



**Keywords:** group, inverse, code, cryptography, secret messages

**Theorem**  $(\mathbb{Z}_n, +), (U(n), \cdot)$  are groups.



输入密码



紧急呼叫

取消



# Salamis Bay' battle





Morse code: " . " (Di) ; "—" (Da) 。 1t; 3t; 5t。

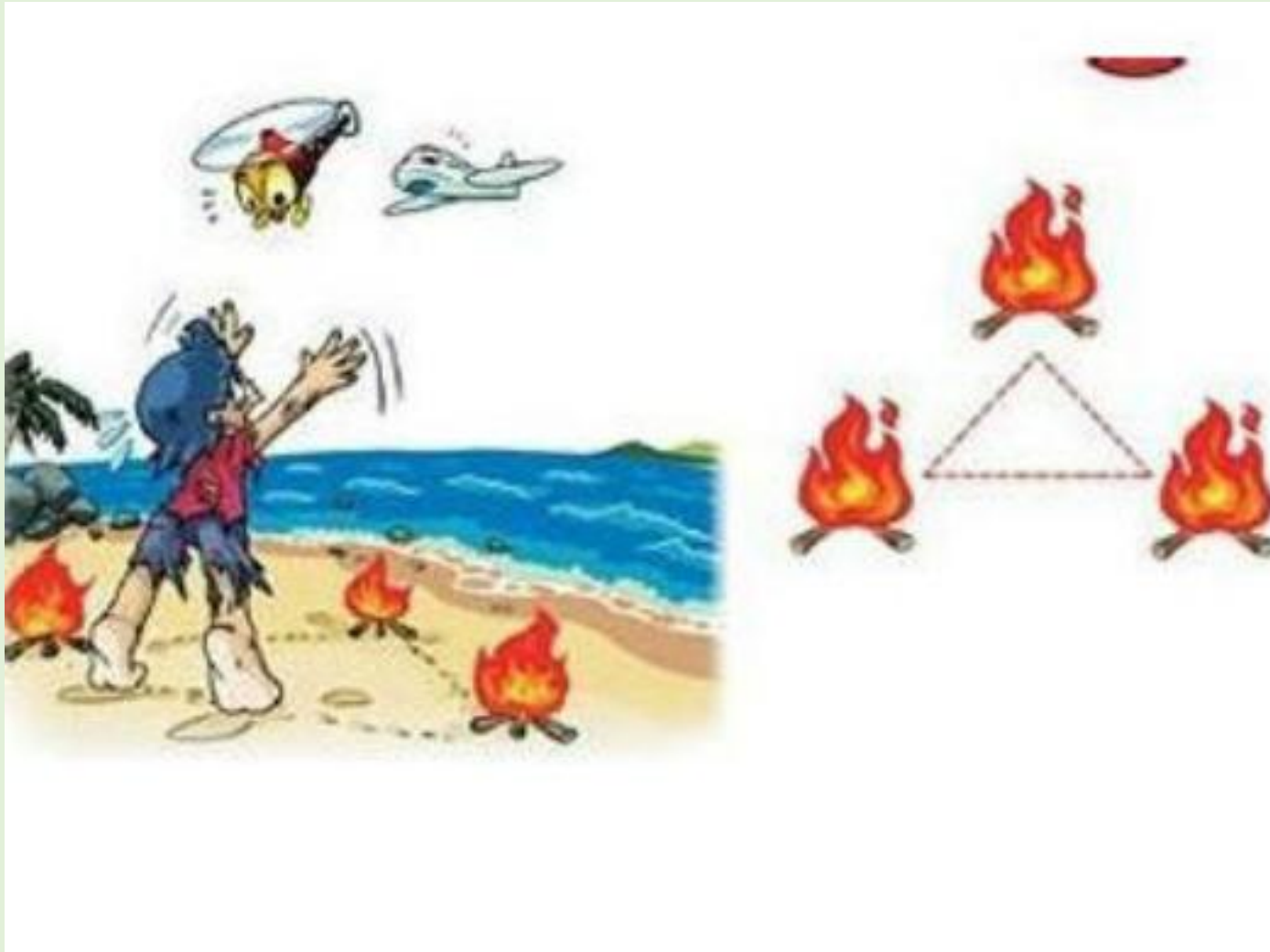
摩 尔 斯 电 码 表

| 字符 | 电码符号    | 字符 | 电码符号    | 字符  | 电码符号        |
|----|---------|----|---------|-----|-------------|
| A  | * —     | N  | — *     | 1   | * — — — —   |
| B  | — * * * | O  | — — —   | 2   | * * — — —   |
| C  | — * — * | P  | * — — * | 3   | * * * — —   |
| D  | — * *   | Q  | — — * — | 4   | * * * * —   |
| E  | *       | R  | * — *   | 5   | * * * * *   |
| F  | * * — * | S  | * * *   | 6   | — * * * *   |
| G  | — — *   | T  | —       | 7   | — — * * *   |
| H  | * * * * | U  | * * —   | 8   | — — — * *   |
| I  | * *     | V  | * * * — | 9   | — — — — *   |
| J  | * — — — | W  | * — —   | 0   | — — — — —   |
| K  | — * —   | X  | — * * — | ?   | * * — — * * |
| L  | * — * * | Y  | — * — — | /   | — * * — *   |
| M  | — —     | Z  | — — * * | ( ) | — * — — * — |
|    |         |    |         | —   | — * * * * — |
|    |         |    |         | *   | * — * — * — |





# 1. Fire



## 2. Smoke

### 浓烟信号

- 在火堆中添加绿草、树叶、苔藓或蕨类植物产生浓烟。
- 潮湿的树枝、草席、坐垫可熏烧更长时间。





### 3. Mirror

- 利用镜子、罐头盖、玻璃、金属片等反射光线。
- 持续的反射将产生一条长线和一个圆点，引人注目。



## 4. Flashlight



1.

|    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| A  | B  | C  | D  | E  | F  | G  | H  | I  | J  | K  | L  | M  |
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 |
| N  | O  | P  | Q  | R  | S  | T  | U  | V  | W  | X  | Y  | Z  |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

encoding function:  $f(P) = P + 3 \mod 26$

Decoding function  $f^{-1}(P) = (P - 3) \mod 26 = (P + 23) \mod 26$

Example: DOJHEUD

*DOJHEUD*  $\longrightarrow$  3,14,9,7,4,20,3

$\xrightarrow{f^{-1}}$  0,11,6,4,1,17,0  $\longrightarrow$  ALGEBRA

## 2.affine cryptosystem

$$f(p)=ap+b \bmod 26, \quad (\mathbb{Z}_{26}, \bullet) \quad \gcd(a, 26)=1$$

$$f^{-1}(p) = a^{-1}p - a^{-1}b \bmod 26$$

Example:  $a = 5, f(p) = 5p + 3 \bmod 26,$

$$f^{-1}(p) = 21p - 21 \cdot 3 \bmod 26 = 21p + 15 \bmod 26$$



### 3.Hill code:

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



action code:

1,3,20,9,15,14

$$A = \begin{pmatrix} 1 & 9 \\ 3 & 15 \\ 20 & 14 \end{pmatrix}$$

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

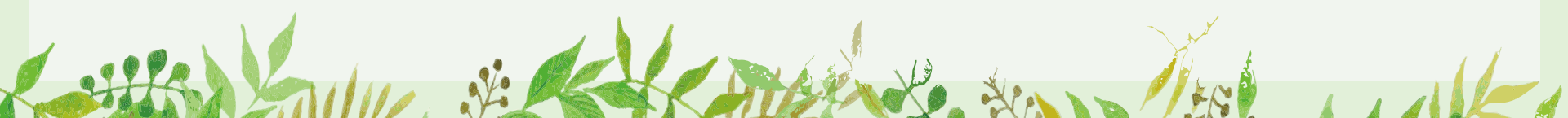
Encryption matrix

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$$

$$AB = \begin{pmatrix} 1 & 9 \\ 3 & 15 \\ 20 & 14 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 67 & 81 \\ 44 & 52 \\ 43 & 43 \end{pmatrix} = C$$

$$B^{-1} = \begin{pmatrix} 0 & 1 & -1 \\ 2 & -2 & -1 \\ -1 & 1 & 1 \end{pmatrix}$$

$$B^{-1}C = \begin{pmatrix} 0 & 1 & -1 \\ 2 & -2 & -1 \\ -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 67 & 81 \\ 44 & 52 \\ 43 & 43 \end{pmatrix} = \begin{pmatrix} 1 & 9 \\ 3 & 15 \\ 20 & 14 \end{pmatrix}$$

[illegible]

$$AB=BA=I \pmod{m}$$

$$A^{-1} = |A|^{-1} \pmod{m} A^*$$

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, A^* = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}, |A| = 3, |A|^{-1} \pmod{26} = 9$$

$$A^{-1} = 9 \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 18 & -9 \\ -9 & 18 \end{pmatrix}$$





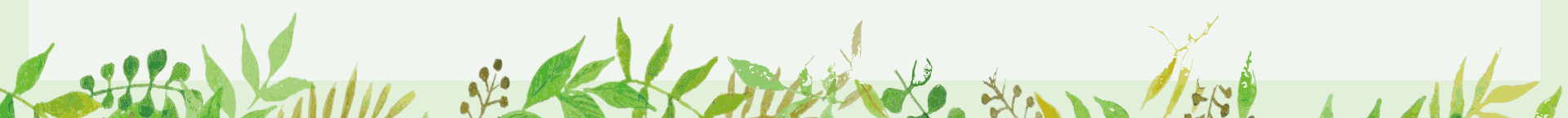
Yes, I do

25, 5, 19, 9, 4, 15

Yes I do

$$p_1 = \begin{pmatrix} 25 \\ 5 \end{pmatrix}, p_2 = \begin{pmatrix} 19 \\ 9 \end{pmatrix}, p_3 = \begin{pmatrix} 4 \\ 15 \end{pmatrix}$$

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

$$q_1 = A \begin{pmatrix} 25 \\ 5 \end{pmatrix} = \begin{pmatrix} 55 \\ 5 \end{pmatrix}, q_2 = A \begin{pmatrix} 19 \\ 9 \end{pmatrix} = \begin{pmatrix} 47 \\ 37 \end{pmatrix}, q_3 = A \begin{pmatrix} 4 \\ 15 \end{pmatrix} = \begin{pmatrix} 23 \\ 34 \end{pmatrix}$$


$$q_1 = A \begin{pmatrix} 25 \\ 5 \end{pmatrix} = \begin{pmatrix} 55 \\ 5 \end{pmatrix}, q_2 = A \begin{pmatrix} 19 \\ 9 \end{pmatrix} = \begin{pmatrix} 47 \\ 37 \end{pmatrix}, q_3 = A \begin{pmatrix} 4 \\ 15 \end{pmatrix} = \begin{pmatrix} 23 \\ 34 \end{pmatrix}$$

mod26

$$s_1 = \begin{pmatrix} 3 \\ 9 \end{pmatrix}, s_2 = \begin{pmatrix} 21 \\ 11 \end{pmatrix}, s_3 = \begin{pmatrix} 23 \\ 8 \end{pmatrix}$$

3, 9, 21, 11, 23, 8    C, I, U, K, W, H



$$t_1 = \begin{pmatrix} -27 \\ 135 \end{pmatrix}, t_2 = \begin{pmatrix} 279 \\ 9 \end{pmatrix}, t_3 = \begin{pmatrix} 342 \\ -63 \end{pmatrix},$$

$$p_1 = \begin{pmatrix} -27 \\ 135 \end{pmatrix} (\bmod 26) = \begin{pmatrix} 25 \\ 5 \end{pmatrix}, p_2 = \begin{pmatrix} 279 \\ 9 \end{pmatrix} (\bmod 26) = \begin{pmatrix} 19 \\ 9 \end{pmatrix},$$

$$p_3 = \begin{pmatrix} 342 \\ -63 \end{pmatrix} (\bmod 26) = \begin{pmatrix} 4 \\ 15 \end{pmatrix},$$

Let  $A = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}$  be invertible

$$A^{-1} = 3^{-1} \begin{pmatrix} 1 & 0 \\ -2 & 3 \end{pmatrix} (\text{mod } 26)$$

$$= 9 \begin{pmatrix} 1 & 0 \\ -2 & 3 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 9 & 0 \\ -18 & 27 \end{pmatrix} (\text{mod } 26)$$

$$= \begin{pmatrix} 9 & 0 \\ 8 & 1 \end{pmatrix}$$

General Roberts was shot.

General Roberts was shot

$$q_1 = \begin{pmatrix} 7 \\ 5 \end{pmatrix}, q_2 = \begin{pmatrix} 14 \\ 5 \end{pmatrix}, q_3 = \begin{pmatrix} 18 \\ 1 \end{pmatrix}, q_4 = \begin{pmatrix} 12 \\ 8 \end{pmatrix}, q_5 = \begin{pmatrix} 15 \\ 5 \end{pmatrix}, q_6 = \begin{pmatrix} 7 \\ 2 \end{pmatrix}$$
$$q_7 = \begin{pmatrix} 20 \\ 19 \end{pmatrix}, q_8 = \begin{pmatrix} 23 \\ 19 \end{pmatrix}, q_9 = \begin{pmatrix} 19 \\ 19 \end{pmatrix}, q_{10} = \begin{pmatrix} 8 \\ 15 \end{pmatrix}, q_{11} = \begin{pmatrix} 20 \\ 20 \end{pmatrix}$$

$$p_i = q_i A$$

$$q_1 = \begin{pmatrix} 21 \\ 19 \end{pmatrix}, q_2 = \begin{pmatrix} 42 \\ 33 \end{pmatrix}, q_3 = \begin{pmatrix} 54 \\ 37 \end{pmatrix}, q_4 = \begin{pmatrix} 36 \\ 42 \end{pmatrix}, q_5 = \begin{pmatrix} 45 \\ 32 \end{pmatrix}, q_6 = \begin{pmatrix} 15 \\ 28 \end{pmatrix}$$

$$q_7 = \begin{pmatrix} 60 \\ 59 \end{pmatrix}, q_8 = \begin{pmatrix} 69 \\ 65 \end{pmatrix}, q_9 = \begin{pmatrix} 57 \\ 57 \end{pmatrix}, q_{10} = \begin{pmatrix} 24 \\ 31 \end{pmatrix}, q_{11} = \begin{pmatrix} 60 \\ 60 \end{pmatrix}$$

$$s_1 = \begin{pmatrix} 21 \\ 19 \end{pmatrix}, s_2 = \begin{pmatrix} 16 \\ 7 \end{pmatrix}, s_3 = \begin{pmatrix} 2 \\ 11 \end{pmatrix}, s_4 = \begin{pmatrix} 10 \\ 16 \end{pmatrix}, s_5 = \begin{pmatrix} 19 \\ 6 \end{pmatrix}, s_6 = \begin{pmatrix} 15 \\ 2 \end{pmatrix}$$

$$s_7 = \begin{pmatrix} 8 \\ 7 \end{pmatrix}, s_8 = \begin{pmatrix} 17 \\ 13 \end{pmatrix}, s_9 = \begin{pmatrix} 5 \\ 5 \end{pmatrix}, s_{10} = \begin{pmatrix} 24 \\ 5 \end{pmatrix}, s_{11} = \begin{pmatrix} 8 \\ 8 \end{pmatrix}$$

$$q_i = A^{-1}s_i(\text{mod } 26)$$

$$q_1 = A^{-1}s_1(\text{mod } 26) = \begin{pmatrix} 9 & 0 \\ 8 & 1 \end{pmatrix} \begin{pmatrix} 21 \\ 19 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 189 \\ 187 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 7 \\ 5 \end{pmatrix}$$

$$q_2 = A^{-1}s_2(\text{mod } 26) = \begin{pmatrix} 9 & 0 \\ 8 & 1 \end{pmatrix} \begin{pmatrix} 16 \\ 7 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 144 \\ 135 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 14 \\ 5 \end{pmatrix}$$



Mathematics is the queen  
of sciences and  
arithmetic the queen of  
mathematics.

-----

Gauss

