

Ime i prezime: *Ivan Kedžo*

KRIPTOGRAFIJA

1. zadaća

1. Dekriptirajte šifrat

CLNFYWLWZ

dobiven Cezarovom šifrom.

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

SFVF YZVL EFYL IZXL YLYL USML CXJD TEFG ZJH

Odredite ključ $K = (a, b)$ i otvoreni tekst (dekriptirajte šifrat), te ako je poznato da je drugi najfrekventniji samoglasnik u otvorenom tekstu E.

3. Dekriptirajte šifrat dobiven supstitucijskom šifrom, i to Cezarovom s ključnom riječi. Poznato je da je otvoreni tekst pisan na hrvatskom jeziku, te da je ključna riječ jedan grad u Hrvatskoj. Odredite ključ=(ključna riječ, broj), gdje "broj" označava poziciju u alfabetu od koje počinje ključna riječ.

RFADO TBBGK KCTLJ TKXFK DGNTV XCXDZ BXKEX EJGHL
FBFZG RXWXE JGHLG JTDRX DGSTH FJMET DTSTA LRXNH
TJBTC XDLTW FDGRX BFCMR XETLX WJMZX FCXLJ GRXDT
KNXMV GBGKL MMFPY FJWM

4. a) Šifrirajte otvoreni tekst

GIOVANNI SORO

pomoću Vigenereove šifre s ključnom riječi PET.

- b) Dešifrirajte šifrat

GJKDNSVNAOW

dobiven pomoću Vigenereove šifre s autoključem. Ključna riječ je DVA.

- c) Dekriptirajte šifrat dobiven Vigenereovom šifrom

NMAAK PZTMJ RTMNJ RIIPN QIVVV WIBRZ NNRQE PQFRV
XOONV VLVBD CNZPP EDJMF DEEGA FOZZV THXJS YQEEE
IOACW NTVOV OWMWA FVJSY WQNHX JSYWQ NHSVR VRZRH
QKOFB VOCZZ DFRZD AQFPN ZDSXM ORTWQ APSZK BUJRR

5. Šifrirajte otvoreni tekst

CHARLES BABBAGE

pomoću Playfairove šifre s ključnom riječi CRYPTOGRAPHY.

6. Odredite ključ K u Hilllovoj šifri, ako je poznato da je $m = 2$, te da otvorenom tekstu

EGOIST

odgovara šifrat

GEIOCT.

7. Dekriptirajte šifrat

TIAG AIOM MTEO UOIR RZAS
KURT LLAT AISM DABR

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku, te da je broj stupaca barem 4 i manji od 8.

8. Dekriptirajte sljedeća dva šifrata

UIHIQZE
SRWGVXHV

ako je poznato da su dobivena istim ključem po pravilu

$$y_i \equiv x_i + k_i \pmod{26}.$$

Poznato je da su oba otvorena teksta riječi na hrvatskom jeziku koje počinju s jednim od slova S, P, N, D.