密碼學導論期中上機考

將每一個字母用另一個(可能會同一個)字母來取代但不重複。 更明確的說，選取26個英文字母的一個排列然後施之於明文即得密文。 衆所皆知，代換密碼可由頻率分析破解。然其過程遠比我們所想像的還複雜的多。

請將下述代換密碼文破解：

GFKV LGC RSHH UKIXE FID JIEEKD JFIXICF FID I DXKIO FK GIE ELIVDMVY PU LFK
VMHK GFKV CSL CR LFK XMZKX LFKXK WIOK SJ EKZKV WCGE EHKKA IVD RIL IVD
LFKU YXIBKD IOCVY LFK XKKDE IRLKX LFKO EKZKV CLFKX WCGE SYHU IVD YISVL WIOK
SJ CSL CR LFK VMHK IVD ELCCD PKEMDK LFCEK CV LFK XMZKXPIVA IVD LFK WCGE LFIL
GKXK SYHU IVD YISVL ILK SJ LFK EKZKV EHKKA RIL WCGE LFKV JFIXICF GCAK SJ FK
RKHH IEHKKJ IYIMV IVD FID I EKWCVD DXKIO EKZKV FKIDE CR YXIMV FKIHLFU IVD YCCD
GKXK YXCGMVY CV I EMVYHK ELIHA IRLKX LFKO EKZKV CLFKX FKIDE CR YXIMV EJXCSLKD
LFMV IVD EWCXWFKD PU LFK KIEL GMVD LFK LFMV FKIDE CR YXIMV EGIHHCGKD SJ LFK
EKZKV FKIHLFU RSHH FKIDE LFKV JFIXICF GCAK SJ ML FID PKKV I DXKIO MV LFK
OCXVMVY FME OMVD GIE LXCSPHKD EC FK EKVL RCX IHH LFK OIYMWMIVE IVD GMEK OKV
CR KYUJL JFIXICF LCHD LFKO FME DXKIOE PSL VC CVK WCSHD MVLKXJXKL LFKO RCX FMO
LFKV LFK WFMKR WSJPKIXKX EIMD LC JFIXICF LCDIU M IO XKOMVDKD CR OU EFCXLWCOMVYE
JFIXICF GIE CVWK IVYXU GMLF FME EKXZIVLE IVD FK MOJXMECVKD OK IVD LFK WFMKR
PIAKX MV LFK FCSEK CR LFK WIJLIMV CR LFK YSIXD KIWF CR SE FID I DXKIO LFK
EIOK VMYFL IVD KIWF DXKIO FID I OKIVMVY CR MLE CGV VCG I UCSVY FKPXKG GIE
LFKXK GMLF SE I EKXZIVL CR LFK WIJLIMV CR LFK YSIXD GK LCHD FMO CSX DXKIOE
IVD FK MVLKXJXKLKD LFKO RCX SE YMZMVY KIWF OIV LFK MVLKXJXKLILMCV CR FME DXKIO
IVD LFMVYE LSXVKD CSL KNIWLHU IE FK MVLKXJXKLKD LFKO LC SE M GIE XKELCXKD LC
OU JCEMLMCV IVD LFK CLFKX OIV GIE MOJIHKD EC JFIXICF EKVL RCX TCEKJF IVD FK
GIE QSMWAHU PXCSYFL RXCO LFK DSVYKCV GFKV FK FID EFIZKD IVD WFIVYKD FME WHCLFKE
FK WIOK PKRCXK JFIXICF JFIXICF EIMD LC TCEKJF M FID I DXKIO IVD VC CVK WIV
MVLKXJXKL ML PSL M FIZK FKIXD ML EIMD CR UCS LFIL GFKV UCS FKIX I DXKIO UCS
WIV MVLKXJXKL ML M WIVVCL DC ML TCEKJF XKJHMKD LC JFIXICF PSL YCD GMHH YMZK
JFIXICF LFK IVEGKX FK DKEMXKE LFKV JFIXICF EIMD LC TCEKJF MV OU DXKIO M GIE
ELIVDMVY CV LFK PIVA CR LFK VMHK GFKV CSL CR LFK XMZKX LFKXK WIOK SJ EKZKV
WCGE RIL IVD EHKKA IVD LFKU YXIBKD IOCVY LFK XKKDE IRLKX LFKO EKZKV CLFKX WCGE
WIOK SJ EWXIGVU IVD ZKXU SYHU IVD HKIV M FID VKZKX EKKV ESWF SYHU WCGE MV IHH
LFK HIVD CR KYUJL LFK HKIV SYHU WCGE ILK SJ LFK EKZKV RIL WCGE LFIL WIOK SJ
RMXEL PSL KZKV IRLKX LFKU ILK LFKO VC CVK WCSHD LKHH LFIL LFKU FID DCVK EC
LFKU HCCAKD TSEL IE SYHU IE PKRCXK LFKV M GCAK SJ MV OU DXKIO M EIG EKZKV
FKIDE CR YXIMV RSHH IVD YCCD YXCGMVY CV I EMVYHK ELIHA IRLKX LFKO EKZKV CLFKX
FKIDE EJXCSLKD GMLFKXKD IVD LFMV IVD EWCXWFKD PU LFK KIEL GMVD LFK LFMV FKIDE
CR YXIMV EGIHHCGKD SJ LFK EKZKV YCCD FKIDE M LCHD LFME LC LFK OIYMWMIVE PSL
VCVK CR LFKO WCSHD KNJHIMV ML LC OK LFKV TCEKJF EIMD LC JFIXICF LFK DXKIOE CR
JFIXICF IXK CVK IVD LFK EIOK YCD FIE XKZKIHKD LC JFIXICF GFIL FK ME IPCSL LC
DC LFK EKZKV YCCD WCGE IXK EKZKV UKIXE IVD LFK EKZKV YCCD FKIDE CR YXIMV IXK
EKZKV UKIXE ML ME CVK IVD LFK EIOK DXKIO LFK EKZKV HKIV SYHU WCGE LFIL WIOK
SJ IRLKXGIXD IXK EKZKV UKIXE IVD EC IXK LFK EKZKV GCXLFHKEE FKIDE CR YXIMV
EWCXWFKD PU LFK KIEL GMVD LFKU IXK EKZKV UKIXE CR RIOMVK ML ME TSEL IE M
EIMD LC JFIXICF YCD FIE EFCGV JFIXICF GFIL FK ME IPCSL LC DC EKZKV UKIXE CR
YXKIL IPSVDIVWK IXK WCOMVY LFXCSYFCSL LFK HIVD CR KYUJL PSL EKZKV UKIXE CR
RIOMVK GMHH RCHHCG LFKO LFKV IHH LFK IPSVDIVWK MV KYUJL GMHH PK RCXYCLLKV

IVD LFK RIOMVK GMHH XIZIYK LFK HIVD LFK IPSVDIVWK MV LFK HIVD GMHH VCL PK
XKOKOPKXKD PKWISEK LFK RIOMVK LFIL RCHHCGE ML GMHH PK EC EKZKXK LFK XKIECV LFK
DXKIO GIE YMZKV LC JFIXICF MV LGC RCXOE ME LFIL LFK OILLKX FIE PKKV RMXOHU
DKWMDKD PU YCD IVD YCD GMHH DC ML ECCV IVD VCG HKL JFIXICF HCCA RCX I
DMEWKXVMVY IVD GMEK OIV IVD JSL FMO MV WFIXYK CR LFK HIVD CR KYUJL HKL
JFIXICF IJJCMVL WCOOMEEMCVKXE CZKX LFK HIVD LC LIAK I RMRLF CR LFK FIXZKEL
CR KYUJL DSXMVY LFK EKZKV UKIXE CR IPSVDIVWK LFKU EFCSHD WCHHKWL IHH LFK RCCD
CR LFKEK YCCD UKIXE LFIL IXK WCOMVY IVD ELCXK SJ LFK YXIMV SVDKX LFK ISLFCXMLU
CR JFIXICF LC PK AKJL MV LFK WMLMKE RCX RCCD LFME RCCD EFCSHD PK FKHD MV
XKEKXZK RCX LFK WCSVLXU LC PK SEKD DSXMVY LFK EKZKV UKIXE CR RIOMVK LFIL GMHH
WCOK SJCV KYUJL EC LFIL LFK WCSVLXU OIU VCL PK XSMVKD PU LFK RIOMVK LFK JHIV
EKKOKD YCCD LC JFIXICF IVD LC IHH FME CRRMWMIHE EC JFIXICF IEAKD LFKO WIV GK
RMVD IVUCVK HMAK LFME OIV CVK MV GFCO ME LFK EJMXML CR YCD LFKV JFIXICF EIMD
LC TCEKJF EMVWK YCD FIE OIDK IHH LFME AVCGV LC UCS LFKXK ME VC CVK EC DMEWKXVMVY
IVD GMEK IE UCS UCS EFIHH PK MV WFIXYK CR OU JIHIWK IVD IHH OU JKCJHK IXK LC
ESPOML LC UCSX CXDKXE CVHU GMLF XKEJKWL LC LFK LFXCVK GMHH M PK YXKILKX LFIV UCS
TCEKJF MV WFIXYK CR KYUJL EC JFIXICF EIMD LC TCEKJF M FKXKPU JSL UCS MV WFIXYK
CR LFK GFCHK HIVD CR KYUJL LFKV JFIXICF LCCA FME EMYVKL XMVY RXCO FME RMVYKX IVD
JSL ML CV TCEKJFE RMVYKX FK DXKEEKD FMO MV XCPKE CR RMVK HMVKV IVD JSL I YCHD
WFIMV IXCSVD FME VKWA FK FID FMO XMDK MV I WFIXMCL IE FME EKWCVD MV WCOOIVD IVD
JKCJHK EFCSLKD PKRCXK FMO OIAK GIU LFSE FK JSL FMO MV WFIXYK CR LFK GFCHK HIVD
CR KYUJL LFKV JFIXICF EIMD LC TCEKJF M IO JFIXICF PSL GMLFCSL UCSX GCXD VC CVK
GMHH HMRL FIVD CX RCCL MV IHH KYUJL JFIXICF YIZK TCEKJF LFK VIOK BIJFKVILF JIVKIF
IVD YIZK FMO IEKVILF DISYFLKX CR JCLMJFKXI JXMKEL CR CV LC PK FME GMRK IVD TCEKJF
GKVL LFXCSYFCSL LFK HIVD CR KYUJL TCEKJF GIE LFMXLU UKIXE CHD GFKV FK KVLKXKD LFK
EKXZMWK CR JFIXICF AMVY CR KYUJL IVD TCEKJF GKVL CSL RXCO JFIXICFE JXKEKVWK IVD
LXIZKHKD LFXCSYFCSL KYUJL DSXMVY LFK EKZKV UKIXE CR IPSVDIVWK LFK HIVD JXCDSWKD
JHKVLMRSHHU TCEKJF WCHHKWLKD IHH LFK RCCD JXCDSWKD MV LFCEK EKZKV UKIXE CR IPSVDIVWK
MV KYUJL IVD ELCXKD ML MV LFK WMLMKE MV KIWF WMLU FK JSL LFK RCCD YXCGV MV LFK
RMKHDE ESXXCSVDMVY ML TCEKJF ELCXKD SJ FSYK QSIVLMLMKE CR YXIMV HMAK LFK EIVD CR
LFK EKI ML GIE EC OSWF LFIL FK ELCJJKD AKKJMVY XKWCXDE PKWISEK ML GIE PKUCVD
OKIESXK PKRCXK LFK UKIXE CR RIOMVK WIOK LGC ECVE GKXK PCXV LC TCEKJF PU IEKVILF
DISYFLKX CR JCLMJFKXI JXMKEL CR CV TCEKJF VIOKD FME RMXELPCXV OIVIEEKF IVD EIMD ML
ME PKWISEK YCD FIE OIDK OK RCXYKL IHH OU LXCSPHK IVD IHH OU RILFKXE FCSEKFCHD LFK
EKWCVD ECV FK VIOKD KJFXIMO IVD EIMD ML ME PKWISEK YCD FIE OIDK OK RXSMLRSH MV LFK
HIVD CR OU ESRRKXMVY LFK EKZKV UKIXE CR IPSVDIVWK MV KYUJL WIOK LC IV KVD IVD LFK
EKZKV UKIXE CR RIOMVK PKYIV TSEL IE TCEKJF FID EIMD LFKXK GIE RIOMVK MV IHH LFK
CLFKX HIVDE PSL MV LFK GFCHK HIVD CR KYUJL LFKXK GIE RCCD GFKV IHH KYUJL PKYIV LC
RKKH LFK RIOMVK LFK JKCJHK WXMKD LC JFIXICF RCX RCCD LFKV JFIXICF LCHD IHH LFK
KYUJLMIVE YC LC TCEKJF IVD DC GFIL FK LKHHE UCS GFKV LFK RIOMVK FID EJXKID CZKX
LFK GFCHK WCSVLXU TCEKJF CJKVKD IHH LFK ELCXKFCSEKE IVD ECHD YXIMV LC LFK KYUJLMIVE
RCX LFK RIOMVK GIE EKZKXK LFXCSYFCSL KYUJL IVD IHH LFK GCXHD
WIOK LC KYUJL LC PSU YXIMV RXCO TCEKJF PKWISEK LFK RIOMVK GIE EKZKXK KZKXUGFKXK