

數論與密碼：期中上機考試 (11/4/2015)

姓名：_____ 序號：_____ 學號：_____ 分數：_____

若有需要，每天8:0AM-5:00PM可到數學系電腦教室使用軟體；11/18/2015上課時繳交

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中的每一個字母即得密文。眾所皆知，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。下面密文(可從網頁下載密文檔案)我們保留了字與字中間的空格，這對解密者當然是一大助益，甚至只要單一字母的頻率分析即可達成任務；因為字的結構是猜測的一大提示。請將下述密文破解：

GK FCHD LFKEK LXSLFE LC PK EKHR KZMDKVL LFIL IHH OKV IXK WXKILKD
 KQSIH LFIL LFKU IXK KVDCGKD PU LFKMX WXKILCX GMLF WKXLMV
 SVIHMKVIPHK XMYFLE LFIL IOCVY LFKEK IXK HMRK HMPKXLU IVD LFK JSXESML
 CR FIJMVKEE LFIL LC EKWSXK LFKEK XMYFLE YCZKXVOKVLE IXK MVELMLSLKD
 IOCVY OKV DKXMZMVY LFKMX TSEL JCGKXE RXCO LFK WCVEKVL CR LFK YCZKXVKD LFIL
 GFKVKZKX IVU RCXO CR YCZKXVOKVL PKWCOKE DKELXSWMZK CR LFKEK KVDE ML
 ME LFK XMYFL CR LFK JKCJHK LC IHLKX CX LC IPCHMEF ML IVD LC
 MVELMLSLK VKG YCZKXVOKVL HIUMVY MLE RCSVDILMCV CV ESWF JXMVWMJHKE
 IVD CXIVMBMVY MLE JCGKXE MV ESWF RCXO IE LC LFKO EFIHH EKKO OCEL
 HMAKHU LC KRRKWL LFKMX EIRKLU IVD FIJMVKEE JXSDKVWK MVDKGD GMHH
 DMWLILK LFIL YCZKXVOKVLE HCVY KELIPHMEFKD EFCSHD VCL PK WFIVYKD RCX
 HMYFL IVD LXIVEMKVL WISEKE; IVD IWWCXDMVYHU IHH KNJKXMKVWK FIE EFCGV
 LFIL OIVAMVD IXK OCXK DMEJCEKD LC ESRKX GFMHK KZMHE IXK ESRKXIPHK
 LFIV LC XMYFL LFKOEKHZKE PU IPCHMEFMVY LFK RCXOE LC GFMWF LFKU IXK
 IWSELCOKD PSL GFKV I HCVY LXIMV CR IPSEKE IVD SESXJILMCVE JSXESMVY
 MVZIXMIPHU LFK EIOK CPTKWL KZMVWKE I DKEMYV LC XKDSWK LFKO SVDKX
 IPECHSLK DKEJCLMEO ML ME LFKMX XMYFL ML ME LFKMX DSLU LC LFXCG CRR
 ESWF YCZKXVOKVL IVD LC JXCZMDK VKG YSIXDE RCX LFKMX RSLSXK EKWSXMLU

1. 數算空白以及每個字母出現的次數(頻率)

字母	♡	A	B	C	D	E	F	G	H	I	J	K	L	M
次數	♡													
字母	空格	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
次數														

2. 用單一字母的頻率分析，破密之明文為何(寫在背面)