

KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaca 1.28 Mihael Petrinjak

1. Dekriptirajte šifrat

STLTRJY

dobiven Cezarovom šifrom.

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

HEDYM LNVEL DCNCF QLILS TFRHL QIDXT OROLC QFUMF
WQLBD NCLTO RBTFI LNCYF IODNT AYTYD QILXF ITILX
FYTNC TFWGD DMADS LCDYD OMTHT CTEWR MITQD NGFIU
YFQDM DODXI LTOMF OTFQD NGILC NXFIT OMFOS TRUDY TOR

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

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

3. Dekriptirajte šifrat

LZNRV RDFTK XJGVR VFRCH ATKTN RHRXT FZHRZ KKZWT
SZFRZ GCAXZ AGZST KRITH RSTVF RCHAN AUROJ FOZGT
LTOJX RITNZ AUNTG ZJKAL RKTIT KZVRA YHRBA UNTGT
WRNRG JGRDF RFTKR CTOZW TSZFR ZGKOR BALRI YZVFR
CHRFT KOZIS TWTLN OTACF ROTHZ NOZ

dobiven supstitucijskom šifrom, i to Cezarovom šifrom s ključnom riječi. Poznato je da je otvoreni tekst pisan na hrvatskom jeziku. Odredite ključ = (ključna riječ, broj), gdje “broj” označava poziciju u alfabetu od koje počinje ključna riječ.