KRIPTOGRAFIJA

Zadaća **2.146** *X*

Rok za podizanje zadaće je od 01.04.2005. do (uključivo) 08.04.2005. Rok za predaju ove zadaće je 15.04.2005.

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

```
QZBTG ITDWO VTSFO TNCBU IEDJF ZSTYA AVTBJ BJKQT
NTSFV TPTPU OHQAS RLTEE KVLGJ VSZRX HECZW HKCJE
RXISW VUBMO NRTBQ ITVVB EEURL TEEJD IHJKP AMWVN
BVAMB OEZVT DCJEQ EJMVJ MWVJF JDBEE UAIDJ SLLKX
```

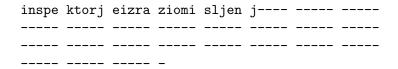
Odredite najprije duljinu ključne riječi, potom samu ključnu riječ, te dekriptirajte šifrat.

2. Dešifrirajte šifrat:

```
LDAME FUDEJ CNKBG PEFBE LDLRV CPFOB CNREO FXRPE
OAGUJ BGYPY AVJBC FBJXS NFNAJ IHCDG EJLRO BUIFK
CQHQF AOSVH VNYFP GAHXO FCBJ
```

šifriran Playfairovom šifrom¹ s ključnom riječi "HONDURAS".

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



odgovara šifrat

LIZMK AKDFD AGRNV QQSYO FYIXT ZBIMY IWEDM RTZZE RQUWY ZGFKZ UBEDC WVMNI EBSJT ADSHU SJINS MFBEB THUUT MTSYZ GFXZQ SRDHU OPUEU BYZEK GRKBO PKMMV KIKGU LKZYK MRJDK B

Dešifrirajte ostatak poruke.

 $^{^1}$ koristite konvenciju "spajanja" ${\tt V}$ i ${\tt W}$ s ključnom riječi te ignorirajte razmake, interpunkciju; hrvatska slova zamijenite kao kod afine šifre