

KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaca 2.31

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

FAMJL KIMET DZDRA DKRRZ RTLOJ HFUUL JOMOA RUVEJ
KOYAF SVRRV MOJTV JSWAG NMLCR KACAK QIPJV RTDUR
KFDBV SUWID DJHUG NVLJV RTLKI HPWOX QAIIA DSWEB
ZOMEU MANOS DSPRK MOPJV RTRKR NIXME NGLMU QUJID
OOGRL BJLMR

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

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

VERNAM

odgovara šifrat

XOHL0C.