

KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaca 2.30

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

EVCTJ RMKWY BRTCP KZKBJ AGBIT JSUKV FQOVI UGVYX
QGMFZ UOZCV WFCDB FXKXI OLDUT ZTCTG JVMJY AAZYI
IOAZY IWXIE BBCJD VEZYK LISRJ KALIF QKTVL ZTXQI
TKWYD FCVYU LEXIW PMTBK SQKVM ZFOAK HXCJQ ETBOY VZCV

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

RIVEST

odgovara šifrat

FYNSRH.