# 数学建模第二次作业

**希尔密码的加密与解密**

## 

**摘要：**

希尔密码是一种利用线性代数矩阵运算对字符进行加密的信息加密方法。利用希尔密码的代数模型，我们可以对字符串进行加密和解密，完成作业题目1和2。

**关键词：希尔密码 加密 解密**

**正文：**

**一、问题重述**

**题目1：**

取  ,用A加密meet,再求其逆矩阵，并对其解密。

**题目2：**

有密文如下:goqbxcbuglosnfal；据英文的行文习惯以及获取密码的途径和背景，猜测是两个字母为一组的希尔密码，前四个明文字母是dear，试破译这段秘文。

**二、模型建立**

希尔密码的加密方式如下：

第一步，选择一个n阶可逆矩阵A作为加密矩阵；

第二步，将明文字符按n个一组分组；

第三步，将明文字符按以下表格变换为整数，组成一组列向量；

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

第四步，用加密矩阵左乘每一列向量；

第五步，将新向量的每个分量关于模m取余运算；

第六步，将新向量的每个整数按表格变换为一个字符并合并。

设密文向量为y，明文向量为x，则有y=Ax（mod 26）。由线性代数中的矩阵运算，有A-1y=A-1Ax=x（mod 26），其中A-1是A的逆矩阵（mod 26）。故希尔密码的解密只需用解密矩阵A-1替代加密矩阵A，重复以上步骤即可。

**三、模型求解**

**题目1求解：**

加密矩阵，明文为meet；

由于加密矩阵是2阶的，将明文以2个字符为一组分组，得{me,et}，转化为向量组为；

对向量组左乘A进行加密得

故密文为wysv。

A的逆矩阵为

对密文向量组左乘A-1进行解密得

即解密得到的明文为meet。

**题目2求解：**

该题目中的加密和解密矩阵均未知，但我们知道矩阵是2阶的且密文goqb解密得到dear。设解密矩阵则

利用Python求解得

继续利用Python，对密文中的每2位使用解密矩阵解密，得到原文为dearmacgodforbid。

求解解密矩阵的代码如下：

for a in range(0,26):

    for b in range(0,26):

        for c in range(0,26):

            for d in range(0,26):

                if((7\*a+15\*b)%26==4):

                    if((7\*c+15\*d)%26==5):

                        if((17\*a+2\*b)%26==1):

                            if((17\*c+2\*d)%26==18):

                                print(a,b,c,d)

结果如下：



求解原文的代码如下：

str="goqbxcbuglosnfal"

strm=""

for i in range(0,len(str),2):

    a=(ord(str[i])-96)%26

    b=(ord(str[i+1])-96)%26

    am=(a+b\*5)%26

    bm=(9\*b)%26

    strm+=chr(am+96)

    strm+=chr(bm+96)

print(strm)

结果如下：



**四、结果分析**

题目1的加密结果为wysv，解密结果为meet。

题目2的解密结果为dearmacgodforbid。

**五、模型评价**

利用希尔密码的代数模型，成功对两道题目进行了加密和解密。希尔密码加密矩阵的选取不宜阶数过小或过大，当矩阵阶数仅有2阶时，他人仅需获知明文的4位字符即可破译全部密文，而矩阵阶数较大时，加密和解密的计算不便。

**结论：题目1的加密结果为wysv，解密结果为meet。**

**题目2的解密结果为dearmacgodforbid。**

参考文献：课堂讲授内容