

# Hill密码的加密、解密与破译

李青林, 5110309074

郑辉煌, 5110209289

## 实验任务1

### 问题描述

在问题(2)中, 若已知密文前4个字母OJWP分别代表TACO, 问能否将此段密码破译?

### 解答

密文:  $\begin{pmatrix} O \\ J \end{pmatrix} \rightarrow$  明文:  $\begin{pmatrix} T \\ A \end{pmatrix}$ , 密文:  $\begin{pmatrix} W \\ P \end{pmatrix} \rightarrow$  明文:  $\begin{pmatrix} C \\ O \end{pmatrix}$

$$\begin{pmatrix} O \\ J \end{pmatrix} \leftrightarrow \beta_1 = \begin{pmatrix} 15 \\ 10 \end{pmatrix} = A\alpha_1 \leftrightarrow \alpha_1 = \begin{pmatrix} 20 \\ 1 \end{pmatrix} \leftrightarrow \begin{pmatrix} T \\ A \end{pmatrix}$$

$$\begin{pmatrix} W \\ P \end{pmatrix} \leftrightarrow \beta_2 = \begin{pmatrix} 23 \\ 16 \end{pmatrix} = A\alpha_2 \leftrightarrow \alpha_2 = \begin{pmatrix} 3 \\ 15 \end{pmatrix} \leftrightarrow \begin{pmatrix} C \\ O \end{pmatrix}$$

$$\det(\beta_1, \beta_2) = \begin{vmatrix} 15 & 23 \\ 10 & 16 \end{vmatrix} = 10$$

$\gcd(10, 26) = 2 \Rightarrow \beta_1, \beta_2$ 在模26下线性相关

因此无法解密

## 实验任务2

### 问题描述

设英文26个字母以下面乱序表与 $Z_{26}$ 中的整数对应:

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<sub>4</sub>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给此明文加密, 并将得到的密文解密。
3. 已知在上述给定表值下的一段Hill<sub>4</sub>密码的密文为  
JCOW ZLVB DVLE QMXC  
对应的明文为  
DELAY OPERATIONSU  
能否确定加密矩阵?

### 解答

1.  $\det(A) = 25 \pmod{26}$   
 $\gcd(25, 26) = 1 \implies A$ 在模26下可逆  
因此 $A$ 可以作为加密矩阵
2. 对明文分组:  
HILL CRYP TOGR APHI CSYS TEMI STRA DITI ONAL  
构造4维向量  
 $\begin{pmatrix} 18 \\ 25 \\ 13 \\ 13 \end{pmatrix}, \begin{pmatrix} 20 \\ 12 \\ 9 \\ 19 \end{pmatrix}, \begin{pmatrix} 21 \\ 1 \\ 4 \\ 12 \end{pmatrix}, \begin{pmatrix} 23 \\ 19 \\ 18 \\ 25 \end{pmatrix}, \begin{pmatrix} 20 \\ 24 \\ 9 \\ 24 \end{pmatrix}, \begin{pmatrix} 21 \\ 15 \\ 7 \\ 25 \end{pmatrix}, \begin{pmatrix} 24 \\ 21 \\ 12 \\ 23 \end{pmatrix}, \begin{pmatrix} 10 \\ 25 \\ 21 \\ 25 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 23 \\ 13 \end{pmatrix}$   
用 $A$ 左乘得

$$\begin{pmatrix} 8 \\ 8 \\ 17 \\ 5 \end{pmatrix}, \begin{pmatrix} 18 \\ 21 \\ 13 \\ 5 \end{pmatrix}, \begin{pmatrix} 10 \\ 15 \\ 3 \\ 22 \end{pmatrix}, \begin{pmatrix} 13 \\ 25 \\ 18 \\ 18 \end{pmatrix}, \begin{pmatrix} 11 \\ 23 \\ 24 \\ 19 \end{pmatrix}, \begin{pmatrix} 4 \\ 0 \\ 10 \\ 9 \end{pmatrix}, \begin{pmatrix} 21 \\ 25 \\ 23 \\ 18 \end{pmatrix}, \begin{pmatrix} 24 \\ 16 \\ 13 \\ 9 \end{pmatrix}, \begin{pmatrix} 12 \\ 18 \\ 4 \\ 21 \end{pmatrix}$$

查表得密文为:

IJMM DSZQ UPHS BQIJ DTZT UFNJ TUSB EJUJ POBM

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

用 $A^{-1}$ 左乘密文向量得

$$\begin{pmatrix} 18 \\ 25 \\ 13 \\ 13 \end{pmatrix}, \begin{pmatrix} 20 \\ 12 \\ 9 \\ 19 \end{pmatrix}, \begin{pmatrix} 21 \\ 1 \\ 4 \\ 12 \end{pmatrix}, \begin{pmatrix} 23 \\ 19 \\ 18 \\ 25 \end{pmatrix}, \begin{pmatrix} 20 \\ 24 \\ 9 \\ 24 \end{pmatrix}, \begin{pmatrix} 21 \\ 15 \\ 7 \\ 25 \end{pmatrix}, \begin{pmatrix} 24 \\ 21 \\ 12 \\ 23 \end{pmatrix}, \begin{pmatrix} 10 \\ 25 \\ 21 \\ 25 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 23 \\ 13 \end{pmatrix}$$

查表即可得明文

3. 对明文分组:

DELA YOPE RATI ONSU

明文向量:

$$\alpha_1 = \begin{pmatrix} 20 \\ 10 \\ 16 \\ 5 \end{pmatrix}, \alpha_2 = \begin{pmatrix} 11 \\ 3 \\ 1 \\ 10 \end{pmatrix}, \alpha_3 = \begin{pmatrix} 6 \\ 5 \\ 24 \\ 18 \end{pmatrix}, \alpha_4 = \begin{pmatrix} 3 \\ 7 \\ 12 \\ 21 \end{pmatrix}$$

$$\det(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \begin{vmatrix} 25 & 9 & 20 & 19 \\ 2 & 16 & 17 & 13 \\ 3 & 17 & 16 & 22 \\ 14 & 23 & 10 & 2 \end{vmatrix} = 15 \pmod{26}$$

$\gcd(26, 15) = 1 \Rightarrow \alpha_1, \alpha_2, \alpha_3, \alpha_4$ 在模26下线性无关

密文向量:

$$\beta_1 = \begin{pmatrix} 25 \\ 2 \\ 3 \\ 14 \end{pmatrix}, \beta_2 = \begin{pmatrix} 9 \\ 16 \\ 17 \\ 23 \end{pmatrix}, \beta_3 = \begin{pmatrix} 20 \\ 17 \\ 16 \\ 10 \end{pmatrix}, \beta_4 = \begin{pmatrix} 19 \\ 13 \\ 22 \\ 2 \end{pmatrix}$$

$$\det(\beta_1, \beta_2, \beta_3, \beta_4) = \begin{vmatrix} 25 & 9 & 20 & 19 \\ 2 & 16 & 17 & 13 \\ 3 & 17 & 16 & 22 \\ 14 & 23 & 10 & 2 \end{vmatrix} = 11 \pmod{26}$$

$\gcd(26, 11) = 1 \Rightarrow \beta_1, \beta_2, \beta_3, \beta_4$ 在模26下线性无关

设加密矩阵为 $A$ ,则有 $A(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\beta_1, \beta_2, \beta_3, \beta_4)$

设 $C = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $P = (\beta_1, \beta_2, \beta_3, \beta_4)$

$$A = PC^{-1} = \begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix}$$