

KRIPTOGRAFIJA

Zadaća 2.90 X

Rok za podizanje zadaće je od 26.03.2004. do (uključivo) 02.04.2004. Rok za predaju ove zadaće je 09.04.2004.

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

```
GMJTS YGQDB ZKWWF BVKBH QKING RSM MB XVKSI WHVNX  
VSDWX CQMDQ CIWBM QJOWN XAONV OIWCK MNGWT UTSSQ  
XBCFT TOOMB BOOBH XBUXH DKS VY ZIBAM YEWCD WQEWU  
TTSMM DT
```

Odredite najprije duljinu ključne riječi, potom samu ključnu riječ, te de-kriptirajte šifrat.

2. Šifrirajte otvoreni tekst

“Na Velikom Brijunu ovih se dana bez ”

pomoću Playfairrove šifre¹ JUTARNJILIST .

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

```
ucrkv enimk rugov imapo sebno u---- -----  
----- ----- ----- ----- -----
```

odgovara šifrat

```
ASPJF JTLEG DNMEV VQCLZ OCXYM GLZHF BFPXB DNNXI  
OBJDE GVHOF ZVCXW LEAZR PXXOW XOEKL OR
```

Dešifrirajte ostatak poruke.

¹koristite konvenciju “spajanja” V i W s ključnom riječi te ignorirajte razmake, interpunkciju; hrvatska slova zamijenite kao kod affine šifre