



華東師範大學

EAST CHINA NORMAL UNIVERSITY

第四讲

矩阵模运算与古典密码

—— Hill₂ 加密解密

主要内容

- 信息加密与古典密码
- 矩阵运算与Hill₂加密解密
- Hill₂密码破译
- MATLAB 实现

信息加密

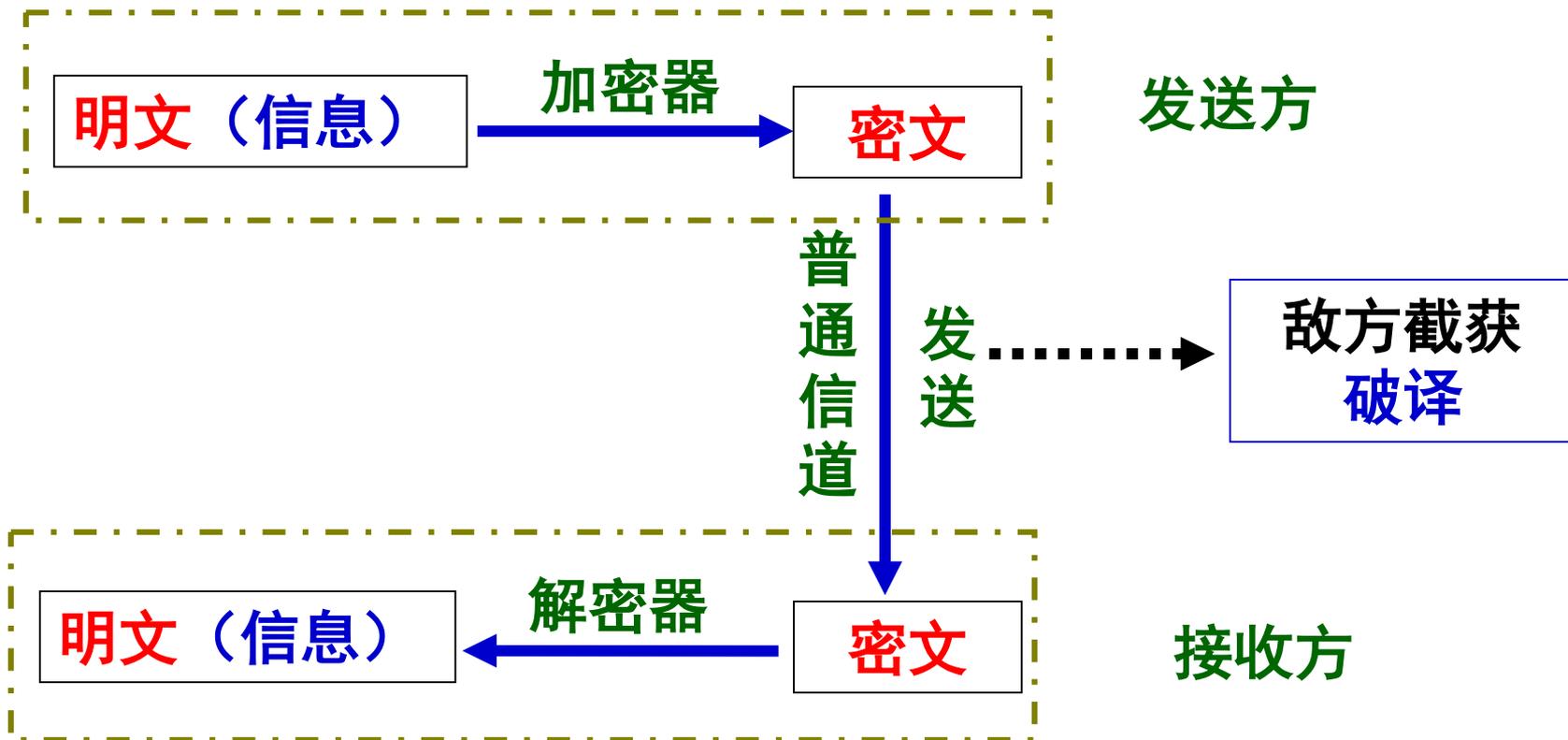
■ 为什么要加密

- 保密通讯无论在军事、政治、经济还是日常生活中都起着非常重要的作用。
- 为了将信息传递给己方的接受者，同时又要防止他人（特别是敌人）知道信息的内容，必须将要传递的信息（明文）加密，变成密文后发送出去，这样，即使敌方得到密文也看不懂，而己方的接受者收到密文后却可以按照预先定好的方法加以解密。

■ 密码分类

- 古典密码：以字符为基本加密单元
- 现代密码：以信息块为基本加密单元

加密信息传递过程



矩阵运算与Hill₂ 密码

Hill2 密码的加密过程

- Hill₂ 密码中所用的数学手段是 **矩阵运算**

- **加密过程:**

① 将 26 个字母与 0 到 25 之间的整数建立一一对应关系，称为字母的表值，然后根据明文字母的表值，将明文信息用数字表示

设通讯双方所给出的 26 个字母的表值如下:

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	0

注: 这里假定明文中只使用 26 个大写字母

Hill2 密码的加密过程

② 选择一个二阶可逆整数方阵 A ，称为Hill2密码的加密矩阵，它是加密体制的“密钥”，是加密的关键，仅通讯双方掌握

③ 将明文字母分组。Hill₂使用的是二阶矩阵，所以将明文字母每2个一组（可以推广至Hill_n密码）。查出每个字母的表值，这样，每组字母构成一个二维列向量 α

若最后仅剩一个字母，则补充一个没有实际意义的哑字母（哑元），这样使得每组都有2个字母

④ 令 $\beta = A\alpha$ ，由 β 的两个分量反查字母表值表，得到相应的两个字母，即为密文字母

Hill2 加密举例

例：设明文为“**HSDSX**”（华东师大数学系），试给出这段明文的 Hill₂ 密文。其中加密矩阵为

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

解：将明文字母分组：

HD SD SX XX

最后的一个字母 X 为哑字母，无实际意义。

查表得每组字母的表值，得到 4 个二维列向量：

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	0

$$\begin{pmatrix} 8 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 24 \end{pmatrix}, \begin{pmatrix} 24 \\ 24 \end{pmatrix}$$

Hill2 加密举例

将上述 4 个二维向量左乘密钥矩阵 A 得：

$$\begin{pmatrix} 16 \\ 12 \end{pmatrix}, \begin{pmatrix} 27 \\ 12 \end{pmatrix}, \begin{pmatrix} 67 \\ 72 \end{pmatrix}, \begin{pmatrix} 72 \\ 72 \end{pmatrix}$$

作模 26 运算，将所有的数都化为 0 到 25 之间的整数：

$$\begin{pmatrix} 16 \\ 12 \end{pmatrix} \pmod{26} = \begin{pmatrix} 16 \\ 12 \end{pmatrix}, \quad \begin{pmatrix} 27 \\ 12 \end{pmatrix} \pmod{26} = \begin{pmatrix} 1 \\ 12 \end{pmatrix}$$
$$\begin{pmatrix} 67 \\ 72 \end{pmatrix} \pmod{26} = \begin{pmatrix} 15 \\ 20 \end{pmatrix}, \quad \begin{pmatrix} 72 \\ 72 \end{pmatrix} \pmod{26} = \begin{pmatrix} 20 \\ 20 \end{pmatrix}.$$

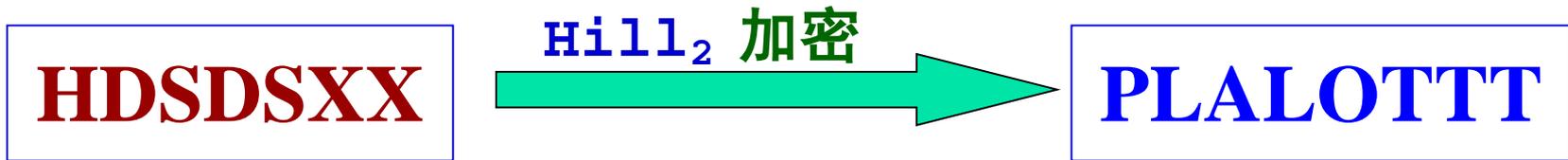
Hill2 加密举例

反查字母表值得每个向量对应的字母组为：

$$\begin{pmatrix} 16 \\ 12 \end{pmatrix}, \begin{pmatrix} 1 \\ 12 \end{pmatrix}, \begin{pmatrix} 15 \\ 20 \end{pmatrix}, \begin{pmatrix} 20 \\ 20 \end{pmatrix}$$

↓ ↓ ↓ ↓

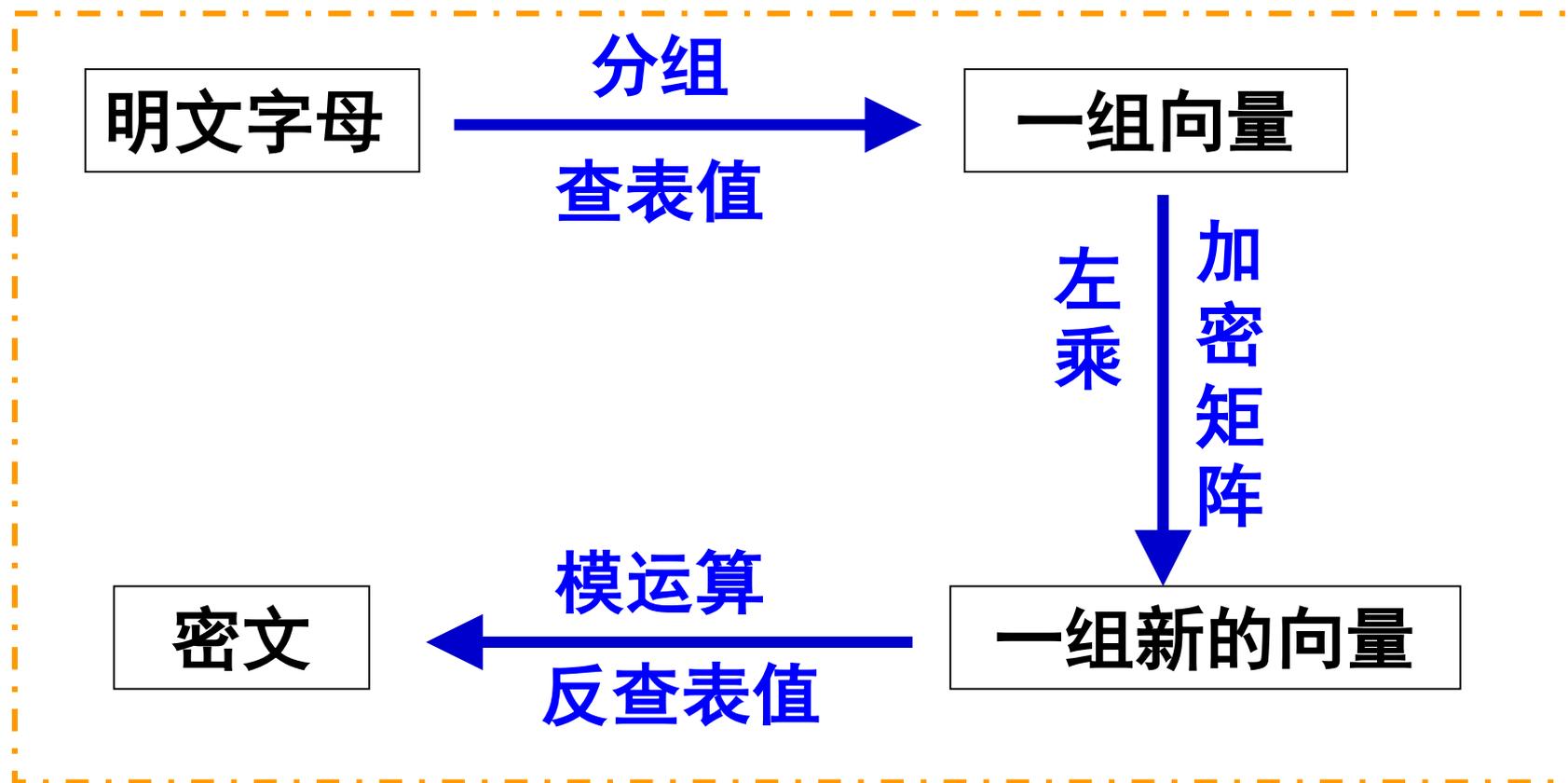
PL **AL** **OT** **TT**



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	0

Hill2 加密过程



问题： 怎样解密？

Hill₂ 密码解密

Hill2 解密过程

■ 解密：加密的逆过程，将加密过程逆转回去即可

例：怎么得到密文 “PLALOTTT” 的原文

先查出密文字母 “PL AL OT TT” 所对应的向量：

$$\begin{pmatrix} 16 \\ 12 \end{pmatrix}, \begin{pmatrix} 1 \\ 12 \end{pmatrix}, \begin{pmatrix} 15 \\ 20 \end{pmatrix}, \begin{pmatrix} 20 \\ 20 \end{pmatrix}$$

上面的向量是由 $\begin{pmatrix} 16 \\ 12 \end{pmatrix}, \begin{pmatrix} 27 \\ 12 \end{pmatrix}, \begin{pmatrix} 67 \\ 72 \end{pmatrix}, \begin{pmatrix} 72 \\ 72 \end{pmatrix}$ 经过模 26 运算

得来的，现在的问题是怎样逆转回去？

在模运算下解方程组： $A\alpha = \beta$

模 m 可逆

记 $Z_m = \{0, 1, 2, \dots, m-1\}$

定义 1: 设 A 为定义在集合 Z_m 上的 n 阶方阵, 若存在一个定义在 Z_m 上的方阵 B , 使得

$$AB = BA = E(\text{mod } m)$$

则称 A 模 m 可逆, B 为 A 的模 m 逆矩阵, 记为

$$B = A^{-1}(\text{mod } m)$$

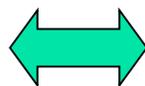
定义 2: 设 $a \in Z_m$, 若存在 $b \in Z_m$ 使得 $ab=1(\text{mod } m)$, 则称 b 为 a 的模 m 倒数或乘法逆, 记作 $b = a^{-1}(\text{mod } m)$ 。

注: a, b 都是 Z_m 中的数

模 m 可逆

■ **问题：** 是否 Z_m 中所有的数都存在模 m 倒数？

a 存在唯一的模 m 倒数



a 与 m 无公共素数因子

命题： 定义在集合 Z_m 上的 n 阶方阵 A 模 m 可逆的充要条件是： m 和 $\det(A)$ 无公共素数因子，即 m 与 $\det(A)$ 互素。

Hill₂ 密码的加密矩阵必须满足上述条件。

$m=26$



m 的素数因子只有 2 和 13

● 定义在 Z_{26} 上的方阵 A 模 26 可逆的充要条件是：

$\det(A)$ 不能被 2 和 13 整除

模 26 可逆

- \mathbb{Z}_{26} 中具有模 26 倒数的整数及其模 26 倒数表

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

- **思考：**如何用 Matlab 编程来找出所有模 m 倒数的整数及其模 m 倒数？（穷举法）

Hill2 解密过程

$$\begin{pmatrix} 16 \\ 12 \end{pmatrix}, \begin{pmatrix} 1 \\ 12 \end{pmatrix}, \begin{pmatrix} 15 \\ 20 \end{pmatrix}, \begin{pmatrix} 20 \\ 20 \end{pmatrix} \xrightarrow{\text{?}} \begin{pmatrix} 8 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 24 \end{pmatrix}, \begin{pmatrix} 24 \\ 24 \end{pmatrix}$$

↔ 在模运算下解方程组: $A\alpha = \beta$

↔ $\alpha = A^{-1}(\text{mod } 26) * \beta (\text{mod } 26)$

问题: 如何计算 $A^{-1}(\text{mod } 26)$?

模 m 逆矩阵的计算

$$A^{-1} = \frac{1}{|A|} A^*$$

A^* 为 A 的伴随矩阵

- 设 $B = k A^*$ 为 A 的模 26 逆，其中 k 为待定系数

➡ $BA = k \cdot |A| \cdot E$

$$BA = E \pmod{26} \iff k \cdot |A| = 1 \pmod{26}$$

$$\iff k = |A|^{-1} \pmod{26}$$

本计算方法可推广到求矩阵 A 的模 m 逆矩阵

Hill2 解密过程

● 设加密矩阵 $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \rightarrow |A| = 3, A^* = \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix}$

$\rightarrow A^{-1}(\text{mod } 26) = \left(3^{-1}(\text{mod } 26) \cdot \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix} \right) (\text{mod } 26)$

$\rightarrow B = A^{-1}(\text{mod } 26)$

$$= 9 \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}$$

$$\begin{pmatrix} 16 \\ 12 \end{pmatrix}, \begin{pmatrix} 1 \\ 12 \end{pmatrix}, \begin{pmatrix} 15 \\ 20 \end{pmatrix}, \begin{pmatrix} 20 \\ 20 \end{pmatrix} \xrightarrow{?} \begin{pmatrix} 8 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 24 \end{pmatrix}, \begin{pmatrix} 24 \\ 24 \end{pmatrix}$$

- 用 B 左乘密文对应的向量得：

$$B \begin{pmatrix} 16 \\ 12 \end{pmatrix} = \begin{pmatrix} 112 \\ 108 \end{pmatrix}, \quad B \begin{pmatrix} 1 \\ 12 \end{pmatrix} = \begin{pmatrix} 97 \\ 108 \end{pmatrix},$$

$$B \begin{pmatrix} 15 \\ 20 \end{pmatrix} = \begin{pmatrix} 175 \\ 180 \end{pmatrix}, \quad B \begin{pmatrix} 20 \\ 20 \end{pmatrix} = \begin{pmatrix} 180 \\ 180 \end{pmatrix}$$

- 模 26 运算后得：

$$\begin{pmatrix} 8 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 24 \end{pmatrix}, \begin{pmatrix} 24 \\ 24 \end{pmatrix}$$

- 查表后得明文分别为： **HD** **SD** **SX** **XX**

Hill2 加密过程总结

① 通讯双方确定**加密矩阵** (密钥) 和字母的**表值对应表**

② 将**明文**字母分组，通过查表列出每组字母对应的**向量** α

若明文只含奇数个字母，则补充一个哑元

③ 令 $\beta = A\alpha \bmod(m)$ ，由 β 的分量反查字母表值表，得到相应的**密文**字母

Hill2 解密过程总结

- ① 将密文字母分组，通过查表列出每组字母对应的向量 β
- ② 求出加密矩阵 A 的模 m 逆矩阵 B
- ③ 令 $\alpha = B * \beta \bmod(m)$ ，由 α 的分量反查字母表值表，得到相应的明文字母

Hill2 解密举例

甲方收到乙方（己方）的一个密文信息，内容为：

WKVACPEAOCIXGWIZUROQWAB
ALOHDKCEAFCLWVCVLEMIMCC

按照甲方与乙方的约定，他们之间采用 Hill₂密码，密钥为 $A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ ，字母表值见下表，问这段密文的原文是什么？

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	0

Hill2 解密举例

① 将密文字母分组，通过查表列出每组字母对应的向量

② 求出加密矩阵 A 的模 26 逆矩阵

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

③ 用 B 左乘每组密文字母组成的向量，然后再反查字母表值表，得到相应的明文字母

Hill2 解密举例

序号	分组密文	密文表值	明文表值	分组成明文
1	W K	23 11	7 21	G U
2	V A	22 1	4 9	D I
3	C P	3 16	1 14	A N
4	E A	5 1	13 9	M I
5	O C	15 3	13 1	M A
6	I X	9 24	19 8	S H

序号	分组密文	密文表值	明文表值	分组成明文
7	G W	7 23	9 25	I Y
8	I Z	9 0	9 0	I Z
9	U R	21 18	9 6	I F
10	O Q	15 17	21 23	U W
11	W A	23 1	5 9	E I
12	B A	2 1	10 9	J I

Hill2 解密举例

序号	分组密文	密文表值	明文表值	分组明文
13	L O	12 15	2 5	B E
14	H D	8 4	14 10	N J
15	K C	11 3	9 1	I A
16	E A	5 1	13 9	M I
17	F C	6 3	4 1	D A
18	L W	12 23	14 25	N Y

序号	分组密文	密文表值	明文表值	分组明文
19	W C	23 3	21 1	U A
20	V L	22 12	14 4	N D
21	E M	5 13	5 13	E M
22	I M	9 13	9 13	I M
23	C C	3 3	1 1	A A

Hill2 解密举例

密文

**WKVACPEAOCIXGWIZUROQWAB
ALOHDKCEAFCLWWCVLEMIMCC**

原文

**GU DIAN MI MA SHI YI ZI FU WEI JI
BEN JIA MI DAN YUAN DE MI MA A**

即：“古典密码是以字符为基本加密单元的密码”

Hill₂ 密码破译

Hill2 密码破译举例

我方截获一段密文

MOFAXJEABAU CRSXJLUYHQATCZHWBCSCP

经分析该密文是用 Hill₂密码 加密，且密文 (U, C) 和 (R, S) 分别对应明文 (T, A) 和 (C, O)，问能否破译这段密文？

- 破译这段密文的关键是找到“密钥”和字母对应的表值
- 猜测密文是由26个字母组成，即 $m=26$ ，
经破译部门通过大量的统计分析和语言分析确定表值

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	0

Hill2 密码破译举例

- 密文 (U, C) 和 (R, S) 分别对应明文 (T, A) 和 (C, O)

$$\begin{pmatrix} U \\ C \end{pmatrix} \rightarrow \begin{pmatrix} T \\ A \end{pmatrix}, \quad \begin{pmatrix} R \\ S \end{pmatrix} \rightarrow \begin{pmatrix} C \\ O \end{pmatrix}$$

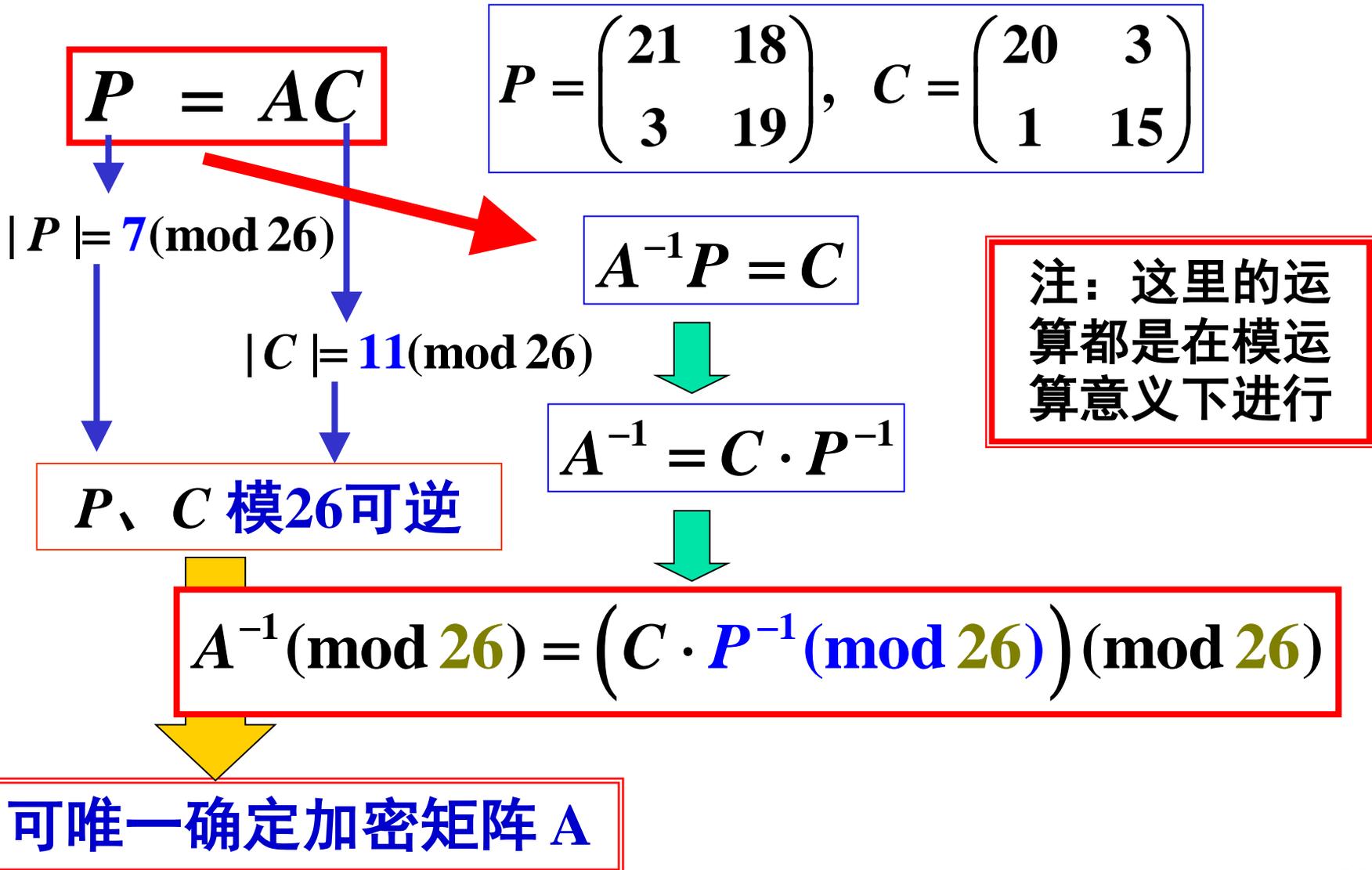
查字母表值

$$\begin{pmatrix} 21 \\ 3 \end{pmatrix} = A \begin{pmatrix} 20 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 18 \\ 19 \end{pmatrix} = A \begin{pmatrix} 3 \\ 15 \end{pmatrix}$$

$$\begin{pmatrix} 21 & 18 \\ 3 & 19 \end{pmatrix} P = A \begin{pmatrix} 20 & 3 \\ 1 & 15 \end{pmatrix} C$$

$$P = AC$$

Hill2 密码破译举例



Hill2 密码破译举例

- 得到加密矩阵的 **模26逆矩阵** 后，根据前面的解密方法即可得密文的原文

HE WILL VISIT A COLLEGE ET HIS AFTER NO ON