

KRIPTOGRAFIJA

zadaca 1.05

1. Afinom šifrom s ključem K je iz otvorenog teksta na hrvatskom jeziku dobiven sljedeći šifrat:

YBCHT USNCN NCQUX UXUJC PAJLH ZMBIH MLDAT AQCIA
XMXUO IHMLD ATAQM XOOPM AMOLA DHUNT XCZCA ECDUE
CDMYI ULASD OLIUM FAHEO TUHCR NMXCA XULAT MCTFC
NUDSI USMFH UOZHM XUEUI CJSUX ASZXU HAZCT AJCMB
XUPUE AQOYU JUIHM LDMHC DM

Navedite pet najfrekventnijih slova, te pet najfrekventnijih bigrama u ovom šifratu. Odredite ključ $K = (a, b)$ i otvoreni tekst (dekriptirajte šifrat).

2. Dekriptirajte šifrat

UDODR BYEYT WESJN NRCYI JRBUF AJRYR BQUSB CYFUW
ACYCY ARIDL CYLCY AXULU RAXYU MQUEJ CAZBY QYRUR
BUFMC UWAFJ CLASR ANUTU RZUBT UJCYX URYRU ZJETA
IBJUL UMAQJ ZZJQY XJWAX JARIT UFLJO RDXUJ LYEJZ
ETAIB JRDRB UFD

dobiven supstitucijskom šifrom, i to Cezarovom šifrom s ključnom riječi. Poznato je da je otvoreni tekst pisan na hrvatskom jeziku, te da je ključna riječ naslov jedne pjesme.

3. Šifrirajte otvoreni tekst

GIOVANNI SORO

pomoću Vigenèreove šifre s ključnom riječi PET.