

KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaca 1.30

1. Dekriptirajte šifrat

HSDZSPE

dobiven Cezarovom šifrom.

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

JGFAO NPUFU UFRNK NKNYF SHYWA IVGZA VWEHO HRFZH
KVKNT ZAVWE HOHRV KTTSV HVTWH EANUO KFIFH DFEND
FEVJZ NWHPE TWZNV CHADT ONAFQ UVKFH KNWHO VFOCF
UNEPZ NPVCA NTIAV KNDNZ FYPNK HPIKN AHIFO HYFVG
KNSND HRTJN YNZAV WEVAF EV

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

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

3. Dekriptirajte šifrat

KQCRX CDUFF QGFIC BXRNB UZXKC UCGTN URPQC BXEQH
QNBXH IBNUD EUYQC QNBXP UNIWC GZIUP WQNBX BXFUE
RQNIG EXENQ XEFFU EGTQK CUVBX CQRQE FIBXS UOQWI
FQWNQ BHXTQ NQROQ WQBXW NXRNB UZXUP RCUKF IOIZU BX

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.