA
   HJDYI IAWRX AUDLE SXDJ
   ```

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

2. Šifrirajte otvoreni tekst

   ```
   GIOVANNI SORO
   ```

   pomoću Playfairove šifre s ključnom riječi CRYPTANALYSIS.

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

   ```
   VERNAM
   ```

   odgovara šifrat

   ```
   PJKZYU.
   ```