KRIPTOGRAFIJA

Zadaća 2.4

Rok za podizanje zadaće je od 28.03.2003. do (uključivo) 04.04.2003. Rok za predaju ove zadaće je 11.04.2003.

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

   ```
   CVVHJ MHFRD YLMDV DXSWJ KHFOM ZGMZM REOWV CSMIM
   VVLJV OVSWD MDWIR EESPN RNTDM IMDOG HEQZK DYAMZ
   ICVSD JICUA WQOUV ZDQER HELUA SMOVD OJJVR MIRHI
   MZDDH OMJTD XTRII NVDDI EFZDR KUVOI WDNLN APNEV
   GAJVL DNOFZ MPMZL GAVVM JVMLN LHXIG VCHNE SMOWD
   VLOIP JJREU GVJLH OMYEF FOPZP RXERO UFDGR QOUZC
   LHIGV MRMAP PBLOI RXAQZ KRGIN JDDIA NVSQD JHHOM
   YEFFO MZOWD SDJUC ZOMZS YPNDN UVOON PIQZS WVO
   ```

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

2. Šifrirajte otvoreni tekst

   ```
   HOMOSAPIENS
   ```

   pomoću Playfairove šifre[1] s ključnom riječi PEKINSKAPATKA.

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

   ```
   **WATERL**
   ```

   odgovara šifrat

   ```
   DIOMUJLHKU .
   ```

   Otkrijte koji se znakovi skrivaju iza zvjezdica u otvorenom tekstu.

[1] koristite konvenciju "spajanja" `V` i `W`