

# KRIPTOGRAFIJA

## 1. zadaća -2

Božić Dragana

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*ORNAMENTALNO*

odgovara šifrat

*JFANSMRQDZSH.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$   
BAEVA SWVCW EWOVK GTOOV MSNAP IOTVD SFCAY ONGAY  
BFJZG GEWVD AYYWJ MEUWS OFCAA SNRGS FIUIA FVDSV  
KGFIU IAFRW WVLWQ OCFLW FHBEL WMWJE EENUB DJWFS  
DZNWZ OHRDN NWAZM SWSWV CAFBJ AERVO QIODN NFBAG  
VRPJA VNZKL DAVAB AVWPA JIIKR OOAERY NBFDA AASNR  
IFRAB ZNWZO HRVAF SJCIB RBBLG DHDFK RGYSK JKSYO  
NGAKI XFKLG FHDIV WAYBJ TGMU LNSQS CVLGO ZBKOC  
EOKJT SECHR PDBHB ZDNVX FKRAP WHCEF NDVKU
3. Napišite program koji za unesenu matricu  $3 \times 3$  i uneseni teks šifrira i dešifrira Hillovom šifrom.
4. Dekriptirajte šifrat  
KADLO AKMOJ DNIPE MNJOE VUDMO  
TMION NNADO AGMXR AOKMM IMAAD  
RXHZK AIIVI RNOOX UNEIL BLTDE  
EOSII UUELC RMVZD E  
ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.
5. Izracunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 01f555b5 \quad i \quad K = 2a123a1f1234.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

## 1. zadaća -3

Bročić Lucija

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*ZRAKOPLOVI*

odgovara šifrat

*FMYSZROBEP.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

SJPLP ENENM TIFEV WIAFE XICMG RZJKP JONQN AEPLO  
QRAIR WTIMM LONIA VPKLE FONQP EEARI UULRL VKPJE  
VWUUL RLVGI NEWMF ATOWM UTSNW MBIAN PUCGS MUMUE  
UIYMO AYAOD CIRIX ILENE NQUNA JPHKA HRZTC ZWKLW  
KDGS LCLBU OQKMS JGMEM ARTAG AFJPO CNWML QPEEA  
TVGMS IYMOA YAGQU EALTR GNSUR TWPWT CWNEB SVINA  
EPLAX JWTWW UTURG MPKSS EWBUL UYIFE TEWWD LSTZS  
TABSE ITOYA ATQTS IODKJ WTCQE IYLPV CPMTF

3. Napišite program koji za unesenu matricu  $3 \times 3$  i uneseni teks šifrira i dešifrira Hillovom šifrom.

4. Dekriptirajte šifrat

PIOLL VODGR UIKOO AMEZO  
IZLJN IDVOI MAIEI MUADS  
REUIK VOAEO KEOKB CIJMM  
HDNNM TMNNT AMNML RRDOX  
NUAAE DAEDX

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izracunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 01ab05b5 \quad i \quad K = 2a234e1f1f34.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

## 1. zadaća -4

Buklijaš Josip

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*POLUOTOK*

odgovara šifrat

*WNSRTTAI.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

TAEYX EOVCZ BIGVK JQAGV MVKMH IOWSP KFCDV AFGAB YR-  
BZG JBIND ABVIB MEXTE GFCDX EFRGV CUMIA ISPKV KJCUM  
IAIOI OVLZN AUFLZ CTTEL ZJIBE EHKGT DJZCE VZNZW AZRDQ  
KISZM VTEOV CDCNB AEUSA IIOGK ZXBAJ SDHJA YKLCL DDSMT  
AVZMM BIINO AGAEB KNXDA DXEFR IIOMT ZNZWA ZRVDC EB-  
CIE ONTLG GEPXK RJVEC JKVVA FGANF JXKLJ CTVIV ZXKTJ TJ-  
JUM LNVNE UVLJL LTKOF BACJT VBOZR PGYTT ZDQSJ XKRDM  
IZCEI KPNKU

3. Napišite program koji za unesenu matricu  $3 \times 3$  i uneseni teks šifrira i dešifrira Hillovom šifrom.

4. Dekriptirajte šifrat

PIOLL VODGR IZLJN IDVOI  
MAIEI MUADS REUIK VOAEO  
KEOKB CIJMM UIKOO AMEZO  
HDNNM TMNNT AMNML RRDOX  
NUAAE DAEDX

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izracunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = a1f55eb5 \quad i \quad K = 2a103a1f123e.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

1. zadaća -5

Ćorić Mate

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*KALKULATOR*

odgovara šifrat

*UEUZRHJDJF.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

LXTDG EGSRE KIYSZ OZAYS BATMZ FDBBP CCRIE AXDPG  
HRTWV OKIFA PGEIT JTCCE YCRIG EXOVA LUEFP NBPCS  
ZOLUE FPNXI GSAEW AMCAE LTLBA ESITB TMTGL AYELE  
NWCEF AROSV TIKWB ACEGS RILNT XTZBA AFDLT ZPYPO  
BDZGP DTLUI SIBML XKEVM TFXSX AYXTG TNPAP IGEXO  
XNXML WCEFA ROKIL ETZXJ XNLIV LNPPH GOEEU GZAEA  
XDPSO JPHAO LTNFK EGKLG IOSUE ICAWE MSAOU LLHDK  
KAUGI AKORO ELHTL WSVBJ PHGIV IRZTN TPFHJ

3. Napišite program koji za unesenu matricu  $3 \times 3$  i uneseni teks šifrira i dešifrira Hillovom šifrom.

4. Dekriptirajte šifrat

IZLJN IDVOI MAIEI MUADS  
REUIK VOAEO KEOKB CIJMM  
UIKOO AMEZO HDNNM TMNNT  
PIOLL VODGR AMNML RRDOX  
NUAAE DAEDX

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izracunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 0bf535b5 \quad i \quad K = 1a1b3c1f1234.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

1. zadaća -6

Livaja Petra

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*GEOMETRIJA*

odgovara šifrat

*GUKWZPWDSB.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

JNPHA EEINI EIWIV STAWI XENMX VZFVP ASNMY AVTLK  
BRRMR SEIDQ LKYIR ZPGWE WSNMA EVERE FUCVL RVP  
VVSFUC VLRRI EIWIQ AKSWI FTJRW IMIRR PQNGJ QUIFE  
LMYIZ APEOZ NIIMX EWEEI NMFNR NPDVA YVZPN ZNOLS  
VDXWL HNLSY OMVMJ NGIPM RVTWR AWPKN NNNQL MAEVE  
TRRMJ MYIZA PEGMF ERPTN RNJYR PHPNX CSYES WVEYA  
VTLWI JNXWS FTLVG IAKJW ESMUC YVEQE KIWSO LJXZO  
EASWE EEOPE APBTJ MOZVJ NXCMP IPPPR NPDFX

3. Napišite program koji za unesenu matricu  $3 \times 3$  i uneseni tekst šifrira i dešifrira Hillovom šifrom.

4. Dekriptirajte šifrat

MAIEI MUADS REUIK VOAEO  
KEOKB CIJMM UIKOO AMEZO  
HDNNM TMNNT IZLJN IDVOI  
PIOLL VODGR AMNML RRDOX  
NUAAE DAEDX

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izračunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = abc555b5 \quad i \quad K = bbb23a1f1234.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

## 1. zadaća -7

Radečić Petra

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*ORNAMENTALNO*

odgovara šifrat

*DINNOYQLZSHR.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

ZNGHI MUIEI MQMIM SBIMI OEVUN VQFDX QSEMG ILTCK  
JZHMI SMQTQ CKGQH ZGGEM MSEMI MLEIE NCSVC RDXQI  
MSNCS VCRZQ UINIY IASNI NBZRN IUQHR GQVOZ QLINM  
BMPIH IFEFZ VQYMO EEMUI EMNVH NGDDI OVQPV HDOCS  
DLNWC HVTIY FMDUZ NXIXU HVKWZ IMNGK VVDQC MIMLE  
KRZUZ MPIHI FEXMN MHPKN ZVZYI PPXDX TSGMI WMEGI  
LTCWQ RDXNS NBBVX IISZW VSUCS YPEYM AINSW TZXQO  
MIIWV EMWFE RPJBZ MFZDR DXTMX QFPGR VXTXW

3. Napišite program u koji korisnik unosi tekst. Program mu nudi šifriranje stupčanom transpozicijskom šifrom tako da tekst slaže u pravokutnik kojem je "razlika stranica" minimalna. Ako nije moguće složiti pravokutnik kojem je neka stranica različita od 1, tekstu se na kraj dodaje jedno slovo  $A$  i radi isti postupak. Izlaz programa je prikaz teksta u pravokutniku i šifrat. Npr. za tekst "OVO JE OGLEDNI TEKST" dobijemo

*OVJOE*

*GLENDI*

*TEKSTA*

i šifrat "OGTVLEOEKJDSIENTOIA".

4. Dekriptirajte šifrat  
REUIK VOAEO KEOKB CIJMM  
UIKOO AMEZO MAIEI MUADS

HDNNM TMNNT IZLJN IDVOI  
PIOLL VODGR AMNML RRDOX  
NUAAE DAEDX

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izračunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 01f55aac \quad i \quad K = 20000a1f1234.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

1. zadaća -8

Radoš Kata

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*ORNAMENTALNO*

odgovara šifrat

*NINNOCEBDEFL.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

OYVRF XJTTS JBBTB CYTBT DOSFC GFP AI FDTWD TAERU  
GKWXX CJBIB RUDBW KVQBX BDTWF XAPXO KNHGR BAIFT  
BCKNH GRWBW JTCSV TPDCS KMOCC SRBWC VASZO BASKX  
QXESE TUPUJ SBNXD OBXJT TWKGW YVNAT DGFZS SSZRC  
AWCHR RSEXJ UWAFO YMSUF WGZGW TBYVU SGSBR WFXAP  
ZBWFO XESET UPMWK XWAZX WGOJX ZMISI ICDXX HBODT  
AERGN CSICC KMQGM SFDOH KCRNH JEOVX PTCCT EOIFY  
JTXHK OJHUP GZGMO XUJAC SHIWU BUAVB SHIL

3. Napišite program u koji korisnik unosi tekst. Program mu nudi šifriranje stupčanom transpozicijskom šifrom tako da tekst slaže u pravokutnik kojem je "razlika stranica" minimalna. Ako nije moguće složiti pravokutnik kojem je neka stranica različita od 1, tekstu se na kraj dodaje jedno slovo  $A$  i radi isti postupak. Izlaz programa je prikaz teksta u pravokutniku i šifrat. Npr. za tekst "OVO JE OGLEDNI TEKST" dobijemo

*OV OJEO*

*GLE DNI*

*TEK STA*

i šifrat "OGTVLEOEKJDSIENTOIA".

4. Dekriptirajte šifrat

NUAAE DAEDX KEOKB CIJMM  
UIKOO AMEZO MAIEI MUADS



REUIK VOA OE HDNNM TMNNT  
IZLJN IDVOI PIOLL VODGR  
AMNML RRDOX

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izračunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 01f55514 \quad i \quad K = 10123a1f1234.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

## 1. zadaća -9

Runjić Mateo

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*ZRAKOPLOVI*

odgovara šifrat

*OLSOPAFHZZH.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

KWNLT EFRLM XIXRT WMAXR VIGMY EXJOP BBLQR AWCJO  
URSVP WXIEZ JORIS INKPE XBLQT EWNPI YUDEJ VOPBR  
TWYUD EJVKI FRUMJ ALBUM YTKAU MFISA NUGGK ZSMYE  
MVWMS AQNMD GIJVV IPEFR LQYNS WNHOA ZEXTG ZOXXJW  
ODYFJ LGLTH MQOMK WEMIM SERAK AXWNO GNOZJ QTEWN  
RVKMK VWMSA QNEQY ESYRR KNKHP TAPOG AWRET FTIRA  
WCJAB JOGUW YTMEE MTKKF CWFUD HWIJE LRUWH LKGXS  
XATFC IXOQN YTUTK VMDOJ OGAQI IQYNV GPEGD

3. Napišite program u koji korisnik unosi tekst. Program mu nudi šifriranje stupčanom transpozicijskom šifrom tako da tekst slaže u pravokutnik kojem je "razlika stranica" minimalna. Ako nije moguće složiti pravokutnik kojem je neka stranica različita od 1, tekstu se na kraj dodaje jedno slovo  $A$  i radi isti postupak. Izlaz programa je prikaz teksta u pravokutniku i šifrat. Npr. za tekst "OVO JE OGLEDNI TEKST" dobijemo

*OVJOEO*

*GLEONI*

*TEKSTA*

i šifrat "OGTVLEOEKJDSENTOIA".

4. Dekriptirajte šifrat

NUAAE DAEDX KEOKB CIJMM  
UIKOO AMEZO AMNML RRDOX

MAIEI MUADS REUIK VOAOE  
HDNNM TMNNT IZLJN IDVOI  
PIOLL VODGR

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izračunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 0aff55b5 \quad i \quad K = 3a12231f1230.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

## 1. zadaća -10

Sladović Sara

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*ZRAKOPLOVI*

odgovara šifrat

*OPYGDMTFXV.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj  $s$  dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

OYYCR RJTWD VVBTE NKNBT GZEZC GIAMC FDWHP NAEUF  
SEWXA NVVIB UFPVW KYBNR BDWHR RAPAZ WHHGU MMCFT  
ENWHH GUMIV JTFDH NPDEF WGOCF DDVWC YLETO BDDWR  
QXHDQ NUPXU EVNXG ZNRJT WHWAW YYYMN DGIKE MSZUN  
MQCHU CEYXJ XHMZO YPDGZ WGCRI NBYYP EASBU HRRAP  
CMIZO XHDQN UPPHW RWACI IAOJA KYCSI LNPRX HEZPN  
AEURZ WSIFN WGQGP DRXOH NNDHH JHZHR PTFNF YOIJJ  
VNXHN ZVBUP JKSGO XXUMW SILHG VUAYM ECHIO

3. Napišite program u koji korisnik unosi tekst. Program mu nudi šifriranje stupčanom transpozicijskom šifrom tako da tekst slaže u pravokutnik kojem je "razlika stranica" minimalna. Ako nije moguće složiti pravokutnik kojem je neka stranica različita od 1, tekstu se na kraj dodaje jedno slovo  $A$  i radi isti postupak. Izlaz programa je prikaz teksta u pravokutniku i šifrat. Npr. za tekst "OVO JE OGLEDNI TEKST" dobijemo

*OVOJEO*

*GLEDMI*

*TEKSTA*

i šifrat "OGTVLEOEKJDSIENTOIA".

4. Dekriptirajte šifrat

KEOKB CIJMM UIKOO AMEZO  
AMNML RRDOX MAIEI MUADS

REUIK VOA OE HDNNM TMNNT  
IZLJN IDVOI PIOLL VODGR  
NUAAE DAEDX

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izračunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 0abc55b5 \quad i \quad K = 2a100a1f1bc4.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

## 1. zadaća -11

Škobić Lucija

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*POLUOTOK*

odgovara šifrat

*JBVFRQGG.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

RXXRE MMSVS IQESD CXIES FORUF FHPZX ICVWC IDDTU  
FZZWZ CIQLA TUCQZ JXQAM ECVWE MDOZO JCKFT BZXIS  
DCJCK FTBVQ MSESU ISCES JBRBE SQQZB XAROR ACSJM  
TWGSD IXOWJ RQQWF OAMMS VWJVZ XXNZI GFHZR HUYTC  
ZLFGT RRTAI WWZUR XOSTU ZFBGV IEXXU RVVAT WEMDO  
BBVUR WGS DI XOOWJ MZZBX VVRIZ ZLXVH KCCMA GDOCI  
DDTGM RVHEC JBTFO SESRG MCQCK IGOUM SSECS TRHHY  
IIAGM OIW XO IZFBR WWJZR VHKWT QXZXB RXLHN

3. Napišite program u koji korisnik unosi tekst. Program mu nudi šifriranje stupčanom transpozicijskom šifrom tako da tekst slaže u pravokutnik kojem je "razlika stranica" minimalna. Ako nije moguće složiti pravokutnik kojem je neka stranica različita od 1, tekstu se na kraj dodaje jedno slovo  $A$  i radi isti postupak. Izlaz programa je prikaz teksta u pravokutniku i šifrat. Npr. za tekst "OVO JE OGLEDNI TEKST" dobijemo

*OV OJEO*

*GLE DNI*

*TEK STA*

i šifrat "OGTVLEOEKJDSENTOIA".

4. Dekriptirajte šifrat

KADLO AKMOJ DNIUN EILBL  
TDEEO SMION NNADO AGMXR

AOKMM IMAAD RXHZK AIIVI  
RNOOX IIUUE LCRMV ZDEPE  
MNJOE VUDMO T

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izračunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 01f55da5 \quad i \quad K = 20223a1f1234.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

## 1. zadaća -12

Tafra Doris

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*POLUOTOK*

odgovara šifrat

*RRXTXEEW.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

OTZLE MJOXM IQBOF WXIBO HIRUC BJJZX FYXQC IAZVO  
FZWSB WIQIW VOCQW FZKAM BYXQE MAKBI JCHBV VZXFO  
FWJCH BVVVQ JOGMU IPYGM JBOXG MQQWX ZUROO WEMJM  
QSIMD IUKYD RQNSH IAMJO XQJWV TZHZI DBJTR HSUVW  
ZLCCV LRTXE YQZUO TQMTU WBDV IBTZO RVSWV QEMAK  
DVVUO SIMDI UKQQJ MWVDR VVOEB TLXSD MWCMX CFICI  
AZVAM RSDGW JBQBQ MESOC OWQCH EIIUM POGWS TODJS  
IIXCO IHWUK KTFBO SYDZR SDMQT QUVZV RXIDP

3. Napišite program šifrira i dešifrira Playfairrovom šifrom. Program prije ispisivanja rezultata treba ispisati matricu slova koja se stvori od unešenog ključa.

4. Dekriptirajte šifrat

RAOKM MIMAA DRXUN EILBL  
TDEEO SMION NNADO AGMXK  
ADLOA KMOJD NIHZK AIIVI  
RNOOX IIUUE LCRMV ZDEPE  
MNJOE VUDMO T

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izračunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 01ac50b5 \quad i \quad K = 00023a1fc234.$$

Napišite sve međukorake!



# KRIPTOGRAFIJA

## 1. zadaća -13

Vučak Ana

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*KALKULATOR*

odgovara šifrat

*KYDRTODYDI.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

KXTOW IFSRP AMXSZ ZPEXS BLJQY FDMRT BCRTU EWDPR  
XVSWV ZAMEA PRUMS JTNSI XCRTW IWOVL BYDFP YRTBS  
ZZBYD FPYNM FSAPM ELCAP BXKBA PIMSB TXJKK AYPBI  
MWCPV EQOSG JMJWB LSIFS RTBRS XTKRE ZFDWJ DOYPZ  
RHYGP OJPTI STRQK XKPLQ SFXDN EXXTR JROAP TWIWO  
XYNQK WCPVE QOKTB ISZXU NRKIV WDTOH GZUIT GZLUE  
WDPDE NOHAZ BXMFK PWOKG IZIYD ICLMI LSAZK PKHDV  
AETGI LASQO EWXXK WSGRN OHGTL MQZTY JTEHJ

3. Napišite program šifrira i dešifrira Playfairrovom šifrom. Program prije ispisivanja rezultata treba ispisati matricu slova koja se stvori od unešenog ključa.

4. Dekriptirajte šifrat

RAOKM MIMAA DRXUN EILBL  
TDEEO SKADL OAKMO JDNIM  
IONNN ADOAG MXHZK AIIVI  
RNOOX IIUUE LCRMV ZDEPE  
MNJOE VUDMO T

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izracunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = a1f505b5 \quad i \quad K = bb123a1f1234.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

## 1. zadaća -14

Vuknić Andrea

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*KALKULATOR*

odgovara šifrat

*IEZNTMRONI.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

PNVLX EKITM BICIB WQACI DIKMD VFJSP GSTQV ABTRO  
YRXMX WBIJQ ROVIX ZVKTE CSTQX EBEXI CUIVR VSPGI  
BWCUI VRVOI KICMN AQSCM CTPRC MJIXR VUKGP QAMCE  
RMEMW AVEUD KIOMD ITEKI TQCNX NVHSA EVFTK ZTORW  
SDDWR LKLYY UQSMP NMMMM XVZAO ACNVO KNTQR QXEBE  
ZVOMP MEMWA VEMQC EXPZR ONPYX TEPTX IWVEY WBIVA  
BTRAF JTXCW CTRVM MXKPW KWJUI YEINE QICWL LPXFS  
BAYWK IBOVE GTYTP MUDSJ TXIQM IVPVV KPJXL

3. Napišite program šifrira i dešifrira Playfairrovom šifrom. Program prije ispisivanja rezultata treba ispisati matricu slova koja se stvori od unešenog ključa.

4. Dekriptirajte šifrat

PEMNJ OEVUD MOTUN EILBL  
TDEEO SKADL OAKMO JDNIM  
IONNN ADOAG MXHZK AIIVI  
RNOOX IIUUE LCRMV ZDERA  
OKMMI MAADR X

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izracunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = abf5c5b5 \quad i \quad K = 2a123a100234.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

1. zadaća -15

Matek David

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*GEOMETRIJA*

odgovara šifrat

*IUUOHSVNTJ.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

LSYEN ZGNWF RDYNE PGVYN GBAHZ AICIK CXWJL VXYUH  
OMTRA PRDFV UHLDT EYDJZ YXWJN ZXJAB SPEAU OIKCN  
EPSPE AUOED GNFFD VMXFF SOLWF FZDTW YNABL VDFSZ  
NRHFM VRJXW ADKRG BJZGN WJSIT SYAIV AAIMA UPTUP  
IYZBU EAGUD XJIHL SPFCH TACTE VYSYH AIPVU JNZXJ  
COEHL RHFMV RJPJS ZTUCK EILDA MUKPC LPLZU BEBLV  
XYUTV EPCFP SONAP FNFLB NPZPE DHBDZ MNFPB GLCIL  
RVUBN BRJRJ JMOOL RXWIE PCLJC DRUYO AKFCO

3. Napišite program šifrira i dešifrira Playfairrovom šifrom. Program prije ispisivanja rezultata treba ispisati matricu slova koja se stvori od unesenog ključa.

4. Dekriptirajte šifrat

PEMNJ OEVUD MOTUN EILBL  
TDEEO SMION NNADO AGMXK  
ADLOA KMOJD NIHZK AIIVI  
RNOOX IIUUE LCRMV ZDERA  
OKMMI MAADR X

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izračunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = abfab5b5 \quad i \quad K = 2a023a101234.$$

Napišite sve međukorake!

# KRIPTOGRAFIJA

1. zadaća -16

Dešpoja Petar

1. Odredite ključ  $K$  u Hillovoj šifri ako je poznato da je  $m = 2$  i da otvorenom tekstu

*GEOMETRIJA*

odgovara šifrat

*EKOSPAZJPB.*

Pokažite međukorake.

2. Dekriptirajte šifrat dobiven Vignereovom šifrom i odredite ključ  $K$  ako je poznato da mu je duljina složen broj s dva netrivialna djelitelja. Opišite međukorake i navedite rezultate.

PXVXX EKSTY BICSB IQACS DUKMD FFVSP GCTCV ABDRA  
YRXWX IBIJA RAVIX JVVTE CCTCX EBOXU CUIFR HSPGS  
BICUI FRHOI KSCYN AQCCY CTPBC YJIXB VGKGP AAYCE  
RWEYW AVOUP KIOWD UTEKS TCCNX XVTSA EFFFK ZTYRI  
SDDGR XKLYI UCSMP XMYMM XFZMO ACXVA KNTAR CXEBO  
ZHOMP WEYWA VOMCC EXZZD ONPIX FEPTH IIVEY GBUVA  
BDRMF JTHCI CTRFM YXKPG KIJUI IEUNE QSCIL LPHFE  
BAYGK UBOVO GFYTP WUPSJ THICM IVZVH KPJHL

3. Napišite program šifrira i dešifrira Playfairrovom šifrom. Program prije ispisivanja rezultata treba ispisati matricu slova koja se stvori od unešenog ključa.

4. Dekriptirajte šifrat

UNEIL BLTDE EOSPE MNJOE  
VUDMO TMION NNADO AGMXK  
ADLOA KMOJD NIHZK AIIVI  
RNOOX RAOKM MIMAA DRXII  
UUELC RMVZD E

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku te ako je broj stupaca broj između 6 i 10.

5. Izračunajte vrijednost DES funkcije  $f(R, K)$  ako je

$$R = 0abb5db5 \quad i \quad K = 0112300f1134.$$

Napišite sve međukorake!