# 第5讲 代数变换模型

## 实验目的

1、了解加密解密基本概念；

2、学习并掌握Hill密码加密解密原理；

3、通过案例学习掌握相关算法、模型及其应用。

## 基本概念

**数据加密：**是一门历史悠久的技术，指通过加密算法和加密密钥将明文转变为密文，而解密则是通过解密算法和解密密钥将密文恢复为明文；

**明文：**指原始的或未加密的数据；**密文：**明文加密后的格式，是加密算法的输出信息；**密钥：**数字、字母或特殊符号组成的字符串，用它控制数据加密、解密的过程；**加密算法：**加密所采用的变换方法；

**希尔密码（Hill Cipher）：**是运用基本矩阵论原理的分组替换密码，由Lester S. Hill在1929年发明的。每个字母当作26进制数字：A=0, B=1, C=2… 一串字母当成n维向量，跟一个n×n的矩阵相乘，再将得出的结果MOD 26。基本思想：将n个明文字母通过线性变换转换为n个密文字母。其重要意义是第一次在密码学中用到了代数方法（代数变换、模运算）。

## 实验内容

### 问题1

若发出明文“accomplish the task.”，试根据密钥矩阵K满足的条件给出加密方法和密文，并利用逆矩阵给出相应的解密方法。

#### 问题分析

分析给出明文，有26个英文字母以及空格和句号，因此将这28个字符有序排列对应28个数字，这里我们区别于教材上面的编码实例进行编码：

**Table 1 26个英文字母、空格和句号对应数字编码**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **…** | **X** | **Y** | **Z** | **空格** | **句号** |
| 1 | 2 | 3 | … | 24 | 25 | 26 | 27 | 28 |

设明文为，密钥矩阵（或线性变换）为可逆的矩阵**K**，则经过线性变换得密文。其中



或写成矩阵形式：



其中



解密得明文**M**：



于是，我们设置如下实验步骤：

CLINTONISGOINGTOVISITACOUNTRYINMIDDLEEAST

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 67 | 76 | 73 | 78 | 84 | 79 | 78 | 73 | 83 | 71 | 79 | 73 | 78 | 71 | 84 | 79 | 86 | 73 | 83 | 73 | 84 |
| 65 | 67 | 79 | 85 | 78 | 84 | 82 | 89 | 73 | 78 | 77 | 73 | 68 | 68 | 76 | 69 | 69 | 65 | 83 | 84 | 84 |

3 12 9 14 20 15 14 9 19 7 15 9 14 7 20 15 22 9 19 9 20

1 3 15 21 14 20 18 25 9 14 13 9 4 4 12 5 5 1 19 20 20

15 23 9 0 24 21 9 5 2 21 18 9 12 8 1 13 12 10 5 8

10 16 19 21 1 21 19 1 1 3 19 16 2 1 13 13 16 10 14 8

15 23 9 23 26 24 21 9 5 2 21 18 9 12 8 1 13 16 10 20 14

10 16 19 1 21 1 21 19 1 1 3 19 16 2 1 13 12 10 15 5 8

15 23 9 23 26 24 21 9 5 2 21 18 9 12 8 1 13 16 10 20 14

10 16 19 1 21 1 21 19 1 1 3 19 16 2 1 13 12 10 15 5 8

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 79 | 87 | 73 | 87 | 90 | 88 | 85 | 73 | 69 | 66 | 85 | 82 | 73 | 76 | 72 | 65 | 77 | 80 | 74 | 84 | 78 |
| 74 | 80 | 83 | 65 | 85 | 65 | 85 | 83 | 65 | 65 | 67 | 83 | 80 | 66 | 65 | 77 | 76 | 74 | 79 | 69 | 72 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. 将明文进行数字编码，转化为4\*5的矩阵**M**，若明文的字符长度不够则最后添加空格代替；

2. 通过添加两个未知量*x*和*y*设置合适的密钥矩阵**K**，用辗转相除法解出合适的方程，并进一步求出合适的x和y；

3. 代入求出来的密钥矩阵**K**和明文矩阵**M**，通过公式将明文转化为密文；

4. 通过求解**K-1**并将其代入公式，可以解密反推出明文矩阵**M**。

5. 将明文矩阵对照字母表转化为字符语句。

#### 实验程序

%问题一代码

%%定义密钥矩阵

clc

M = [ 1 13 19 8 1;

3 16 8 5 19;

3 12 0 0 11;

15 9 20 20 27]; %将明文数字编码为矩阵M

syms x y; %定义符号变量

K = [4 x 8 y; %定义密钥矩阵，并设置x和y

12 1 6 9;

3 6 4 6;

2 11 3 8];

det\_K = det(K)

%得到det\_K = -105\*x + 187\*y - 760,辗转相除法得

%[187;105]=[1 1;1 0]\*[1 1;1 0]\*[3 1;1 0]\*[1 1;1 0]\*[1 1;1 0]\*[3 1;1 0]\*[3 1;1 0]

%%求解密钥矩阵

Q = [1 1;1 0]\*[1 1;1 0]\*[3 1;1 0]\*[1 1;1 0]\*[1 1;1 0]\*[3 1;1 0]\*[3 1;1 0]

S = [187;105]

Q\*[1;0] %验证矩阵S是否与其相等

Q\_inv = inv(Q) %Q的逆矩阵

xy0 = [-761\*Q\_inv(1,2) -761\*Q\_inv(1,1)] %方程特解

gs = gcd(S(1),S(2)); %最大公约数

x = xy0(1)-S(1)/gs\*t; %x的通解

y = -(xy0(2)+S(2)/gs\*t); %y的通解

x0 = xy0(1)-S(1)/gs\*(-232)

y0 = -(xy0(2)+S(2)/gs\*(-232))

%求出x0=7，y0=8

K = [4 7 8 8; %定义密钥矩阵，并设置x和y

12 1 6 9;

3 6 4 6;

2 11 3 8];

disp('加密后密文为：')

C = mod(K \* M,28)

disp('解密后明文为：')

M\_ = mod(K\C,28)

#### 实验结果

加密后密文为：

C =

1 24 12 3 21

0 17 24 1 4

11 13 1 6 15

24 2 6 7 12

解密后明文为：

M\_ =

1.0000 13.0000 19.0000 8.0000 1.0000

3.0000 16.0000 8.0000 5.0000 19.0000

3.0000 12.0000 0.0000 28.0000 11.0000

15.0000 9.0000 20.0000 20.0000 27.0000

#### 结果分析

利用辗转相除法设置了一组合适的密钥矩阵（即可逆），分析可得密文和解密后的明文与案例提供答案一致，实验结果正确。

### 问题2

例１ 在某次战争中，假设总指挥部要给前线部队发送信息ＦＩＲＩＮＧ，但需加密后才能发出．双方约定用可逆矩阵



作为加密矩阵，且字母与数字一一对应如Tab-2所示：

**Table 2 字母与数字的对应**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 字母 | A | B | C | D | E | F | G | H | I | J | K | L | M |
| 对应数字 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 字母 | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 对应数字 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

试写出总指挥部发出的密文代码，并给出前线部队收到密文后如何解密．

#### 问题分析

我们将总指挥部要发送的字母信息 ＦＩＲＩＮＧ 转化为明文代码6,9,18,9,14,7。然后得到了明文矩阵



接着通过将明文矩阵**M**转换为密文矩阵**C**：



最后将密文矩阵**C**转换成密文代码15,-3,21,2,16,12发出。前线部队收到密文后可以用解密矩阵**K-1** 采用对应的算法进行解密得明文矩阵M：



再将明文矩阵**M**转换成明文代码6,9,18,9,14,7。对照字母表，前线部队就可以得到总部发来的信息ＦＩＲＩＮＧ。

于是，我们设置如下实验步骤：

1. 将明文进行数字编码，转化为3\*2的矩阵**M**，若明文的字符长度不够则最后添加空格代替；

2. 代入密钥矩阵**K**和明文矩阵**M**，通过公式将明文转化为密文；

3. 通过求解**K-1**并将其代入公式，可以解密反推出明文矩阵**M**。

4. 将明文矩阵对照字母表转化为字符语句。

#### 实验程序

%问题二代码

clc

M = [6 9; %将明文数字编码为矩阵M

9 14;

18 7];

K = [1 -1 1; %定义密钥矩阵K

1 1 -1;

-1 1 1];

disp('加密后密文为：')

C = mod(K\*M,26) %加密密文

disp('解密后明文为：')

M = mod(K\C,26) %解密密文

#### 实验结果

加密后密文为：

C =

15 2

23 16

21 12

解密后明文为：

M =

6 9

9 14

18 7

#### 结果分析

总指挥部给出的密文代码为15,-3,21,2,16,12，前线部队在已知密钥矩阵的情况下可通过求出明文代码6,9,18,9,14,7，然后对照字母表将其转化为字符ＦＩＲＩＮＧ。

### 问题三

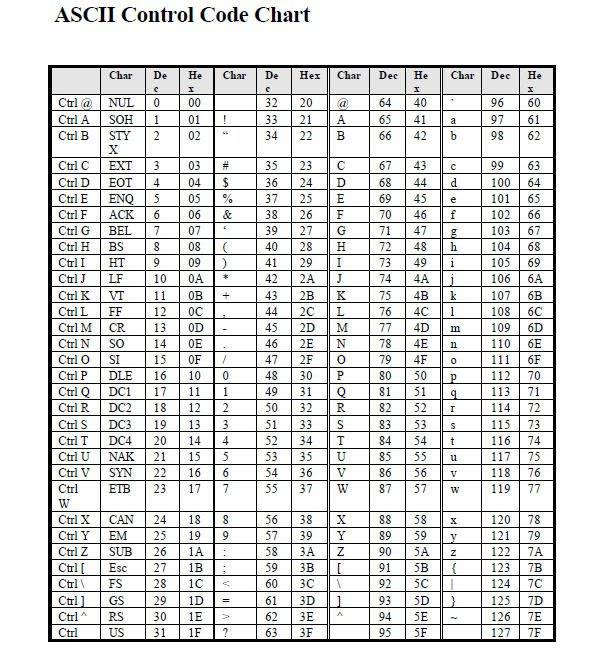
在商业交往中，甲乙两家公司关系非常密切，常常会相互传送商业机密．两公司事先约定用可逆矩阵



作为加密矩阵．现假设甲公司收到来自乙公司的密文Ｆ＞ｉＢＰＬ，请译出原信息。其中Ｆ＞ｉＢＰＬ对应的ASCII代码值分别为70,62,108,66,80,76。

#### 问题分析

根据题目要求，我们将所有字符都转化为ASCII码，一共128个转化字符（如Fig-1所示）：



**Figure 1 ASCII Control Code Chart**

我们将甲公司要发送的信息Ｆ＞ｉＢＰＬ转化为密文代码70,62,108,66,80,76。然后得到了密文矩阵：

**注：假设原信息不含空格**



接着将密文矩阵**C**采用对应的算法进行解密得明文矩阵M：



再将明文矩阵**M**转换成明文66,85,89,73,78,71。对照ASCII字母表（如Fig-1），甲公司就可以得到乙公司发来的信息BUYING。

#### 实验程序

%问题三代码

clc

C = [70 66; %将明文数字编码为矩阵M

62 80;

108 76];

K = [1 -1 1; %定义密钥矩阵K

1 1 -1;

-1 1 1];

disp('解密后明文为：')

M = mod(K\C,128) %解密密文

#### 实验结果

解密后明文为：

M =

66 73

85 78

89 71

#### 结果分析

甲公司在收到密文后可以建立密文矩阵**C**，在已知密钥矩阵K的前提下通过公式可以求出明文矩阵，对照ASCII编码表（如Fig-1）可以推出乙公司发的明文是BUYING。

### 问题四

假设某高层领导人甲有一张机密的黑白图片文件资料：secret文件.jpg（假定在甲电脑Ｄ盘中），要发送给另一个高层领导人乙，为防止外交通信过程中文件信息被第三方截获，发送方甲必须对图片进行加密后才能发出．事先双方约定好了加密矩阵，接收方乙收到密文（假定存放在乙的电脑 Ｅ盘中）后可

用相应的逆矩阵在 ＭＡＴＬＡＢ中解密得到原图片。

#### 问题分析

本题较为开放，网上有很多图片加密方法，这里选择行列加密（即打乱像素矩阵的行列分布）为了能够实时展现代码，这里不选择存储在硬盘里的图片，而是选择网页上的图片（华工校徽）。

#### 实验程序

%问题四代码（参考网上资料）

clc

clear all

photo = imread('https://ss0.bdstatic.com/70cFuHSh\_Q1YnxGkpoWK1HF6hhy/it/u=797069786,413509340&fm=26&gp=0.jpg');

figure;imshow(photo)

title('原图')

[M,N] = size(photo);

Rm = randsample(M,M)';

Mchange = [1:1:M;Rm];

Rn = randsample(N,N)';

Nchange = [1:1:N;Rn];

%打乱行顺序

photo (Mchange(1,:),:) = photo (Mchange(2,:),:);

figure;imshow(photo)

title('行加密后图像')

%打乱列顺序

photo (:,Nchange(1,:)) = photo (:,Nchange(2,:));

figure;imshow(photo)

title('列加密后图像')

%列变换还原

photo (:,Nchange(2,:)) = photo (:,Nchange(1,:));

figure;imshow(photo)

title('列解密后图像')

%行变换还原

photo (Mchange(2,:),:) = photo (Mchange(1,:),:);

figure;imshow(photo)

title('解密后图像')

#### 实验结果

原图：



**Figure 2 原图**

行加密后图像：



**Figure 3 行加密后图像**

列加密后图像：



**Figure 4 列加密后图像**

列解密后图像：



**Figure 5 列解密后图像**

行解密后图像：



**Figure 6 行解密后图像**

#### 结果分析

加密结果较好，对图片处理很到位，解密还原也很出色，实现了需要的功能。

## 实验感想

本次案例学习中，我按时上线接收文件，细致地观看了PPT和电子课本。通过本次对PPT和电子课件附录的学习，我基本理解了加密解密的基本原理、Hill密码加密解密原理以及相关算法、模型及应用的掌握，同时复习了一些矩阵运算知识和数学知识（如辗转相除法）。

我认为这次实验是非常有意义有价值的，通过这次案例学习，我对代数运算的相关知识和应用有了更深的理解。在运行程序的过程中出了一些报错，我经过仔细核对和调试，最终都解决了它们，通过这些解决经验我对常见的报错（比如矩阵维数不对等）有了更进一步的认识，这有助于我在后面的实验中降低出现类似错误出现的概率。在这次实验中，网上查阅到的一些函数的使用方法我都认真记了下来，丰富了我的matlab知识储备。在本次案例学习中，所有的实验均由我独立完成，相关代码和图片结果也都整理到位，代码中存在疑惑的地方以及需要注意的地方均已注释好，以备下次复习时使用。

在这次实验里，我认真完成了四个课堂任务，颇有所获，相信未来几次实验会继续收获不少新知识。

6 许柏城 62号 第五次课

2020-04-09 19:00