

# 希尔密码

Hill Cipher

刘卓

## 1 矩阵的模运算

矩阵的模运算 (Modulo arithmetic on matrices)。令  $A, B$  是  $m \times n$  的矩阵，矩阵元素都为整数。如果

$$a_{i,j} \equiv b_{i,j} \pmod{m}$$

对于全部的  $a_{i,j}, b_{i,j}$ . 则  $A$  and  $B$  是模  $m$  的同余. 记作  $A \equiv B \pmod{m}$ .

如果存在  $A, B$  是  $n \times n$  矩阵，其元素都为整数，使得

$$AB = I \pmod{m} \text{ 和 } BA = I \pmod{m},$$

那么  $A^{-1} = B \pmod{m}$ ,  $B$  是  $A$  模  $m$  的逆。

**例 1**

令  $m = 5$ ,  $A = \begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix}$  和  $B = \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}$ .

$$\begin{aligned} A + 2B \pmod{5} &= \begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 2 & 4 \\ \textcolor{red}{6} & 4 \end{bmatrix} \pmod{5} \\ &= \begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 2 & 4 \\ \textcolor{red}{1} & 4 \end{bmatrix} \pmod{5} \\ &= \begin{bmatrix} 4 & 7 \\ 3 & 5 \end{bmatrix} \pmod{5} \\ &= \begin{bmatrix} 4 & 2 \\ 3 & 0 \end{bmatrix} \pmod{5} \end{aligned}$$

$$\begin{aligned} BA \pmod{5} &= \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix} \pmod{5} \\ &= \begin{bmatrix} 6 & 5 \\ 10 & 11 \end{bmatrix} \pmod{5} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{5} \end{aligned}$$

## 2 矩阵行列式的模

矩阵行列式 (determinant)。

$$\det(A) \bmod m$$

例 2

$$A = \begin{bmatrix} 3 & 4 \\ -9 & 8 \end{bmatrix} \bmod 10$$

$$\det(A) = ad - bc = (3)(8) - (-9)(4) = 60 = 0 \bmod 10$$

## 3 希尔密码

希尔密码 (Hill cipher) 是一种分组密码，将成对的明文字母通过转换加密：

$$Y = AX \bmod 26$$

其中 A 是一个  $2 \times 2$  的可逆矩阵 (invertible matrix) 并且  $\bmod 26$ 。

模 26 的逆：

$$\begin{aligned} 1^{-1} &\equiv 1(\bmod 26) & 3^{-1} &\equiv 9(\bmod 26) \\ 9^{-1} &\equiv 3(\bmod 26) & 5^{-1} &\equiv 21(\bmod 26) \\ 21^{-1} &\equiv 5(\bmod 26) & 7^{-1} &\equiv 15(\bmod 26) \\ 15^{-1} &\equiv 7(\bmod 26) & 11^{-1} &\equiv 19(\bmod 26) \\ 19^{-1} &\equiv 11(\bmod 26) & 17^{-1} &\equiv 23(\bmod 26) \\ 23^{-1} &\equiv 17(\bmod 26) & 25^{-1} &\equiv 25(\bmod 26) \end{aligned}$$

例 3

令  $A = \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix}$ ，使用希尔密码加密明文 “MISSING”。

解：

0	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
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

$$\begin{aligned} \begin{bmatrix} M \\ I \end{bmatrix} &\rightarrow \begin{bmatrix} 12 \\ 8 \end{bmatrix} \rightarrow AX \bmod 26 \rightarrow \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix} \begin{bmatrix} 12 \\ 8 \end{bmatrix} \bmod 26 \rightarrow \begin{bmatrix} 368 \\ 172 \end{bmatrix} \bmod 26 \rightarrow \begin{bmatrix} 4 \\ 16 \end{bmatrix} \rightarrow \begin{bmatrix} E \\ Q \end{bmatrix} \\ \begin{bmatrix} S \\ S \end{bmatrix} &\rightarrow \begin{bmatrix} 18 \\ 18 \end{bmatrix} \rightarrow \begin{bmatrix} 6 \\ 2 \end{bmatrix} \rightarrow \begin{bmatrix} G \\ C \end{bmatrix} \\ \begin{bmatrix} I \\ N \end{bmatrix} &\rightarrow \begin{bmatrix} 8 \\ 13 \end{bmatrix} \rightarrow \begin{bmatrix} 7 \\ 23 \end{bmatrix} \rightarrow \begin{bmatrix} H \\ X \end{bmatrix} \\ \begin{bmatrix} G \\ K \end{bmatrix} &\rightarrow \begin{bmatrix} 6 \\ 10 \end{bmatrix} \rightarrow \begin{bmatrix} 2 \\ 12 \end{bmatrix} \rightarrow \begin{bmatrix} C \\ M \end{bmatrix} \end{aligned}$$

遇到明文长度为奇数时，可以规定某个字母为填充项。这里使用字母 **K** 作为填充项。  
最后密文为：EQGCHXCM

□

希尔密码解密为： $X = A^{-1}Y \bmod 26$

**例 4**

解密"ZGWQ", 令  $A = \begin{bmatrix} 3 & 7 \\ 9 & 10 \end{bmatrix}$

解：

$$\begin{aligned}
 A^{-1} &= \frac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \bmod 26 \\
 &= \det(A)^{-1} \cdot \begin{bmatrix} 10 & -7 \\ -9 & 3 \end{bmatrix} \bmod 26 \\
 &= \det(A)^{-1} \begin{bmatrix} 10 & 19 \\ 17 & 3 \end{bmatrix} \bmod 26 \\
 &= (-33 \bmod 26)^{-1} \times \begin{bmatrix} 10 & 19 \\ 17 & 3 \end{bmatrix} \bmod 26 \\
 &= 19^{-1} \times \begin{bmatrix} 10 & 19 \\ 17 & 3 \end{bmatrix} \bmod 26 \\
 &= 11 \times \begin{bmatrix} 10 & 19 \\ 17 & 3 \end{bmatrix} \bmod 26 \\
 &= \begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \bmod 26
 \end{aligned}$$

$$\begin{aligned}
 \begin{bmatrix} Z \\ G \\ W \\ Q \end{bmatrix} &\rightarrow \begin{bmatrix} 25 \\ 6 \\ 22 \\ 16 \end{bmatrix} \rightarrow \begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 25 \\ 6 \\ 22 \\ 16 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 11 \\ 18 \\ 14 \end{bmatrix} \rightarrow \begin{bmatrix} A \\ L \\ S \\ O \end{bmatrix}
 \end{aligned}$$

解密字符为："ALSO"

### 例 5

加密 CODE, 令  $A = \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix}$

---

```
import numpy as np

Plaintext = 'COKE'#字母需要大写

A = np.mat([[22,13],[11,5]])

Ciphertext = ''

if len(Plaintext)%2 == 0:
    pass
else:
    Plaintext += 'K' #填充K

for i in range(len(Plaintext)):
    if i%2 == 0:
        M = Plaintext[i:i+2]

        X = np.mat([[ord(M[0]) - 65],[ord(M[1]) - 65]])
        Y = A*X%26

        Ciphertext += chr(int(Y[0]) + 65)
        Ciphertext += chr(int(Y[1]) + 65)
print(Ciphertext)
```

---

输出: SOMA

### 例 6

已知密文"*DLHIVDLZHIPNEU*", 已知使用希尔密码和  $2 \times 2$  作为加密手段。并且有明显证据证明明文开头为 *DEAR*。尝试解密。

解:

D	L	H	I	V	D	L	Z	H	I	P	N	E	U
3	11	7	8	21	3	11	25	7	8	15	13	4	20
D	E	A	R										
3	4	0	17										

$$\begin{bmatrix} D \\ L \end{bmatrix} \mapsto \begin{bmatrix} D \\ E \end{bmatrix}$$

$$\begin{bmatrix} H \\ I \end{bmatrix} \mapsto \begin{bmatrix} V \\ D \end{bmatrix}$$

下一步计算  $A^{-1}$ ,

$$A^{-1} \begin{bmatrix} 3 \\ 11 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \end{bmatrix} \pmod{26}$$

$$A^{-1} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 0 \\ 17 \end{bmatrix} \pmod{26}$$

因为:

$$A^{-1} \begin{bmatrix} 3 & 7 \\ 11 & 8 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 4 & 17 \end{bmatrix}$$

所以:

$$A^{-1} = \begin{bmatrix} 3 & 0 \\ 4 & 17 \end{bmatrix} \cdot \begin{bmatrix} 3 & 7 \\ 11 & 8 \end{bmatrix}^{-1} = \begin{bmatrix} 3 & 0 \\ 4 & 17 \end{bmatrix} \cdot \begin{bmatrix} 18 & 7 \\ 11 & 23 \end{bmatrix} = \begin{bmatrix} 2 & 21 \\ 25 & 3 \end{bmatrix} \pmod{26}$$

$X = A^{-1} \cdot Y$ , 与例 4 同理