

# KRIPTOGRAFIJA

## zadaca 2.34

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

AJFAN VCJAS ZQEJO GXASK GAWDK EXGSD MXSKK RIKIP  
JQJAX BMMPO LWEPY KBMPU MRWPB NQHUD MXGVS BMKTS  
GXASK FAMSD SDRAC ANJIB SVBEU GRAJO FCVIY NQKEY  
VRWDX WHSMT WWZK KDSKY KTGvy GBNob WVGgd WSKTK

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

2. Šifrirajte otvoreni tekst

LEN ADLEMAN

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

TSURCE.