Hill 密码的加密、解密与破译

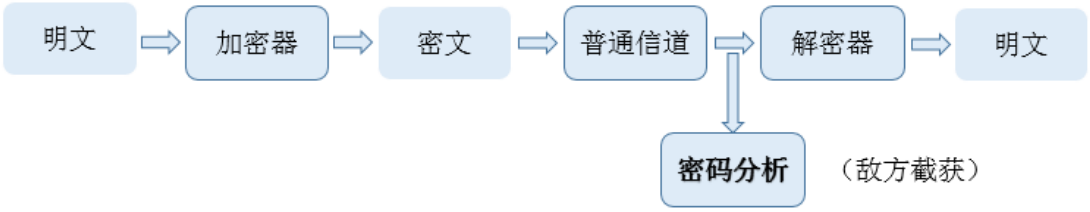
5121209117 徐小博
5122409009 王力功

一、 实验目的

本实验主要涉及代数，利用模运算意义下的矩阵乘法、求逆矩阵、线性无关、线性空间与线性变换等概念和运算，学习 Hill 密码体制的加密、解密和破译过程。

二、 Hill 密码的数学模型

在加密过程中运用的数学手段是矩阵运算，加密过程的具体步骤如下：



1. 根据明文字母的表值，将明文信息用数字表示，设明文信息只需要 26 个字母 A~Z（也可以不止 26 个，如还有数字、标点符号等），通信双方给出这 26 个字母的表值。
2. 选择一个二阶（四阶）可逆整数方阵 A，称为 $Hill_2$（$Hill_4$）密码的加密矩阵，它是这个加密体制的密钥（是加密的关键，仅由通信双方掌握）。
3. 将明文字母依次逐对分组。$Hill_n$ 密码的加密矩阵为 n 阶矩阵，则明文字母 n 个一组。若最后一组不足 n 位，则补充没有实际意义的哑字母，使得每一组都由 n 个明文字母组成。查出每个明文字母的表值，构成一个 n 维列向量 α。
4. A 乘以 α，得一新的 n 维列向量$\beta = A\alpha$，由β的两个向量反查字母表值，得到的 n 个字母即为密文字母。

以上四步即为 Hill 密码的加密过程。而解密过程，就是上述过程的逆过程。

三、 实际问题

问题一：

利用 $Hill_2$ 密码体制的原理，根据给定的 26 个英文字母的乱序表值（如表 1 所示），设

计与监理 $Hill_4$ 密码体制的加密、解密与破译框图并建立必要的计算机程序。设英文 26 个字母以下面的乱序表与 Z_{26} 中的整数对应：

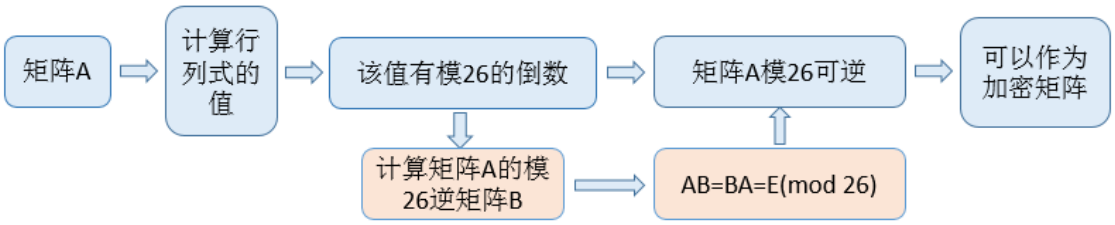
表 1

A	B	C	D	E	F	G	H	I	J	K	L	M
5	23	2	20	10	15	8	4	18	25	0	16	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	3	1	19	6	12	24	21	17	14	22	11	9

（1） 设$A=\begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix}$，验证矩阵 A 能否作为 $Hill_4$ 密码体制的加密矩阵。用框图画出你的验算过程，并编写相应的计算机程序。

问题的解答：

如果 A 为 $Hill_4$ 密码体制的加密矩阵，则 A 必为四阶可逆（模 26 可逆）整数方阵，验算过程如下所示：



通过 Mathematica，我们计算出 det(A) = -1，它有模 26 的倒数，所以矩阵 A 可逆，他可以作为加密矩阵。我们继续用代码验证矩阵 A 的模 26 逆矩阵 B 是否和 A 左乘可得模 26 意义下的单位矩阵。代码如下所示：

```
In[1526]:= A = {{8, 6, 9, 5}, {6, 9, 5, 10}, {5, 8, 4, 9}, {10, 6, 11, 4}};
           A // MatrixForm
           Det@A
           invA = Inverse[A, Modulus → 26];
           invA // MatrixForm
           (A.invA) ~Mod~ 26 // MatrixForm
```

Out[1527]//MatrixForm=

$$\begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix}$$

```
Out[1528]= -1
```

Out[1530]//MatrixForm=

$$\begin{pmatrix} 23 & 20 & 5 & 1 \\ 2 & 11 & 18 & 1 \\ 2 & 20 & 6 & 25 \\ 25 & 2 & 22 & 25 \end{pmatrix}$$

Out[1531]//MatrixForm=

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

从代码中我们再次验证了，矩阵 A 可以作为 $Hill_4$ 密码体制的加密矩阵。

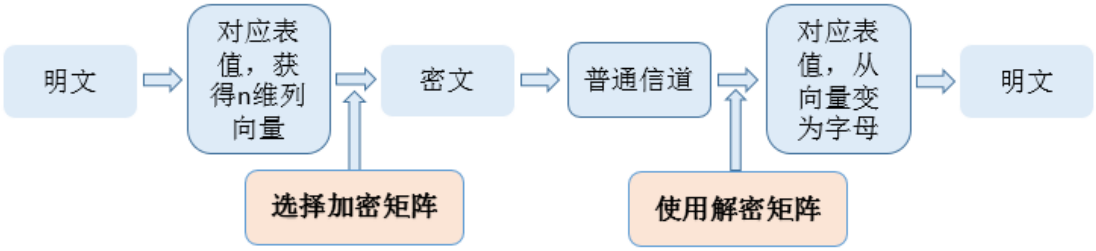
（2） 设明文为

HILL CRYPTOGRAPHIC SYSTEM IS TRADITIONAL

利用上面的表值与加密矩阵为此明文加密，并将得到的密文解密，画出加密与解密过程的框图并编写相应的计算机程序。

问题的解答：

我们先将加密和解密过程用如下框图描述：



然后我们把明文以相邻 4 个字母为一组：

HILL CRYP TOGR APHI CSYS TEMI STRA DITI ONAL

查出每组字母的表值，并构造 4 维列向量：

$$\begin{pmatrix} 4 \\ 18 \\ 16 \\ 16 \end{pmatrix}, \begin{pmatrix} 2 \\ 6 \\ 11 \\ 1 \end{pmatrix}, \begin{pmatrix} 24 \\ 3 \\ 8 \\ 6 \end{pmatrix}, \begin{pmatrix} 5 \\ 1 \\ 4 \\ 18 \end{pmatrix}, \begin{pmatrix} 2 \\ 12 \\ 11 \\ 12 \end{pmatrix}, \begin{pmatrix} 24 \\ 10 \\ 13 \\ 18 \end{pmatrix}, \begin{pmatrix} 12 \\ 24 \\ 6 \\ 5 \end{pmatrix}, \begin{pmatrix} 20 \\ 18 \\ 24 \\ 18 \end{pmatrix}, \begin{pmatrix} 3 \\ 7 \\ 5 \\ 16 \end{pmatrix}$$

用矩阵 A 左乘上述 9 个向量，得到 9 个新的列向量：

$$\begin{pmatrix} 364 \\ 426 \\ 372 \\ 388 \end{pmatrix}, \begin{pmatrix} 156 \\ 131 \\ 111 \\ 181 \end{pmatrix}, \begin{pmatrix} 312 \\ 271 \\ 230 \\ 370 \end{pmatrix}, \begin{pmatrix} 172 \\ 239 \\ 211 \\ 172 \end{pmatrix}, \begin{pmatrix} 247 \\ 295 \\ 258 \\ 261 \end{pmatrix}, \begin{pmatrix} 459 \\ 479 \\ 414 \\ 515 \end{pmatrix}, \begin{pmatrix} 319 \\ 368 \\ 321 \\ 350 \end{pmatrix}, \begin{pmatrix} 574 \\ 582 \\ 502 \\ 644 \end{pmatrix}, \begin{pmatrix} 191 \\ 266 \\ 235 \\ 191 \end{pmatrix}$$

我们再进行模 26 运算，得到新的 9 个列向量：

$$\begin{pmatrix}0\\10\\8\\24\end{pmatrix},\ \begin{pmatrix}0\\1\\7\\25\end{pmatrix},\ \begin{pmatrix}0\\11\\22\\6\end{pmatrix},\ \begin{pmatrix}16\\5\\3\\16\end{pmatrix},\ \begin{pmatrix}13\\9\\24\\1\end{pmatrix},\ \begin{pmatrix}17\\11\\24\\21\end{pmatrix},\ \begin{pmatrix}7\\4\\9\\12\end{pmatrix},\ \begin{pmatrix}2\\10\\8\\20\end{pmatrix},\ \begin{pmatrix}9\\6\\1\\9\end{pmatrix}$$

这些向量对应的字母为

KEGT KPNJ KYXR LAOL MZTP VYTU NHZS CEGD ZRPZ

通过 Mathematica 的代码（如下所示），我们求得了 A 的模 26 逆矩阵：

```
In[1543]:= map = {"A" → 5, "B" → 23, "C" → 2, "D" → 20, "E" → 10, "F" → 15,
              "G" → 8, "H" → 4, "I" → 18, "J" → 25, "K" → 0, "L" → 16,
              "M" → 13, "N" → 7, "O" → 3, "P" → 1, "Q" → 19, "R" → 6, "S" → 12,
              "T" → 24, "U" → 21, "V" → 17, "W" → 14, "X" → 22, "Y" → 11, "Z" → 9};
            invmap = Table[i[[2]] -> i[[1]], {i, map}];

In[1713]:= textP = "HILLCRYPTOGRAPHICSYSTEMISTRADITIONAL";
            Ps = Transpose@(Partition[Characters@textP, 4] /. map);
            Ps // MatrixForm
            A.Ps // MatrixForm
            Qs = (A.Ps) ~Mod~ 26;
            Qs // MatrixForm
            textQ = StringJoin[Transpose@(Qs /. invmap)]
            invA.Qs // MatrixForm
            Ps = (invA.Qs) ~Mod~ 26;
            Ps // MatrixForm
            textP = StringJoin[Transpose@(Ps /. invmap)]
```

然后，在模 26 的意义下，明文的向量矩阵可以被求得：

$$\alpha = A^{-1}\beta(mod\ 26)$$

$$\begin{pmatrix}4\\18\\16\\16\end{pmatrix},\ \begin{pmatrix}2\\6\\11\\1\end{pmatrix},\ \begin{pmatrix}24\\3\\8\\6\end{pmatrix},\ \begin{pmatrix}5\\1\\4\\18\end{pmatrix},\ \begin{pmatrix}2\\12\\11\\12\end{pmatrix},\ \begin{pmatrix}24\\10\\13\\18\end{pmatrix},\ \begin{pmatrix}12\\24\\6\\5\end{pmatrix},\ \begin{pmatrix}20\\18\\24\\18\end{pmatrix},\ \begin{pmatrix}3\\7\\5\\16\end{pmatrix}$$

将得到的明文向量对应表中的字母，得到解密后的明文：

HILL CRYP TOGR APHI CSYS TEMI STRA DITI ONAL

整理得 Hill cryptographic system is traditional.

（3） 已知在上述给定表值下的一段 $Hill_4$ 密码的密文为

JCOW ZLVB DVLE QMXC

对应的明文为

DELAY OPERATIONSU

能否确定相应的加密矩阵？给出你的判断过程。

问题的解答：

由题意，我们知道密文可查表转成矩阵

$$P=\begin{pmatrix}25 & 9 & 20 & 19\\ 2 & 16 & 17 & 13\\ 3 & 17 & 16 & 22\\ 14 & 23 & 10 & 2\end{pmatrix}$$

明文可查表转成矩阵

$$C=\begin{pmatrix}20 & 11 & 6 & 3\\ 10 & 3 & 5 & 7\\ 16 & 1 & 24 & 12\\ 5 & 10 & 18 & 21\end{pmatrix}$$

由于 P=AC，所以加密矩阵 $A=PC^{-1}$，通过 Mathematica 我们可以求出

$$A=\begin{pmatrix}8 & 6 & 9 & 5\\ 6 & 9 & 5 & 10\\ 5 & 8 & 4 & 9\\ 10 & 6 & 11 & 4\end{pmatrix}$$

Mathematica 代码如下所示：

```
In[140]:= textP = "JCOWZLVBDVLEQMXC";
          textC = "DELAYOPERATIONSU";
          c = Transpose@((Characters@textC /. map) ~Partition~ 4);
          c // MatrixForm
          p = Transpose@((Characters@textP /. map) ~Partition~ 4);
          p // MatrixForm
          A = (p.Inverse[c, Modulus → 26]) ~Mod~ 26;
          A // MatrixForm
          invA = Inverse[A, Modulus → 26];
          invA // MatrixForm
          StringJoin[Transpose[((A.c) ~Mod~ 26) /. invmap]]
          StringJoin[Transpose[((invA.p) ~Mod~ 26) /. invmap]]
```

我们为了验证，再次求了 A 模 26 意义下的逆矩阵，然后解密了对应的密文，求出了原来的原文。输出结果如下所示：

```
Out[149]//MatrixForm=
{{23, 20, 5, 1}, {2, 11, 18, 1}, {2, 20, 6, 25}, {25, 2, 22, 25}}

Out[150]= JCOWZLVBDVLEQMXC

Out[151]= DELAYOPERATIONSU
```

所以该题是可以确定相应的加密矩阵的。

问题二：

设已知一份密文为 Hilll$_2$ 密码体系，其中出现频数最高的双字母是 RH 和 NI，而在明文语言中，出现频数最高的双字母 TH 和 HE。由这些信息按表 2 给出的表值能得到什么样的加密矩阵？

表 2

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

问题的解答：

由于加密矩阵 A 为可逆矩阵，所以，当我们知道了两个线性无关的二维明文向量与其对应的密文向量以后，就可以求出它的加密矩阵 A 和 A^{-1}。题中，我们可以看到存在两种可能的对应关系：

$$\binom{\mathrm{R}}{\mathrm{H}} \leftrightarrow \binom{\mathrm{T}}{\mathrm{H}},\ \binom{\mathrm{N}}{\mathrm{I}} \leftrightarrow \binom{\mathrm{H}}{\mathrm{E}}$$

密文 ↔ 明文，密文 ↔ 明文

或是

$$\binom{\mathrm{R}}{\mathrm{H}} \leftrightarrow \binom{\mathrm{H}}{\mathrm{E}},\ \binom{\mathrm{N}}{\mathrm{I}} \leftrightarrow \binom{\mathrm{T}}{\mathrm{H}}$$

由于这两种对应关系的处理是一样的，我们先假设对应关系如第一组所示。按照表 2 可得：

$$\binom{\mathrm{R}}{\mathrm{H}} \leftrightarrow \beta_1 = \binom{17}{7} = \mathrm{A}\alpha_1 \Leftrightarrow \alpha_1 = \binom{19}{7} \leftrightarrow \binom{\mathrm{T}}{\mathrm{H}}$$

$$\binom{\mathrm{N}}{\mathrm{I}} \leftrightarrow \beta_2 = \binom{13}{8} = \mathrm{A}\alpha_2 \Leftrightarrow \alpha_2 = \binom{7}{4} \leftrightarrow \binom{\mathrm{H}}{\mathrm{E}}$$

在模 26 意义下，

$$\det(\beta_1, \beta_2) = \begin{vmatrix} 17 & 13 \\ 7 & 8 \end{vmatrix} (mod\ 26) = 45(mod\ 26) = 19$$

它有模 26 倒数，所以β_1, β_2在模 26 意义下线性无关。同理，

$$\det(\alpha_1, \alpha_2) = \begin{vmatrix} 19 & 7 \\ 7 & 4 \end{vmatrix} (mod\ 26) = 27(mod\ 26) = 1$$

所以α_1, α_2在模 26 意义下也是线性无关的。

记 $P = (\beta_1, \beta_2), C = (\alpha_1, \alpha_2)$，则$P = AC, A = PC^{-1}$。这样，我们就可以利用 Mathemetica 代码求得A和A^{-1}。

Mathematica 代码如下所示：

```
In[623]:= a = {{{"T", "H"}, {"H", "E"}}, {{"R", "H"}, {"N", "I"}}};
          b =
           (Partition[Flatten[((Map[ToCharacterCode, #, 1]) - 65) ~Mod~ 26,
                 2], 2]) & /@ a
          α1 = b[[1, 1]];
          α2 = b[[1, 2]];
          β1 = b[[2, 1]];
          β2 = b[[2, 2]];
          c = Transpose@{α1, α2};
          c // MatrixForm
          p = Transpose@{β1, β2};
          p // MatrixForm
          Det[c] ~Mod~ 26
          Det[p] ~Mod~ 26
          A = (p.Inverse[c, Modulus → 26]) ~Mod~ 26;
          A // MatrixForm
          Det@A
          Divisors[Det@A]
          Divisors@26
          invA = Inverse[A, Modulus → 26];
          invA // MatrixForm
          (A.c) ~Mod~ 26 // MatrixForm
          (invA.p) ~Mod~ 26 // MatrixForm
```

输出的结果为：

```
Out[624]= {{{19, 7}, {7, 4}}, {{17, 7}, {13, 8}}}

Out[630]//MatrixForm=
( 19  7 )
(  7  4 )

Out[632]//MatrixForm=
( 17  13 )
(  7   8 )

Out[633]= 1

Out[634]= 19

Out[636]//MatrixForm=
(  3  24 )
( 24  25 )

Out[637]= -501

Out[638]= {1, 3, 167, 501}

Out[639]= {1, 2, 13, 26}

Out[641]//MatrixForm=
( 15  22 )
( 22   7 )

Out[642]//MatrixForm=
( 17  13 )
(  7   8 )

Out[643]//MatrixForm=
( 19  7 )
(  7  4 )
```

所以解密矩阵$A^{-1}=\begin{pmatrix}15 & 22\\ 22 & 7\end{pmatrix}$

下面我们考虑第二种对应情况，由于思考过程是完全一致的，我们只需将代码改为：

```
In[644]:= a = {{{"T", "H"}, {"H", "E"}}, {{"R", "H"}, {"N", "I"}}};
          b =
           (Partition[Flatten[((Map[ToCharacterCode, #, 1]) - 65) ~Mod~ 26,
                2], 2]) & /@ a
          α1 = b[[1, 2]];
          α2 = b[[1, 1]];
          β1 = b[[2, 1]];
          β2 = b[[2, 2]];
          c = Transpose@{α1, α2};
          c // MatrixForm
          p = Transpose@{β1, β2};
          p // MatrixForm
          Det[c] ~Mod~ 26
          Det[p] ~Mod~ 26
          A = (p.Inverse[c, Modulus → 26]) ~Mod~ 26;
          A // MatrixForm
          Det@A
          Divisors[Det@A]
          Divisors@26
          invA = Inverse[A, Modulus → 26];
          invA // MatrixForm
          (A.c) ~Mod~ 26 // MatrixForm
          (invA.p) ~Mod~ 26 // MatrixForm
```

运行代码，得到输出：

```
Out[645]= {{{19, 7}, {7, 4}}, {{17, 7}, {13, 8}}}
```

Out[651]//MatrixForm=

$$\begin{pmatrix} 7 & 19 \\ 4 & 7 \end{pmatrix}$$

Out[653]//MatrixForm=

$$\begin{pmatrix} 17 & 13 \\ 7 & 8 \end{pmatrix}$$

```
Out[654]= 25

Out[655]= 19
```

Out[657]//MatrixForm=

$$\begin{pmatrix} 11 & 24 \\ 9 & 25 \end{pmatrix}$$

```
Out[658]= 59

Out[659]= {1, 59}

Out[660]= {1, 2, 13, 26}
```

Out[662]//MatrixForm=

$$\begin{pmatrix} 11 & 4 \\ 21 & 9 \end{pmatrix}$$

Out[663]//MatrixForm=

$$\begin{pmatrix} 17 & 13 \\ 7 & 8 \end{pmatrix}$$

Out[664]//MatrixForm=

$$\begin{pmatrix} 7 & 19 \\ 4 & 7 \end{pmatrix}$$

从输出结果中可以看到，其中α_1, α_2和β_1, β_2在模 26 意义下都是线性无关的。所以我们得到了最终解密矩阵$A^{-1} = \begin{pmatrix} 11 & 4 \\ 21 & 9 \end{pmatrix}$

问题三：

如下的密文根据表 3 以 Hill_2 加密，密文为

VIKYNOTC**LK**YRJQETIRECVUZLNOJTUYDIMHRCFITQ

已获知其中相邻字母 LK 表示字母 KE，试破译这份密文。

表 3

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

问题的解答：

加密矩阵与解密矩阵一定是模 26 可逆的，我们可以利用已知的明文与密文向量，寻找一个具有模 26 可逆的解密矩阵。这相当于在模 26 意义下解一个有多组解的线性方程组：

密文向量 LK 对应的表值为$\binom{12}{11}$，对应的明文向量 KE 表值为$\binom{11}{5}$。设解密矩阵

$$\mathrm{B}=\begin{pmatrix}x_1 & x_2\\ x_3 & x_4\end{pmatrix}$$

则有：

$$\begin{pmatrix}x_1 & x_2\\ x_3 & x_4\end{pmatrix}\binom{12}{11}=\binom{11}{5}$$

对四个变量的方程组，在模 26 意义下可以求得通解，求解过程如下面 Mathematica 代码所示：

```
text = "VIKYNOTCLKYRJQETIRECVUZLNOJTUYDIMHRCFITQ";
f = ((ToCharacterCode@#) - 64) ~Mod~ 26 &;
g = FromCharacterCode@(If[# == 0, 26 + 64 + 32, # + 64 + 32]) &;
Ps = Transpose@{#} & /@ Partition[f@text, 2]
a = {{"K", "E"}, {"L", "K"}};
b = (Flatten /@ ToCharacterCode /@ a - 64) ~Mod~ 26
sol = Solve[{b[[2, 1]] * x1 + b[[2, 2]] * x2 == b[[1, 1]],
    b[[2, 1]] * x3 + b[[2, 2]] * x4 == b[[1, 2]]}, {x1, x2, x3, x4},
  Modulus → 26]
Bs = #[[1]] &@({{x1, x2}, {x3, x4}} /. sol /. #) ~Mod~ 26 & /@
    (Table[{C[1] → i, C[2] → j}, {i, 0, 25}, {j, 0, 25}] ~Flatten~ 1);
Length@Bs
Bs =
  Select[Bs,
   Length@(Divisors@Det@# ~Intersection~ {2, 13}) == 0 &];
Length@Bs
Qs = Table[(B.P) ~Mod~ 26, {B, Bs}, {P, Ps}];
Dimensions@Qs
StringJoin@(g /@ (# ~Flatten~ 2)) & /@ Qs;
```

运行结果为：

```
Out[1301]= {{{22}, {9}}, {{11}, {25}}, {{14}, {15}}, {{20}, {3}},
           {{12}, {11}}, {{25}, {18}}, {{10}, {17}}, {{5}, {20}},
           {{9}, {18}}, {{5}, {3}}, {{22}, {21}}, {{0}, {12}},
           {{14}, {15}}, {{10}, {20}}, {{21}, {25}}, {{4}, {9}},
           {{13}, {8}}, {{18}, {3}}, {{6}, {9}}, {{20}, {17}}}

Out[1303]= {{11, 5}, {12, 11}}

Out[1304]= {{x1 → C[1], x2 → 1 + 6 C[1], x3 → C[2], x4 → 17 + 6 C[2]}}

Out[1306]= 676

Out[1308]= 312

Out[1310]= {312, 20, 2, 1}
```

即解密矩阵为

$$\mathrm{B} = \begin{pmatrix} c_1 & 1+6c_2 \\ c_2 & 17+6c_2 \end{pmatrix}$$

对 c_1, c_2 从 0 到 25 进行搜索，可以得到其中所有模 26 可逆的矩阵，有 676 个。

用所得的矩阵与那段密文可求得 676 段明文，从中我们寻找到了有意义的明文为：

CAN YOU MAKE AN OMELETTE WITHOUT BREAKING EGGS S

（你可以在不打碎鸡蛋的情况下做出煎蛋吗？）含义：有得必有失

问题四：

找出元素属于 Z_{26} 的所有可能的 $HILL_2$ 密码加密矩阵，若截获了如下二段密文

UTCQCVFOYQUVMGMGULFOLEYHDUHOPEASWXTIFBAMWT ①

CKYNOHKQMAXJQBHAZWUHDAOQWXIPQZBKMPUTIPVSWSBYXKKWQHADMBDM ②

且已知它们是根据表 3 按 $Hill_2$ 密码体制加密的，你能否将其解密？

问题的解答：

对于所有的二阶矩阵，我们找到所有可逆矩阵，接近 16 万个。Mathematica 代码如下所示：

```
f = ((ToCharacterCode@#) - 64) ~Mod~ 26 &;
g = FromCharacterCode@(If[# = 0, 26 + 64 + 32, # + 64 + 32]) &;

In[1452]:= text1 = "UTCQCVFOYQUVMGMGULFOLEYHDUHOPEASWXTIFBAMWT";
Ps1 = Transpose@{#} & /@ Partition[f@text1, 2];

In[1458]:= text2 =
  "CKYNOHKQMAXJQBHAZWUHDAOQWXIPQZBKMPUTIPVSWSBYXKKWQHADMBDM";
Ps2 = Transpose@{#} & /@ Partition[f@text2, 2];

Bs =
  (Table[{{x1, x2}, {x3, x4}}, {x1, 0, 25}, {x2, 0, 25},
     {x3, 0, 25}, {x4, 0, 25}] ~Flatten~ 3);
Length@Bs
Bs =
  Select[Bs,
   Length@(Divisors@Det@# ~Intersection~ {2, 13}) = 0 &];
Length@Bs

Out[1320]= 456976

Out[1322]= 157248
```

然后我们把密文全部相应一一求得明文，再借助语言的特点来筛选。因为不知道明文是英文还是汉语拼音，所以我们采取了一个策略，就是去掉所有“连续出现 3 个以上辅音字母”的明文，最终得到了几百条结果，最后进行人工识别，把非常明显不会搭配在一起的辅音字母再做进一步的剔除。Mathematica 代码如下所示（由于输出的内容比较多，所以只截取一部分明文显示）：

```
Qs1 = Table[(B.P) ~Mod~ 26, {B, Bs}, {P, Ps1}];
ans1 = StringJoin@(g /@ (# ~Flatten~ 2)) & /@ Qs1;
Dimensions@Qs1
Dimensions@ans1

Out[1325]= {157248, 21, 2, 1}

In[1462]:= Qs2 = Table[(B.P) ~Mod~ 26, {B, Bs}, {P, Ps2}];
ans2 = StringJoin@(g /@ (# ~Flatten~ 2)) & /@ Qs2;
Dimensions@Qs2
Dimensions@ans2

Out[1464]= {157248, 28, 2, 1}

Out[1465]= {157248}
```

```
consonants = Characters["bcdfghjklmnpqrstvwxyz"];
check =
  (For[tmax = 0; t = 0; i = 1, i ≤ Length@#1, i ++,
     If[MemberQ[consonants, #1[[i]]], t = t + 1, t = 0];
     tmax = Max[t, tmax];]; If[tmax > #2, False, True]) &;

res1 = Select[ans1, Characters@# ~ check ~ 3 &];
Length@res1
```

In[1469]:=
```
res2 = Select[ans2, Characters@# ~ check ~ 4 &];
Length@res2
```

Out[1470]=
```
954
```

In[1471]:=
```
res2
```

Out[1471]=
```
{czrinegtenxzjieokwnieugnpibizgcubcvubiqyqduicakznotijomg,
 uzvitewtinlzriioywtiiuwnhinizguuncxunioyodqiuayztojiromg,
 umvitewgialzriibyjtiihwahinizguhncxunioloqqvunymtojiromt,
```

最后得到了两条密文的明文：

WEI RUAN GONG SI JI JIANG TUI CHU XIN YI DAI BEN TENG G ①

微软公司即将推出新一代奔腾

ZAI BEN TENG ZHI HOU WEI RUAN YI JING TUI CHU XIN YI DAI CAO ZUO XI TONG G ②

在奔腾之后微软已经推出新一代操作系统

四、 分工情况

王力功：分析问题，数学建模，编程实现及作图

徐小博：组织文章结构，整理数据及编写，结果分析