技術型高中數學推動中心
素養導向教案設計

<table>
<tr><td colspan="2">領域/科目</td><td>數學領域</td><td>設計者</td><td>鳳商商工林正傑</td></tr>
<tr><td colspan="2">實施年級</td><td>11 年級(C 版)</td><td>總節數</td><td>共__1___節，_50__分鐘</td></tr>
<tr><td colspan="2">單元名稱</td><td colspan="3">矩陣的運算</td></tr>
<tr><td colspan="5">課程設計原則與教學理念說明</td></tr>
<tr><td colspan="2">教學單元主題設計原則與教學理念說明</td><td colspan="3">矩陣的運算是工程數學最重要的內容之一，而古典密碼中的希爾密碼正是利用矩陣來加密與解密，本教案引導學生認識希爾密碼，實作加密與解密希爾密碼，最後運用 Python 來實踐希爾密碼。</td></tr>
<tr><td colspan="2">學生學習經驗分析</td><td colspan="3">1. 熟習矩陣的運算
2. 熟習二階反矩陣的計算</td></tr>
<tr><td colspan="2">教材設計</td><td colspan="3">1. 學習單
2. 希爾密碼 python 程式碼</td></tr>
<tr><td colspan="2">教學活動</td><td colspan="3">1. 複習矩陣的運算與二階反矩陣的計算
2. 介紹與實作希爾密碼的加密與解密
3. 演示 python 程式碼與總結</td></tr>
<tr><td colspan="2">學習評量</td><td colspan="3">學習單</td></tr>
<tr><td colspan="5">設計依據</td></tr>
<tr><td rowspan="2">核心素養</td><td>領綱
(詳見表末備註)</td><td colspan="3">■數V-U-A1 □數V-U-A2 □數V-U-A3
□數V-U-B1 ■數V-U-B2 □數V-U-B3
□數V-U-C1 □數V-U-C2 □數V-U-C3</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="4">學習重點</td><td>學習表現</td><td colspan="3">□1-V-1 概念的了解 ■1-V-2 程序的執行 □1-V-3 問題的解決
□1-V-4 連結與應用 □2-V-1 工具的應用 □3-V-1 信念的養成</td></tr>
<tr><td rowspan="3">學習內容編碼
(請參閱領綱例:N-10-1)</td><td colspan="3">□數學(A)：</td></tr>
<tr><td colspan="3">□數學(B)：</td></tr>
<tr><td colspan="3">■數學(C)：A-11-3</td></tr>
<tr><td rowspan="3">議題融入</td><td>融入主題
(可複選)</td><td colspan="3">□無 □性別平等 □人權 □環境 □海洋 □品德 □生命
□法治 □科技 ■資訊 □能源 □安全 □防災 □家庭教育
□生涯規劃 □多元文化 □閱讀素養 □戶外教育 □國際教育
□原住民族教育</td></tr>
<tr><td>所融入之學習重點</td><td colspan="3">● 了解希爾密碼的加密與解密
● 利用演算法與程式設計呈現希爾密碼的加密與解密流程，以使學生更深刻體驗抽象化與步驟化之歷程與重要性。</td></tr>
<tr><td>實質內涵</td><td colspan="3">● 資 E4 認識常見的資訊科技共創工具的使用方法。
● 資 E6 認識與使用資訊科技以表達想法。</td></tr>
<tr><td colspan="2">具備跨科整合</td><td colspan="3">□是□否 | 跨 科 課 程 | 科目： ，課程名稱:</td></tr>
<tr><td colspan="2">適用群別</td><td colspan="3">□均可
□家政群 □藝術群 □商業與管理群 □外語群 □設計群 □農業群
□食品群 □餐旅群 □海事群 □水產群 ■機械群 ■動力機械群
■電機與電子群 ■化工群 ■土木與建築群</td></tr>
<tr><td colspan="2">教材來源</td><td colspan="3">網路資料
數學 C 第 3 冊
參考書籍: Secret History: The Story of Cryptology</td></tr>
<tr><td colspan="2">教學設備/資源</td><td colspan="3">筆記型電腦
Colab 線上 python 執行平台</td></tr>
</table>

學習目標
一、 認知目標 ：了解希爾密碼。 二、 技能目標 ：學會加密與解密希爾密碼。 三、 情意目標 ：了解能用 python 程式語言加密與解密希爾密碼。

教學活動設計

教學活動內容及實施方式	時間	備註
● 複習矩陣的基本運算。 1. 矩陣的乘法 **定義** 矩陣的乘法 設 $m\times n$ 階矩陣 $A=[a_{ij}]_{m\times n}$，$n\times l$ 階矩陣 $B=[b_{ij}]_{n\times l}$，則 A 和 B 的乘積 $AB=C=[c_{ij}]_{m\times l}$ 是 $m\times l$ 階矩陣，其中 $c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{in}b_{nj}$，即 $\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1l} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2l} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nj} & \cdots & b_{nl} \end{bmatrix}=\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1l} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2l} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{i1} & c_{i2} & \cdots & c_{ij} & \cdots & c_{il} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mj} & \cdots & c_{ml} \end{bmatrix}$ 2. 2 階反矩陣的計算 **公式** 二階反方陣 設二階方陣 $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$，若其行列式 $\det(A)=ad-bc\neq 0$，則 A 的乘法反方陣 A^{-1} 存在，且 $A^{-1}=\frac{1}{\det(A)}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	8 分	● 這是數學 C 的課本內容，本節課會用到的部分是矩陣的基本運算(+、－、*)以及二階反矩陣的計算。
● 介紹密碼學中字母的表示法與完成對照表。 英文有 26 個字母，在密碼學裡為了配合程式設計會用 0 到 25 來表示從 A 到 Z 的字母，如下表 再加密前要將英文字轉換成數字，經過加密變成密文(此時是數字)，再將密文變為英文，傳給收件者，此時收件者得到的是一堆亂碼，要有金鑰才能解密變成看得懂的文字。 ● 介紹希爾密碼的加密與解密方式。 A. 自定加密矩陣 自訂一個金鑰且對應一個可逆矩陣，再轉換為加密數字矩陣	28 分	● 引導學生依序完成學習單的內容

字母	A	B	C	D	E	F	G	H	I	J	K	L	M
數字													
字母	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
數字													

	金鑰	金鑰矩陣	轉換為數字矩陣
例子	hill	$\begin{bmatrix} h & i \\ l & l \end{bmatrix}$	$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$
我的金鑰			

B. 明文分組

首先將明文分成兩兩一組(不包含空格)，如果是奇數個字母，在最後一個字後面補上 X，每一組明文字母轉為數字碼。

	明文	明文分組	轉換成數字向量
例子	Meet in FSVS at nine AM.	M e i F V a n n A e t n S S t i e M	12 4 8 5 21 0 13 13 0 4 19 13 18 18 19 8 4 12
我的明文			

C. 用加密矩陣加密(C=KP)

以加密矩陣乘以明文數字化後的向量，並除以 26 的餘數形成密文的數字向量，再將密文數字向量對照字母表轉為字母即加密完成。

$$\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}12\\4\end{bmatrix}=\begin{bmatrix}116\\176\end{bmatrix}\equiv\begin{bmatrix}12\\20\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}4\\19\end{bmatrix}\equiv\begin{bmatrix}180\\462\end{bmatrix}=\begin{bmatrix}24\\19\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}8\\13\end{bmatrix}=\begin{bmatrix}160\\374\end{bmatrix}\equiv\begin{bmatrix}4\\23\end{bmatrix}$$

$$\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}5\\18\end{bmatrix}\equiv\begin{bmatrix}179\\451\end{bmatrix}=\begin{bmatrix}23\\19\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}21\\18\end{bmatrix}=\begin{bmatrix}291\\627\end{bmatrix}\equiv\begin{bmatrix}5\\13\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}0\\19\end{bmatrix}=\begin{bmatrix}152\\418\end{bmatrix}\equiv\begin{bmatrix}22\\1\end{bmatrix}$$

$$\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}13\\8\end{bmatrix}\equiv\begin{bmatrix}155\\319\end{bmatrix}=\begin{bmatrix}25\\23\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}13\\4\end{bmatrix}=\begin{bmatrix}123\\231\end{bmatrix}\equiv\begin{bmatrix}19\\5\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}0\\12\end{bmatrix}=\begin{bmatrix}96\\264\end{bmatrix}\equiv\begin{bmatrix}18\\2\end{bmatrix}$$

數字加密結果: 12 20 24 19 4 23 23 19 5 13 22 1 25 23 19 5 18 2

字母加密結果:MUYTEXXTFNWBZXTFSC

D. 計算解密矩陣

舉例: 1. 計算$\det\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}=7\times11-8\times11=-11\equiv15 \bmod 26$

2. 計算$\frac{1}{15}\equiv7 \bmod 26$

3. $\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}^{-1}=7\times\begin{bmatrix}11 & -8\\-11 & 7\end{bmatrix}=\begin{bmatrix}77 & -56\\-77 & 49\end{bmatrix}\equiv\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}$

E. 密文分組

將密文分成兩兩一組，再將密文字母轉為數字碼。

	密文	密文分組	轉換成數字向量
例子	MUYTEXXTFNWBZXTFSC	M Y E X F W Z T S U T X T N B X F C	12 24 4 23 5 22 25 19 18 20 19 23 19 13 1 23 5 2
我的密文			

F. 解密($P=K^{-1}C$)

在前面乘上解密矩陣K的反矩陣(K^{-1})，再取除以26的餘數形成明文的數字矩陣，再將明文數字矩陣對照字母表轉為字母即解密完成。

$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}12\\20\end{bmatrix}=\begin{bmatrix}740\\472\end{bmatrix}\equiv\begin{bmatrix}12\\4\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}24\\19\end{bmatrix}=\begin{bmatrix}1018\\461\end{bmatrix}\equiv\begin{bmatrix}4\\19\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}4\\23\end{bmatrix}=\begin{bmatrix}606\\533\end{bmatrix}\equiv\begin{bmatrix}8\\13\end{bmatrix}$
$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}23\\19\end{bmatrix}=\begin{bmatrix}993\\460\end{bmatrix}\equiv\begin{bmatrix}5\\18\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}5\\13\end{bmatrix}=\begin{bmatrix}411\\304\end{bmatrix}\equiv\begin{bmatrix}21\\18\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}22\\1\end{bmatrix}=\begin{bmatrix}572\\45\end{bmatrix}\equiv\begin{bmatrix}0\\19\end{bmatrix}$
$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}25\\23\end{bmatrix}=\begin{bmatrix}1131\\554\end{bmatrix}\equiv\begin{bmatrix}13\\8\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}19\\5\end{bmatrix}=\begin{bmatrix}585\\134\end{bmatrix}\equiv\begin{bmatrix}13\\4\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}18\\2\end{bmatrix}=\begin{bmatrix}494\\64\end{bmatrix}\equiv\begin{bmatrix}0\\12\end{bmatrix}$

數字解密結果: 12 4 4 19 8 13 5 18 21 18 0 19 13 8 13 4 0 12

字母解密結果: MEETINFSVSATNINEAM

- 分析與討論希爾密碼的安全性。

1. 已知明文攻擊法
2. 選擇明文攻擊法
3. 選擇密文攻擊法

以上 3 種攻擊法都可視為解線性聯立方程式的問題。

4. 金鑰空間的討論

希爾密碼出現在 1950 左右，以當時的科技技術似乎要破解是有困難的，我們就暴力法來討論盲試的可能性。首先，我們要了解金鑰空間的大小。

6 分

- 僅需要講述密碼學檢視密碼安全的基本概念，不需要太過理論化的細講。

這是一個等價於線性代數中有多少個不同的逆矩陣的問題。若從排列組合的角度討論是困難的。若從線性獨立向量的方向下手會容易許多。 其他的攻擊法 5. 奇偶性的攻擊法 6. 計分模式攻擊法 ● 實作希爾密碼的加密與解密方式。 參閱 Python 原始程式碼 ● 結論。 矩陣不只是枯燥無味的數學遊戲，也可以是密碼學上的工具，這節課要大家了解希爾密碼的原理並動手操作，最後見證利用 Python 程式來加解密。	5 分 3 分	● 僅需要演示 Python 程式的執行，不需要細講程式的語法與結構。

試教成果：無

參考資料：

Bauer, Craig P./ Rosen, Kenneth H. Secret History: The Story of Cryptology, CRC Press , 2013
Python 教學手冊

附錄：

列出與此示案有關之補充說明。

備註：

※核心素養

數 V-U-A1 具備學好數學的信心與態度，發展個人潛能，並能自主學習，自我超越與精進，努力不懈地探究、分析與解決數學問題。

數 V-U-A2 藉由單元之間數學觀念的統整，強化生活情境與問題理解，學習由不同面向分析問題與解決問題，並將生活問題經由觀察，找出相關性，做成數學推測，找到解決方法。

數 V-U-A3 具備將現實情境的問題轉化為數學問題的能力，並能探索、擬定與執行解決問題的計畫，並能從多元、彈性與創新的角度解決問題，並活用於現實生活。

數 V-U-B1 能辨識問題與數學的關聯，運用數學知識、技能、精確地使用適當的符號去描述、模擬、解釋與預測各種現象，以數學思維做出理性反思與判斷，並在解決問題的歷程中，有效地與他人溝通彼此的觀點，並能連結抽象符號與專業類科、真實世界的問題，靈活運用數學知識、技能與符號，進行經驗、思考、價值與情意之表達，並能理性地與他人溝通並解決問題。

數 V-U-B2 能夠運用科技工具有效解決日常實際問題，與專業領域內的實務問題。以數學理解為基礎，能識讀、批判及反思媒體表達的資訊意涵與議題本質。

數 V-U-B3 藉由繪圖操作使學生涵養對藝術之欣賞、創作的能力，進而創作與發揮創意。利用幾何圖形與曲線之變化，運用線條的韻律、造形的構成、對稱、平衡等，並能於生活中對於美善的人事物進行鑑賞。藉由日常情境中自然界的圖像與媒體的視覺，從中了解數學的關聯性。

數 V-U-C1 具備立基於證據的態度，建構可行的論述，並發展和他人理性溝通的素養，成為理性反思與道德實踐的公民。

數 V-U-C2 具備和他人合作解決問題的素養，並能尊重多元的問題解法，建立良好的互動關係。

數 V-U-C3 具備國際化視野，尊重與欣賞不同文化數學發展的歷史，了解與使用跨文化數學工具。透過數學的理解，關心全球化議題。

※議題融入

請參閱國教院議題融入說明手冊，網址 https://pse.is/KHPBB

希爾密碼學習單

1.完成字母與數字對照表字母

字母	A	B	C	D	E	F	G	H	I	J	K	L	M
數字													
字母	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
數字													

2.加密矩陣

請自訂一個加密金鑰並對照為一可逆矩陣

	金鑰	金鑰矩陣	轉換為數字矩陣
例子	hill	$\begin{bmatrix} h & i \\ l & l \end{bmatrix}$	$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$
我的金鑰			

3. 明文分組

	明文	明文分組	轉換成數字向量
例子	Meet in FSVS at nine AM.	M e i F V a n n A e t n S S t i e M	12 4 8 5 21 0 13 13 0 4 19 13 18 18 19 8 4 12
我的明文			

4. 用加密矩陣加密(C=KP)

舉例:

$$\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}12\\4\end{bmatrix}=\begin{bmatrix}116\\176\end{bmatrix}\equiv\begin{bmatrix}12\\20\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}4\\19\end{bmatrix}\equiv\begin{bmatrix}180\\462\end{bmatrix}=\begin{bmatrix}24\\19\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}8\\13\end{bmatrix}=\begin{bmatrix}160\\374\end{bmatrix}\equiv\begin{bmatrix}4\\23\end{bmatrix}$$

$$\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}5\\18\end{bmatrix}\equiv\begin{bmatrix}179\\451\end{bmatrix}=\begin{bmatrix}23\\19\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}21\\18\end{bmatrix}=\begin{bmatrix}291\\627\end{bmatrix}\equiv\begin{bmatrix}5\\13\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}0\\19\end{bmatrix}=\begin{bmatrix}152\\418\end{bmatrix}\equiv\begin{bmatrix}22\\1\end{bmatrix}$$

$$\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}13\\8\end{bmatrix}\equiv\begin{bmatrix}155\\319\end{bmatrix}=\begin{bmatrix}25\\23\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}13\\4\end{bmatrix}=\begin{bmatrix}123\\231\end{bmatrix}\equiv\begin{bmatrix}19\\5\end{bmatrix}\quad \begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}\begin{bmatrix}0\\12\end{bmatrix}=\begin{bmatrix}96\\264\end{bmatrix}\equiv\begin{bmatrix}18\\2\end{bmatrix}$$

數字加密結果: 12 20 24 19 4 23 23 19 5 13 22 1 25 23 19 5 18 2

字母加密結果:MUYTEXXTFNWBZXTFSC

我的加密過程

數字加密結果:

字母加密結果:

5. 計算解密矩陣

公式 **二階反方陣**

設二階方陣 $A=\begin{bmatrix}a & b\\c & d\end{bmatrix}$，若其行列式 $\det(A)=ad-bc\neq 0$，則 A 的乘法反方陣 A^{-1} 存在，且 $A^{-1}=\dfrac{1}{\det(A)}\begin{bmatrix}d & -b\\-c & a\end{bmatrix}$

舉例: 1. 計算$\det\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}=7\times 11-8\times 11=-11\equiv 15 \mod 26$

2. 計算$\frac{1}{15}\equiv 7 \mod 26$

3. $\begin{bmatrix}7 & 8\\11 & 11\end{bmatrix}^{-1} = 7\times\begin{bmatrix}11 & -8\\-11 & 7\end{bmatrix} = \begin{bmatrix}77 & -56\\-77 & 49\end{bmatrix} \equiv \begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}$

6. 密文分組

	密文	密文分組	轉換成數字向量
例子	MUYTEXXTFNWBZXTFSC	M Y E X F W Z T S U T X T N B X F C	12 24 4 23 5 22 25 19 18 20 19 23 19 13 1 23 5 2
我的密文			

7.解密($P=K^{-1}C$)

舉例:

$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}12\\20\end{bmatrix} = \begin{bmatrix}740\\472\end{bmatrix} \equiv \begin{bmatrix}12\\4\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}24\\19\end{bmatrix} = \begin{bmatrix}1018\\461\end{bmatrix} \equiv \begin{bmatrix}4\\19\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}4\\23\end{bmatrix} = \begin{bmatrix}606\\533\end{bmatrix} \equiv \begin{bmatrix}8\\13\end{bmatrix}$
$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}23\\19\end{bmatrix} = \begin{bmatrix}993\\460\end{bmatrix} \equiv \begin{bmatrix}5\\18\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}5\\13\end{bmatrix} = \begin{bmatrix}411\\304\end{bmatrix} \equiv \begin{bmatrix}21\\18\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}22\\1\end{bmatrix} = \begin{bmatrix}572\\45\end{bmatrix} \equiv \begin{bmatrix}0\\19\end{bmatrix}$
$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}25\\23\end{bmatrix} = \begin{bmatrix}1131\\554\end{bmatrix} \equiv \begin{bmatrix}13\\8\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}19\\5\end{bmatrix} = \begin{bmatrix}585\\134\end{bmatrix} \equiv \begin{bmatrix}13\\4\end{bmatrix}$	$\begin{bmatrix}25 & 22\\1 & 23\end{bmatrix}\begin{bmatrix}18\\2\end{bmatrix} = \begin{bmatrix}494\\64\end{bmatrix} \equiv \begin{bmatrix}0\\12\end{bmatrix}$

數字解密結果: 12 4 4 19 8 13 5 18 21 18 0 19 13 8 13 4 0 12

字母解密結果: MEETINFSVSATNINEAM

我的解密過程

數字解密結果:

字母解密結果:

程式碼

```
import numpy as np
print('以下的討論將用 2 階的矩陣來加密加密')
K=input("請問你的加密密鑰?(4 位英文字)")
# Following function generates the key matrix for the key stringmi
keyMatrix = [[0] * 2 for i in range(2)]
def getKeyMatrix(key):
 k = 0
 for i in range(2):
print('以下的討論將用 2 階的矩陣來加密加密')
K=input("請問你的加密密鑰?(4 位英文字)")
# Following function generates the key matrix for the key string
keyMatrix = [[0] * 2 for i in range(2)]
def getKeyMatrix(key):
 k = 0
 for i in range(2):
  for j in range(2):
   keyMatrix[i][j] = ord(key[k]) % 65
   k += 1
key=str(K).upper()
print(key)
getKeyMatrix(key)

P=input("請輸入明文 ")
P=P.replace(" ","")
P=P.replace(",","")
P=P.replace(".","")
print("我們將使用希爾密碼來加密，你的加密矩陣 K = ")
print(np.array([[key[0],key[1]],[key[2],key[3]]]))
print("經過轉換成數字矩陣變為")
print(np.mat(keyMatrix))
print("我們將明文 2 個 2 個分組，結果如下")
def classify_letter(msg):
   if len(msg)%2 ==0:
      msg = msg
      c=int(len(msg)/2)
   else:
      msg += "X"
      c=int((len(msg)+1)/2)
   M_chr=np.array([['x']*c,['x']*c])
   for i in range(c):
      M_chr[0][i]=msg[2*i].upper()
      M_chr[1][i]=msg[2*i+1].upper()
   return M_chr
print(classify_letter(P))
print("明文矩陣經過轉換成數字矩陣變為")
def classify_num(msg):
   if len(msg)%2 ==0:
      msg = msg
      c=int(len(msg)/2)
   else:
      msg += "X"
      c=int((len(msg)+1)/2)
   M_ord=np.array([[0]*c,[0]*c])
   for i in range(c):
      M_ord[0][i]=ord(msg[2*i].upper())%65
      M_ord[1][i]=ord(msg[2*i+1].upper())%65
   return M_ord
print(classify_num(P))
print('利用加密矩陣加密(C=KP)得到')
C=np.matmul(np.mat(keyMatrix),classify_num(P))%26
print(C)
print("數字矩陣經過轉換成字母矩陣變為")
def num_to_letter(Mat):
   c=int(Mat.shape[1])
   Mat1=np.mat([['x']*c,['x']*c])
   for i in range(c):
      Mat1[0,i]=chr(Mat[0,i]+65)
      Mat1[1,i]=chr(Mat[1,i]+65)
   return Mat1
print(num_to_letter(C))
cipher_M=num_to_letter(C)
print('加密後的密文為')
def mat_to_text(M):
   text=''
   n=int(M.shape[1])
   for i in range(n):
      text=text+M[0,i]+M[1,i]
   return text
mat_to_text(cipher_M)
cipher_text=mat_to_text(cipher_M)
print(cipher_text)
print("")
print("接著，我們來解密加密後的密文 %s"%cipher_text)
print("首先，我們將密文 2 個 2 個分組，結果如下")
print(cipher_M)
print("再將字母數字化")
print(C)
print('先求出解密矩陣 K 的反矩陣 K^(-1)')
def GCD(a,b):
   while(a%b!=0):
      a,b=b,a%b
   return b

def inv(a,n):
   if GCD(a,n)!=1:
      print("不存在乘法反元素")
   else:
      for i in range(n):
         inverse=-1
         if a*i%n==1:
            inverse=i
            break
      return inverse
Key_Mat_N=np.array(keyMatrix)
Det_KM=int(np.linalg.det(Key_Mat_N))
Key_Matinverse_N1=np.array([[Key_Mat_N[1][1],-
1*Key_Mat_N[0][1]],[-1*Key_Mat_N[1][0],Key_Mat_N[0][0]]])
Key_Matinv=np.dot(inv(Det_KM,26),Key_Matinverse_N1)%26
print(Key_Matinv)
print('利用解密矩陣解密(P=K^(-1)C)得到')
Decipher=np.matmul(Key_Matinv,C)%26
print(Decipher)
print("解密後的數字矩陣經過轉換，變為字母矩陣")
print(num_to_letter(Decipher))
decipher_M=num_to_letter(Decipher)
print('解密後的明文為')
decipher_text=mat_to_text(decipher_M)
print(decipher_text)
```

執行結果

以下的討論將用 2 階的矩陣來加密加密
HILL
請輸入明文　**Goodjob**
我們將使用希爾密碼來加密，你的加密矩陣 K =
[['H' 'I']
['L' 'L']]
經過轉換成數字矩陣變為
[[7　8]
[11 11]]
我們將明文 2 個 2 個分組，結果如下
[['G' 'O' 'J' 'B']
['O' 'D' 'O' 'X']]
明文矩陣經過轉換成數字矩陣變為
[[6 14　 9　 1]
[14　 3 14 23]]
利用加密矩陣加密(C=KP)得到
[[24 18 19　 9]
[12　 5 19　 4]]
數字矩陣經過轉換成字母矩陣變為
[['Y' 'S' 'T' 'J']
['M' 'F' 'T' 'E']]
加密後的密文為
YMSFTTJE

接著，我們來解密加密後的密文 **YMSFTTJE**
首先，我們將密文 2 個 2 個分組，結果如下
[['Y' 'S' 'T' 'J']
['M' 'F' 'T' 'E']]
再將字母數字化
[[24 18 19　 9]
[12　 5 19　 4]]
先求出解密矩陣 K 的反矩陣 K^(-1)
[[25 22]
[1 23]]
利用解密矩陣解密(P=K^(-1)C)得到
[[6 14　 9　 1]
[14　 3 14 23]]
解密後的數字矩陣經過轉換，變為字母矩陣
[['G' 'O' 'J' 'B']
['O' 'D' 'O' 'X']]
解密後的明文為
GOODJOBX