Ime i prezime: *Vesna Pekić*

KRIPTOGRAFIJA
1. zadaća

1. Dekriptirajte šifrat

LHMXIZIK

dobiven Cezarovom šifrom.

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

XKWK VMWI TKVI JMEI VIVI FXYI LEAC OTKB MAS

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

VCRAP WIIOH HKWJG WHDCH AOMWY DKDAB IDHND NGOEJ
CICBO VDZDN GOEJO GWAVD AOTWE CGLNW AWTWR JVDME
WGIWK DAJWZ CAOVD ICKLV DNWJD ZGLBD CKDJG OVDAW
HMDLY OIOHJ LLCQU CGZL

4. **a)** Šifrirajte otvoreni tekst

ROSSIGNOL

pomoću Vigenereove šifre s ključnom riječi OSAM.

b) Dešifrirajte šifrat

XWIZSKEONGW

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

c) Dekriptirajte šifrat dobiven Vigenereovom šifrom

FETRC HSKEB KKEFC IAAIE IAOMN OBSJR GEJIX GIXKM
PGHEN NEMTV VERHI VVBFW VWXXS XHQRN MYPBL PIWXV
AGTTO FMMGN HNEOT WNBLP OIGYP BLPOI GYKNK MJRKY
ICHWT NHTRR WWJRW RIXIE RVLOE GKKOI TGKRD SMBKI

5. Šifrirajte otvoreni tekst

KERCKHOFFS

pomoću Playfairove šifre s ključnom riječi CRYPTANALYSIS.

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

HEBERN

odgovara šifrat

JMTQCT.

7. Dekriptirajte šifrat

OMMT EOTI AGAI UOIR RZAS
KURT SMDA BRLL ATAI

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

SCIVSVFO
QLWLFCNF

ako je poznato da su dobivena istim ključem po pravilu

$$y_i \equiv x_i + k_i \bmod 26.$$

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