西安交通大学

数学实验报告

希尔密码对信息的加密与解密

Xi'an Jiaotong University

Report on Mathematical Experiments

The Encryption and Decryption of Information

by Hill Cipher

评分表:

班级	学号	姓名	班号	组号	任务	成绩
电类 938	2194323176	胡欣盈	7	52	模型的代码实现	
电类 937	2196123402	何佩阳			建立数学模型	
电类 935	2196123421	刘雪婷			撰写实验报告	

2020 年 7 月 14 日

希尔密码对信息的的加密与解密

一、问题重述

1.1 问题背景

信息安全本身包括的范围很大，大到国家军事政治等机密安全，小范围的当然还包括如防范商业企业机密泄露，个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名，信息认证，数据加密等），直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。在密码学的发展中出现了希尔密码，现对希尔密码做出应用，以希尔密码为原理实现信息的加密与解密。

1.2 目标任务

根据上述基本要求，需要解决以下问题：

（1）运用希尔密码体制对明文进行加密。

（2）运用希尔密码体制对密文进行解密，并验证上述明文的加密结果。

二、符号说明

A	密钥矩阵
x	明文对应的向量
%	求余
mod	

三、问题分析

本题是一个以希尔密码体制为基础的应用问题。问题要求我们运用给定矩阵对明文加密，以及根据已有明文字母对希尔密码加密的密文解密。

四、模型的建立与求解

4.1 希尔密码的加密

4.1.1 模型的整体分析

密码学的发展使密钥极为多变，希尔密码是一种代数密码，其运用的密钥为矩阵。具体操作为：将密文分成 n 个一组，用对应的数字代替，就变成了一个 n 维向量。如果取定一 个 n 阶的非奇异矩阵 A（此矩阵为主要密钥），用 A 去乘每一向量，即可起到加密的效果。解密时，将密文也分成 n 个一组，同样变换成 n 维向量，只需用A^{-1}去乘这些向量，即可变回原先的明文。

4.1.2 建立希尔密码加密模型

（1）选择一个 n 阶可逆矩阵 A 作为加密矩阵；

（2）将明文字符按顺序排列分组；

（3）将明文字符对应一个整数，组成一组列向量；

（4）用加密矩阵左乘每一列向量；

（5）将新向量的每个分量关于模 m 取余运算；

（6）将新向量的每个整数对应于一个字符。

4.1.3 模型求解

已知字母对应的数字为

m-13 e-5 t-20

取$x_1 = \begin{pmatrix}13\\5\end{pmatrix}$, $x_2 = \begin{pmatrix}5\\20\end{pmatrix}$,

$$A \cdot x_1(mod26) = \begin{pmatrix}1 & 2\\0 & 5\end{pmatrix}\begin{pmatrix}13\\5\end{pmatrix}(mod26) = \begin{pmatrix}23\\25\end{pmatrix}(mod26) = \begin{pmatrix}23\\25\end{pmatrix} = \begin{pmatrix}w\\y\end{pmatrix}$$

$$A \cdot x_2(mod26) = \begin{pmatrix}1 & 2\\0 & 5\end{pmatrix}\begin{pmatrix}5\\20\end{pmatrix}(mod26) = \begin{pmatrix}19\\22\end{pmatrix}(mod26) = \begin{pmatrix}19\\22\end{pmatrix} = \begin{pmatrix}s\\v\end{pmatrix}$$

故加密后为 wysv

4.1.4 验证加密过程

$|A| = 5, \therefore |A^{-1}| = 21;$

$A^{-1} = 21\begin{pmatrix}5 & -2\\ 0 & 1\end{pmatrix}(mod26) = \begin{pmatrix}1 & 10\\ 0 & 21\end{pmatrix};$

$\begin{pmatrix}1 & 10\\ 0 & 21\end{pmatrix}\begin{pmatrix}23\\ 25\end{pmatrix}(mod26) = \begin{pmatrix}13\\ 5\end{pmatrix} = \begin{pmatrix}m\\ e\end{pmatrix}$

$\begin{pmatrix}1 & 10\\ 0 & 21\end{pmatrix}\begin{pmatrix}23\\ 25\end{pmatrix}(mod26) = \begin{pmatrix}5\\ 20\end{pmatrix} = \begin{pmatrix}e\\ t\end{pmatrix}$, 解密成功

4.1.5 代码实现

加密：

A=input('矩阵 A：')

B=input('矩阵 x：')

c=A*B%c 为加密后的密码单词在 26 个英文字母中的排序

验证加密过程：

```
function X=A(A,B)
%求解矩阵方程
A=input('请输入矩阵方程的系数矩阵：')
B=input('请输入矩阵方程的常系数矩阵：')
c=[A B];
d=sym(A);
e=sym(B);
[m1,n1]=size(A);
[m2,n2]=size(B);
if ((m1==1)&&(n1==1))||((m2==1)&&(n2==1))
   error('请输入向量')
end
if isequal(B,zeros(m2,1))
   if rank(A)<n1
      X=null(d)
   elseif rank(A)==n1
      X=d\B
   else
      error('一元线性其次方程不存在这种情况');
```

```
    end
  else
    if rank(A)~=rank(c)
      error('非线性方程组在此情况下无解');
    else
      if rank(A)<n1
        X1=null(d)
        X2=sym(d\e)
      elseif rank(A)==n1
        X=sym(d\e)
      else
        error('非线性齐次方程组无这种情况 11')
      end
    end
  end
```

4.2 希尔密码的解密

4.2.1 建立希尔密码解密模型

希尔密码是以矩阵法为基础的,明文与密文的对应由 n 阶矩阵 A 确定。矩阵 A 的阶数是事先约定的，与明文分组时每组字母的字母数量相同，如果明文所含字数 n 不匹配,则最后几个分量可任意补足。根据其特点，具体有以下步骤：

（1）求密匙矩阵的逆矩阵；

（2）再次进行矩阵乘法运算；

（3）对照编码表。

4.2.3 模型求解

根据密文（goqbxcbuglosnfal）；已知两个字母为一组的希尔密码，前四个明文字母是 dear，可得以下等式：

$A\cdot\begin{bmatrix}d\\e\end{bmatrix}=\begin{bmatrix}g\\0\end{bmatrix}$,$A\cdot\begin{bmatrix}a\\r\end{bmatrix}=\begin{bmatrix}q\\b\end{bmatrix}$;即：$A\cdot\begin{bmatrix}4\\5\end{bmatrix}=\begin{bmatrix}7\\15\end{bmatrix}$，$A\cdot\begin{bmatrix}1\\18\end{bmatrix}=\begin{bmatrix}17\\2\end{bmatrix}$；

设 A=$\begin{bmatrix}a & d\\b & c\end{bmatrix}$,则有：$\begin{cases}(4a+5d)\%26=7\\(a+18d)\%26=17\\(4b+5c)\%26=15\\(b+18c)\%26=2\end{cases}$

前两组明文字母 de 和 ar 对应的二维向量是$P_1=\begin{bmatrix}4\\5\end{bmatrix}$,$P_2=\begin{bmatrix}1\\18\end{bmatrix}$

按同一对应整数表，密文中对应这两组的二维向量是：

$q_1 = Ap_1 = \begin{bmatrix}7\\15\end{bmatrix}$，$q_2 = Ap_2 = \begin{bmatrix}17\\2\end{bmatrix}$，$Q = \begin{bmatrix}q_1\\q_2\end{bmatrix}$由此可得

$[Q,P] \rightarrow$（初等行变换）$(mod26) \rightarrow [I,(A^T)^{-1}]$，对应上面有

$$\left(\begin{bmatrix}7 & 15\\17 & 2\end{bmatrix},\begin{bmatrix}4 & 5\\1 & 18\end{bmatrix}\right) \rightarrow \text{初等行变换并取同余} \rightarrow \left(\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix},\begin{bmatrix}1 & 0\\5 & 9\end{bmatrix}\right)$$

可得$(A^{-1})^T = \begin{bmatrix}1 & 0\\5 & 9\end{bmatrix}$，$A^{-1} = \begin{bmatrix}1 & 5\\0 & 9\end{bmatrix}$

利用这一逆矩阵，可对截获密文进行解密，破译出的电文是

Dear Mac God forbid

4.2.4 代码实现

```
clc;
clear;
syms a b c d;
[a,b,c,d]=solve('4*a+5*d=7(mod26)','4*b+5*c=15(mod26)','a+18*d=17(mod26)','b+18*c=2(mod 26)',a,b,c,d)
```

4.3 模型的整体分析

希尔密码算法中有两个非常重要的条件。第一个条件是字符与数字对应表，当加密矩阵的阶数 n 越大,破译的难度就会增大,计算量也大.第二个条件是加密矩阵,如何定义、求解这个矩阵对于密码的加密和破译至关重要。

从破译密码的角度来看，传统的密码可从统计出来的字符频率中找到规律，进而找出破译的突破口。希尔密码算法则完全克服了这一缺陷，它通过采用线性代数中的矩阵乘法运算和逆运算，能够较好地抵抗频率分析，很难被攻破。

希尔密码体系为破译者至少设置了三道关口，加大了破译难度。破译希尔密码的关键是猜测文字被转换成几维向量、所对应的字母表是怎样排列的，更为重要的是要设法获取加密矩阵 A。要破解密码，向量的维数、字母的排列表和加密矩阵三者缺一不可。希尔密码不失为一种简便高效的密码。

五、参考文献

[1]韩中庚，数学建模方法及应用（第二版），2009，北京：高等教育出版社

[2]李继成，数学实验（第二版），2014，北京：高等教育出版社

[3]姜启源、谢金星、叶俊，数学模型（第四版），2011，北京：高等教育出版社