

KRIPTOGRAFIJA

zadaca 1.34

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

XZAMH FPOZU IZWHB JOUHG ZBIPG FXBJO UJUFS QFQHJ
BIJXF ZWJVH SHUHZ WGZBI PGFXB ZMUFI SZGZU HAFSJ
LFEOF MHIJL FBJOU FQHAZ MJEJF LHGZO UFSTJ BPMHF
POZUI PIWZU TPBXF EHXZQ ZLBHL QHUJM UYJSF WQHIU ZWF

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

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

2. Dekriptirajte šifrat

XWLQF WVIZV VXSXF BDFCB QAQPQ TKXDF JXBQD FQJXI
OCKCK KXIHK XACJA KXBDF UBTUD FCHCF QBQDF QJIKX
UPIRU CHUGI TIWXJ XHGHC DXHBQ XGHXZ CWUBX UBQPJ
QCKIK XXAXO HFUTB UGHFC KPQOC WUFQB KX

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.

3. Šifrirajte otvoreni tekst

JEFFERSON

pomoću Vigenèreove šifre s ključnom riječi PET.