

KRIPTOGRAFIJA

zadaća 2.42

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

EPCSB RSPDB SGTAC WECDB MEZDB BTDBB GQUIO ADYML
LDNMF MYPWG VPZVT RXGSK AEEWZ JPQAD WYPLG SSKJX
FYPOH NPTLX BPOIL WJVZB HIZTH YXUQI JXXRX FYFRX
EPEMF SITST GHEIE SYPCM GKCQC WBPAT EDTLX BP

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

2. Šifrirajte otvoreni tekst

EDWARD HEBERN

pomoću Playfairove šifre s ključnom riječi CRYPTOGRAPHY.

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

RIVEST

odgovara šifrat

TZHFIN.