

KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaca 2.63

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

KEKQX XEQIA RURSV ZRHXG DAMIY XTHKN GESQR CNDJN
OEQQR HPNKR DSDHN CILIG XZZSE XPSWY DGHRH GJDAN
KAICP XMZTR DGKIF TUMWI XNZUN CEJQB STHPB VLZAN
QIKQF JSHNE XRZVV EAIMO PZDZV TSMRV WOUQZ SEJZV
ETHZN CJDUM PBZDY YANXE XJZBR AJD

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

2. Šifrirajte otvoreni tekst

VIGENERE

pomoću Playfairrove šifre s ključnom riječi CRYPTOLOGY.

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

VERNAM

odgovara šifrat

NSURKE.