代換密碼

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；因爲字的結構是猜測的一大提示。請將下述密文破解：

RCSXEWCXK IVD EKZKV UKIXE IYC CSX RILFKXE PXCSYFL RCXLF CV
LFME WCVLMVKVL I VKG VILMCV WCVWKMZKD MV HMPKXLU IVD
DKDMWILKD LC LFK JXCJCEMLMCV LFIL IHH OKV IXK WXKILKD KQSIH

VCG GK IXK KVYIYKD MV I YXKIL WMZMH GIX LKELMVY GFKLFKX
LFIL VILMCV CX IVU VILMCV EC WCVWKMZKD IVD EC DKDMWILKD WIV
HCVY KVDSXK GK IXK OKL CV I YXKIL PILLHKRMKHD CR LFIL GIX
GK FIZK WCOK LC DKDMWILK I JCXLMCV CR LFIL RMKHD IE I
RMVIH XKELMVY JHIWK RCX LFCEK GFC FKXK YIZK LFKMX HMZKE
LFIL LFIL VILMCV OMYFL HMZK ML ME IHLCYKLFKX RMLLMVY IVD
JXCJKX LFIL GK EFCSHD DC LFME

PSL MV I HIXYKX EKVEK GK WIVVCL DKDMWILK GK WIVVCL
WCVEKWXILK GK WIVVCL FIHHCG LFME YXCSVD LFK PXIZK OKV HMZMVY
IVD DKID GFC ELXSYYHKD FKXK FIZK WCVEKWXILKD ML RIX IPCZK
CSX JCCX JCGKX LC IDD CX DKLXIWL LFK GCXHD GMHH HMLLHK
VCLK VCX HCVY XKOKOPKX GFIL GK EIU FKXK PSL ML WIV VKZKX
RCXYKL GFIL LFKU DMD FKXK ML ME RCX SE LFK HMZMVY XILFKX
LC PK DKDMWILKD FKXK LC LFK SVRMVMEFKD GCXA GFMWF LFKU GFC
RCSYFL FKXK FIZK LFSE RIX EC VCPHU IDZIVWKD ML ME XILFKX
RCX SE LC PK FKXK DKDMWILKD LC LFK YXKIL LIEA XKOIMVMVY
PKRCXK SE LFIL RXCO LFKEK FCVCXKD DKID GK LIAK MVWXKIEKD
DKZCLMCV LC LFIL WISEK RCX GFMWF LFKU YIZK LFK HIEL RSHH
OKIESXK CR DKZCLMCV LFIL GK FKXK FMYFHU XKECHZK LFIL LFKEK
DKID EFIHH VCL FIZK DMKD MV ZIMV LFIL LFME VILMCV SVDKX
YCD EFIHH FIZK I VKG PMXLF CR RXKKDCO IVD LFIL YCZKXVOKVL
CR LFK JKCJHK PU LFK JKCJHK RCX LFK JKCJHK EFIHH VCL
JKXMEF RXCO LFK KIXLF

英文字母頻率表 **(Beker and Piper)**

0	1	2	3	4	5	6	7	8	9	10	11	12
a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
.082	.015	.028	.043	.127	.022	.020	.061	.070	.002	.008	.040	.024

13	14	15	16	17	18	19	20	21	22	23	24	25
n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
.067	.075	.019	.001	.060	.063	.091	.028	.010	.023	.001	.020	.001

據此，Beker and Piper 將 26 個英文字母分成五組如下：

1. e 其概率大約爲 0.12
2. t,a,o,i,n,s,h,r 其概率介於 0.06 至 0.09 之間
3. d,l 其概率大約爲 0.04
4. c,u,m,w,f,g,y,p,b 其概率介於 0.015 至 0.023 之間
5. v,k,j,x,q,z 其概率略少於 0.01

二字串及三字串也可能有用。其排序如下：

- 30 個常用的二字串按序爲
  th he in er an re ed on es st en at to nt ha
  nd ou ea ng as or ti is et it ar te se hi of
- 12 個常用的三字串按序爲
  the ing and her ere ent tha nth was eth for dth