

KRIPTOGRAFIJA

zadaća 1.39

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

PQSFM MRKFP EPHAX DOPVF DVXMF HODVG ROFLF UFVPI
KPKFS AXROX GDHOD VGROL RAXOK CPORG RODCP AXVGP
DOPVF SVRVG FCUFV PIKPK FSAXL DAPAX SRMPD CPVXD
MAXMS XUFHA XSXUF VCFLD VWDCD DGCDK XSDTG XLVGF

Navedite pet najfrekventnijih slova, te pet najfrekventnijih bigrama u ovom šifratu.

Odredite ključ $K = (a, b)$ i otvoreni tekst (dekriptirajte šifrat).

2. Dekriptirajte šifrat

COCDO LEBCC FOMDI LBMIM CDFIL IFCIF OCAOI LBDFO
AOLCA OGLOF ILBID MALLQ BFBIM CDFIL ICODO DOCFB
MALFI MLLGB FOKAL KQGBF IMFBD LCFCC MGLIC FFHLB
CCMGL MDGML OAMAD OICDL BDLCL AFDOL BHIOG LBFOK
AMCDB

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

ROSSIGNOL

pomoću Vigenèreove šifre s ključnom riječi PET.