



# 資訊安全實習 ⑥

## 本實驗之目的

主要讓學員瞭解Matlab 操作與使用方法，並以此軟體實作AES。

- 安裝MATLAB
- AES會用到的基本指令
- 使用help與function browser
- VPN

## 實驗所需背景

- 了解 AES 理論與成因
- 使用 Matlab 實作

## 1.安裝 MATLAB

Step1	<p>進入資網資中心的首頁 <a href="http://www.inc.ndhu.edu.tw/bin/home.php">http://www.inc.ndhu.edu.tw/bin/home.php</a> 相關服務 -&gt; 一般服務 -&gt; 校園授權軟體</p> 
-------	---

Step2

點選 [下載校園授權軟體](#)

校園授權軟體

注意事項：

- 一、授權範圍「全校」定義：東華大學校園範圍內皆可使用。
- 二、授權範圍「行政及教學單位」定義：
  1. 全校行政、教學使用之電腦，包含辦公室、實驗室、電腦教室、研究室及教職員宿舍等。
  2. 學生宿舍及個人使用電腦不涵蓋在內。
- 三、授權範圍「Concurrent」定義：
  1. 使用範圍同「全校」之定義。
  2. 程式同一時間能執行之套數受購買之License量為限。
  3. 若有非「全校」皆可安裝之限制則會特別註明。
- 四、授權範圍為「XX套」之軟體，可安裝範圍為「行政及教學單位」。安裝套數則受購買套數之限制。
- 五、微軟大量授權之作業系統有使用限制，請全校師生特別注意。[微軟作業系統授權限制說明]
- 六、若無看到下載連結，請先確定是否在學校裡面且請勿使用proxy。
- 七、中心所屬電腦教室軟體安裝列表：[電腦教室相關資訊]
- 八、請確實遵守「著作權法」及相關法令規定。

[下載網頁使用說明&常見問題](#) | [下載校園授權軟體](#)

軟體名稱	授權範圍或
CorelDRAW X3	全校
自然輸入法 9	全校
嗶蝦米輸入法 5.7&6&7	全校

Step3

依照資網中心的規則去輸入帳號密碼  
再點選登入

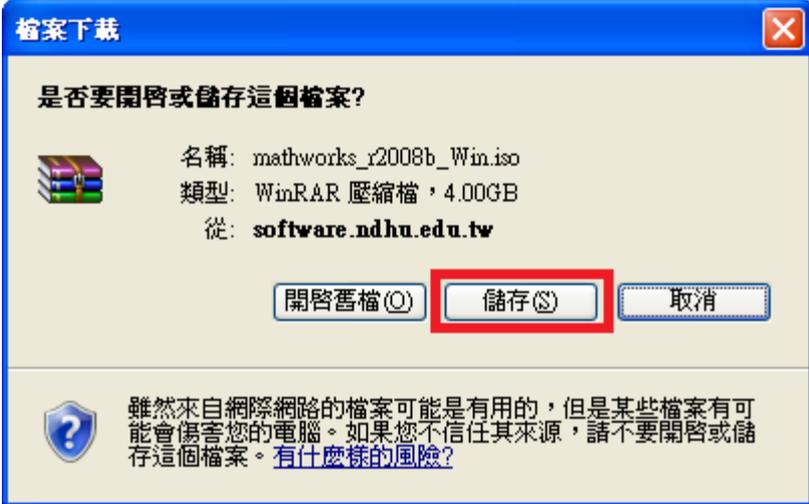
授權軟體使用者登入畫面

電子郵件帳號：

例如：inc@mail.ndhu.edu.tw 只需打 inc 即可

電子郵件密碼：

[English Version](#)

<p>Step4</p>	<p>請點選學習軟體底下的<a href="#">MATLAB R2008b Windows 平台 (DVD)</a></p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p><b>學習軟體</b></p> <table border="0" style="width: 100%;"> <tr> <td>BookFlix 線上電子書</td> <td>EndNote X5 for MAC</td> </tr> <tr> <td>EndNoteX2 For Mac OS 10.4.1 or higher</td> <td>EndNoteX2 For Windows</td> </tr> <tr> <td>EndNoteX3 For Mac OS 10.4.1 or higher</td> <td>EndNoteX3 For Windows</td> </tr> <tr> <td>EndNoteX4 For Mac</td> <td>EndNoteX4 For Windows</td> </tr> <tr> <td>EndNoteX5 For Windows</td> <td>MATLAB R2008b UNIX Linux Mac</td> </tr> <tr> <td style="border: 2px solid red;">MATLAB R2008b Windows平台 (DVD)</td> <td>SAS 9.1.3 2010年 授權碼 (非安裝)</td> </tr> <tr> <td>SPSS 11</td> <td>SPSS 14</td> </tr> <tr> <td>SYSTAT 12</td> <td>譯點通 9.0</td> </tr> <tr> <td>譯典通 7.0</td> <td></td> </tr> </table> </div>	BookFlix 線上電子書	EndNote X5 for MAC	EndNoteX2 For Mac OS 10.4.1 or higher	EndNoteX2 For Windows	EndNoteX3 For Mac OS 10.4.1 or higher	EndNoteX3 For Windows	EndNoteX4 For Mac	EndNoteX4 For Windows	EndNoteX5 For Windows	MATLAB R2008b UNIX Linux Mac	MATLAB R2008b Windows平台 (DVD)	SAS 9.1.3 2010年 授權碼 (非安裝)	SPSS 11	SPSS 14	SYSTAT 12	譯點通 9.0	譯典通 7.0	
BookFlix 線上電子書	EndNote X5 for MAC																		
EndNoteX2 For Mac OS 10.4.1 or higher	EndNoteX2 For Windows																		
EndNoteX3 For Mac OS 10.4.1 or higher	EndNoteX3 For Windows																		
EndNoteX4 For Mac	EndNoteX4 For Windows																		
EndNoteX5 For Windows	MATLAB R2008b UNIX Linux Mac																		
MATLAB R2008b Windows平台 (DVD)	SAS 9.1.3 2010年 授權碼 (非安裝)																		
SPSS 11	SPSS 14																		
SYSTAT 12	譯點通 9.0																		
譯典通 7.0																			
<p>Step5</p>	<p>點選儲存</p> 																		
<p>Step6</p>	<p>需要一點點時間等待 先去學校信箱收認證信</p> 																		

Step7 進入信箱會收到資網中心的信

日來源: ccop@mail.ndhu.edu.tw  
 收信: u9721020@ems.ndhu.edu.tw  
 標題: MATLAB R2008b Windows平台 (DVD) [\[加入標籤\]](#)  
 日期: Sun, 3 Jun 2012 20:57:43 +0800 (CST)

- 1.請先下載安裝過程所需的license檔案。  
[http://software.ndhu.edu.tw/MATLAB\\_2008b\\_license.dat](http://software.ndhu.edu.tw/MATLAB_2008b_license.dat)
- 2.在出選安裝視窗時 選 "Install manually without using the Internet"
- 3.在"Provide File Installaion Key"畫面時選擇"I have the File Installation Key for my license." 並輸入序號"29071-1-28432-38713"
- 4."Provide license file location"畫面時選取步驟1所下載的檔案。
- 5.安裝動作結束後，即完成。

註備：  
 [1]請先檢查下載之檔案大小是否為"4,301,848,576 位元組"，若不一樣，請重新下載。  
 [2]亦可使用md5sum 檢察iso檔：cd6b3fbb152398b963bda8a51a3d5a98  
 [3]此檔案為光碟映像檔，使用方式簡單來說有二種。  
 1.燒錄成光碟片：若使用燒錄成光碟片之方式，在燒錄時請使用燒錄映像檔的方式燒錄。  
 2.用光碟模擬程式(免燒光碟片)：請參考此網頁 <http://software.ndhu.edu.tw/doc/alccohol/index.html>

Step8 將信中第一點所需的檔案下載下來  
 對著網址點右鍵 -> 另存目標 放到你記得的位子即可  
 先暫時把此檔案擱著 最後認證才會使用到

Mail2000電子信箱--u9721020 - Windows Internet Explorer  
<http://ems.ndhu.edu.tw/cgi-bin/star?m=1296092642&wzap=1>

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)  
 我的最愛 建議的網站 自訂連結 免費的 Hotmail 取得更多附加元件

Mail2000電子信箱--u9721020

**Mail2000** V4.5

u9721020 收信匣 460封信, 1 / 5頁

信件匣  
 收信匣 (460)  
 虛擬信件匣  
 送信匣 (64/249)  
 草稿匣 (2/31)  
 回收箱 (149/267)  
 廣告信件  
 信件匣管理  
 預約寄信管理

通訊錄  
 我的檔案  
 信箱服務  
 個人設定

日來源: ccop@mail.ndhu.edu.tw  
 收信: u9721020@ems.ndhu.edu.tw  
 標題: MATLAB R2008b Windows平台 (DVD) [\[加入標籤\]](#)  
 日期: Sun, 3 Jun 2012 20:57:43 +0800 (CST)

- 1.請先下載安裝過程所需的license檔案。  
[http://software.ndhu.edu.tw/MATLAB\\_2008b\\_license.dat](http://software.ndhu.edu.tw/MATLAB_2008b_license.dat)
- 2.在出選安裝視窗時 選 "Install manually without using the Internet"
- 3.在"Provide File Installaion Key"畫面時選擇"I have the File Installation Key for my license." 並輸入序號"29071-1-28432-38713"
- 4."Provide license file location"畫面時選取步驟1所下載的檔案。
- 5.安裝動作結束後，即完成。

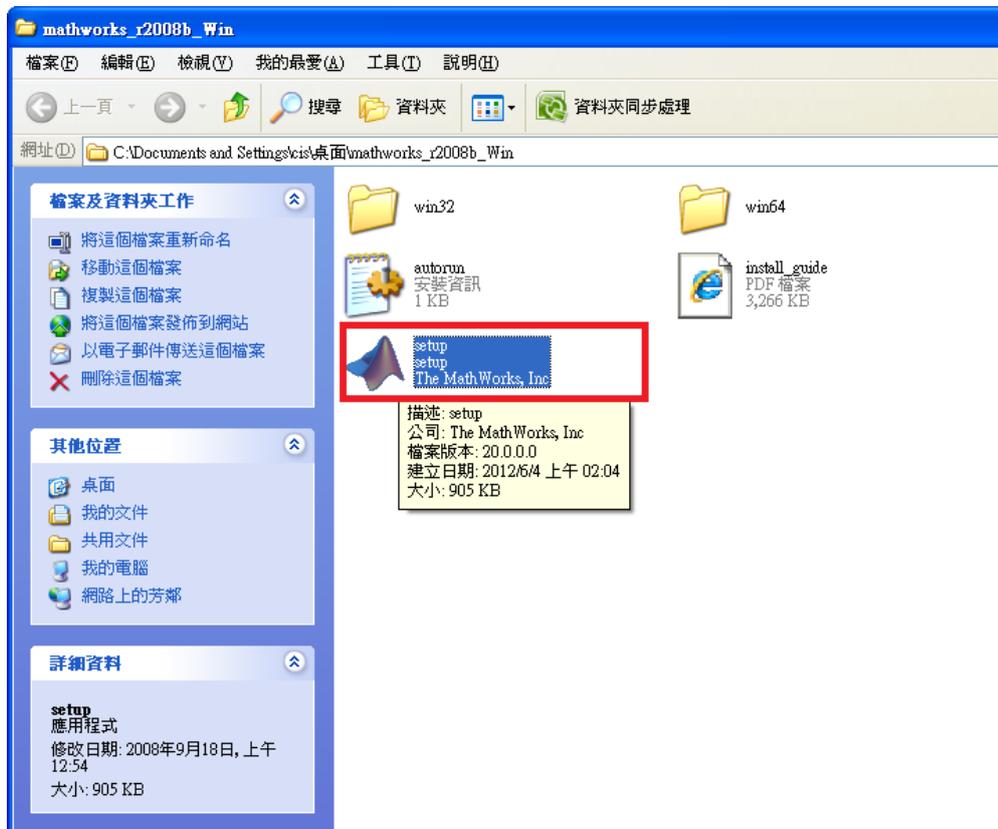
註備：  
 [1]請先檢查下載之檔案大小是否為"4,301,848,576 位元組"，若不一樣，請重新下載。  
 [2]亦可使用md5sum 檢察iso檔：cd6b3fbb152398b963bda8a51a3d5a98  
 [3]此檔案為光碟映像檔，使用方式簡單來說有二種。  
 1.燒錄成光碟片：若使用燒錄成光碟片之方式，在燒錄時請使用燒錄映像檔的方式燒錄。  
 2.用光碟模擬程式(免燒光碟片)：請參考此網頁 <http://software.ndhu.edu.tw/doc/alccohol/index.html>

另存目標(A)...  
 列印目標(L)  
 剪下  
 複製(C)  
 複製捷徑(D)  
 貼上(E)

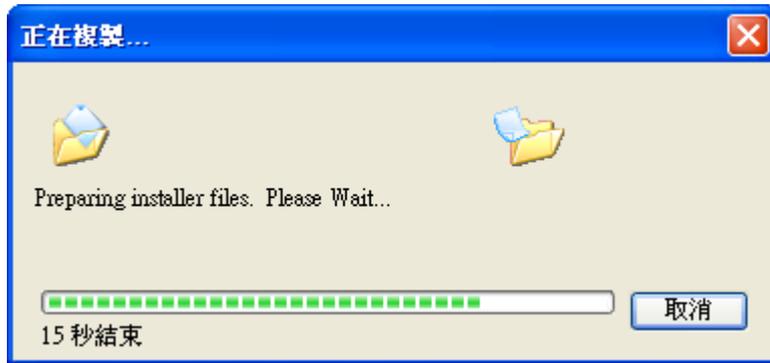
Step9 從資網中心下載完 MATLAB R2008b 的檔案後  
對此檔案點右鍵 -> 將檔案解壓縮出來



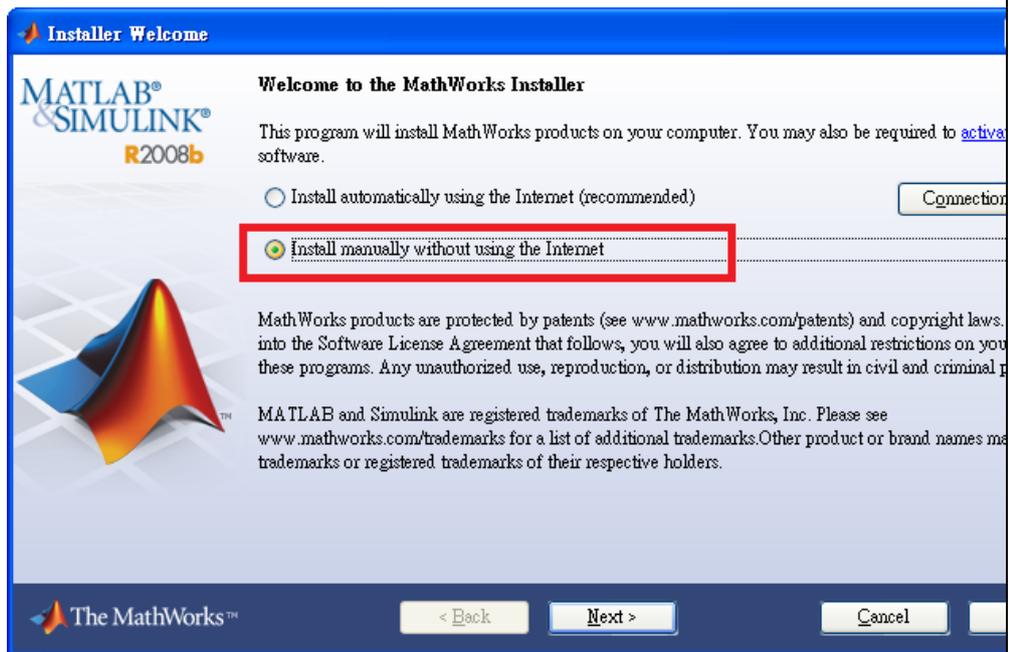
Step10 對 setup 點兩下



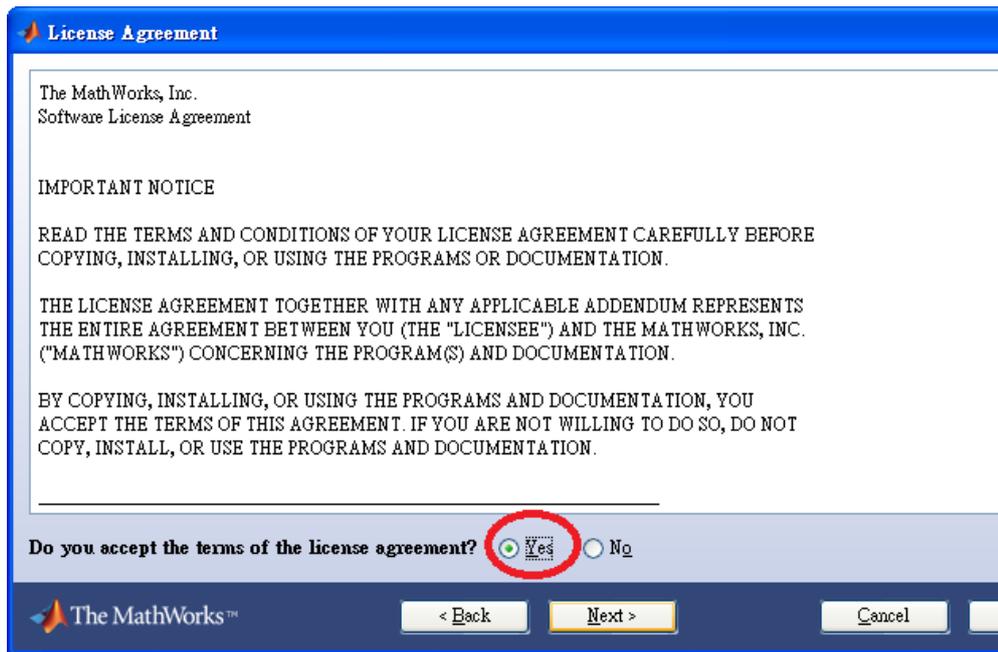
Step11 等待一會兒



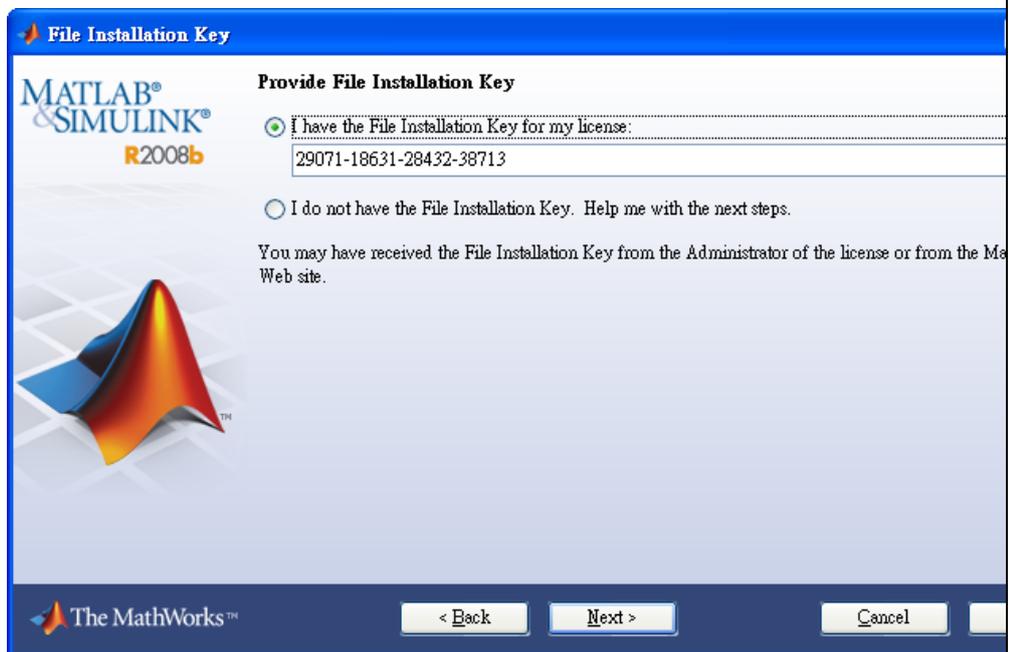
Step12 點選"Install manually without using the Internet"  
即可按 next



Step13 點選 yes 即可按 next

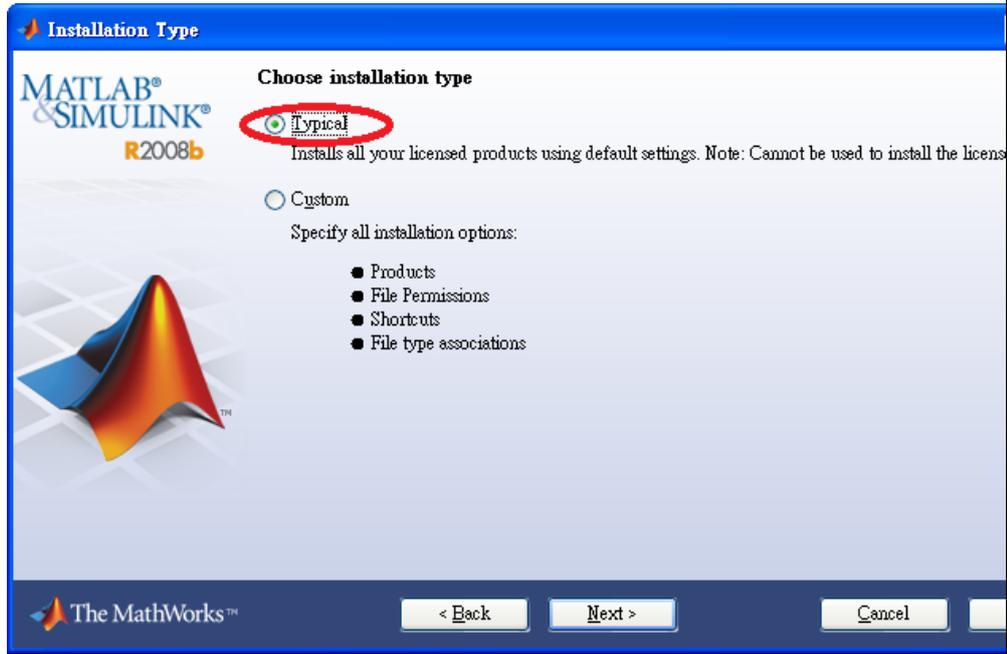


Step14 選擇"I have the File Installation Key for my license."  
並輸入序號"29071-18631-28432-38713"  
(學校的認證信有提供序號)  
即可按 next



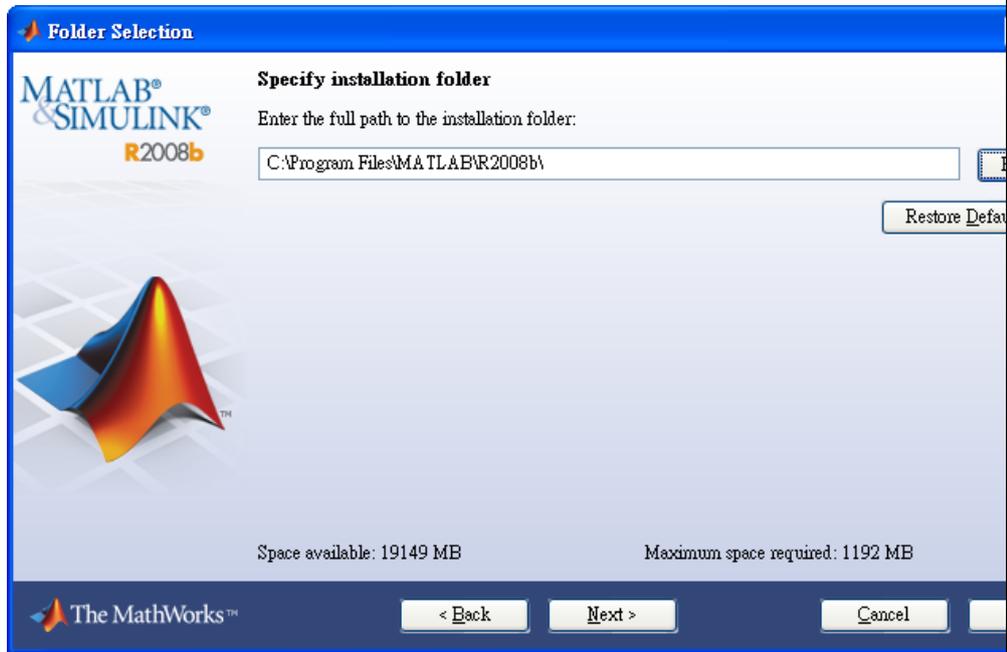
Step15

選擇 Typical  
即可按 next

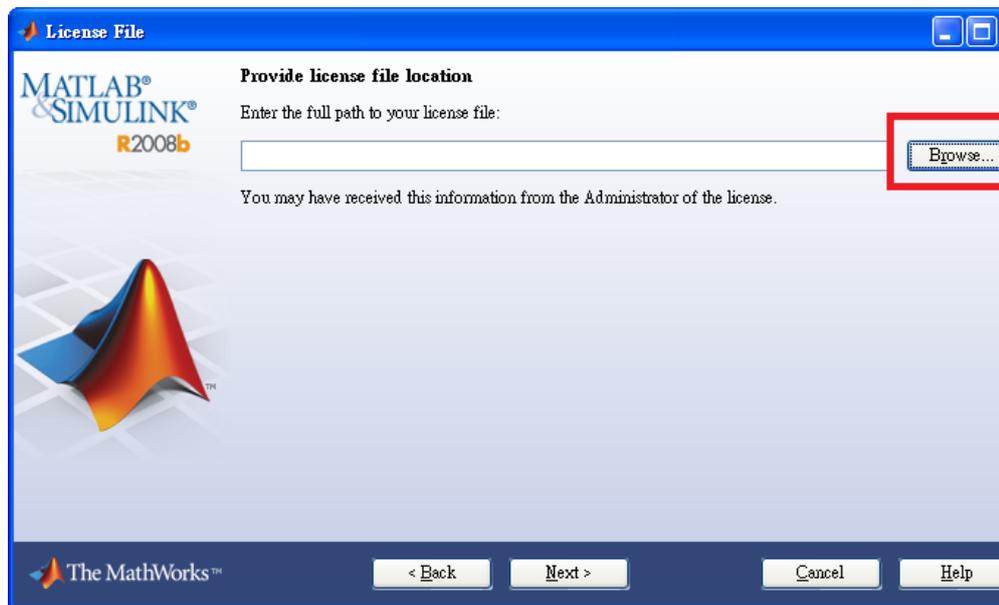


Step16

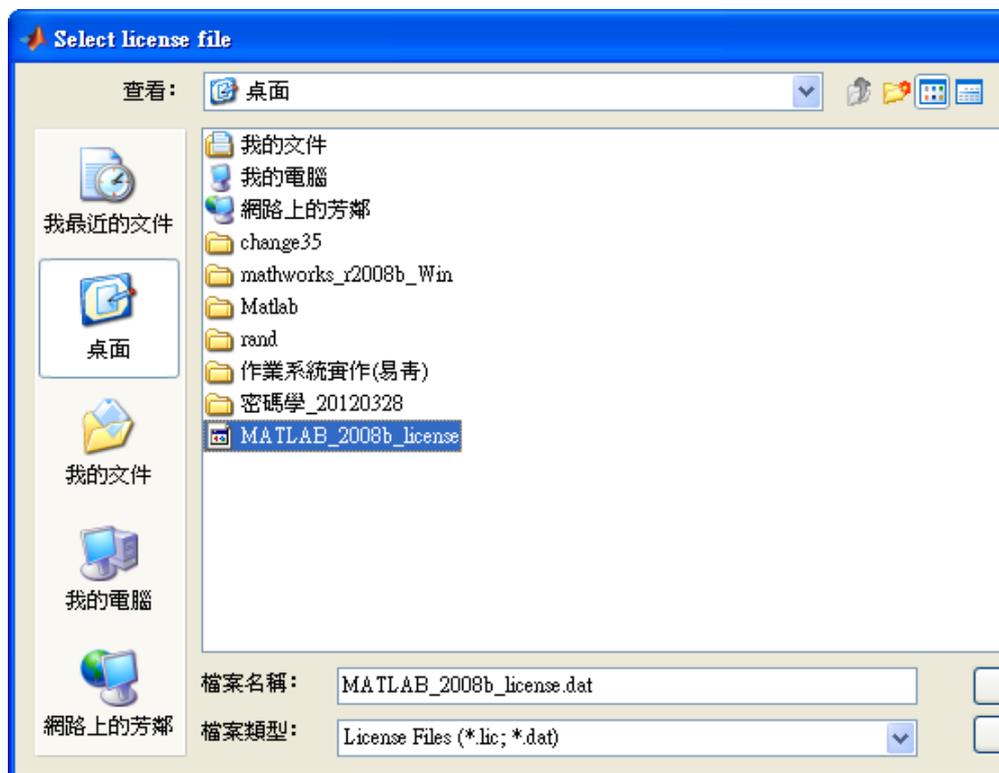
選擇安裝路徑  
即可按 next



Step17 點選 Brown

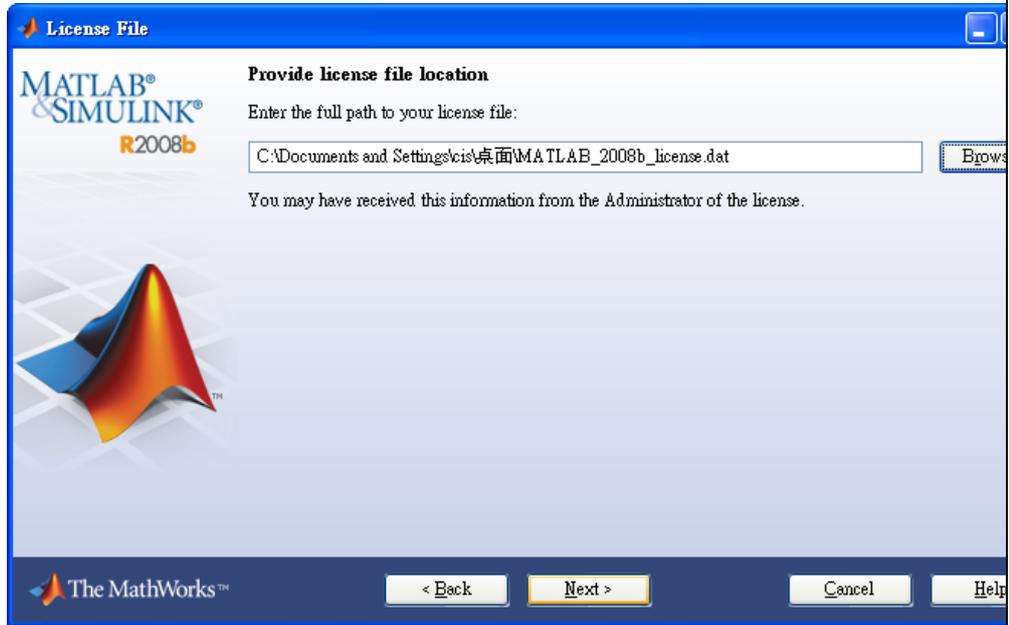


Step18 選擇在 Step8 所下載的認證的檔案



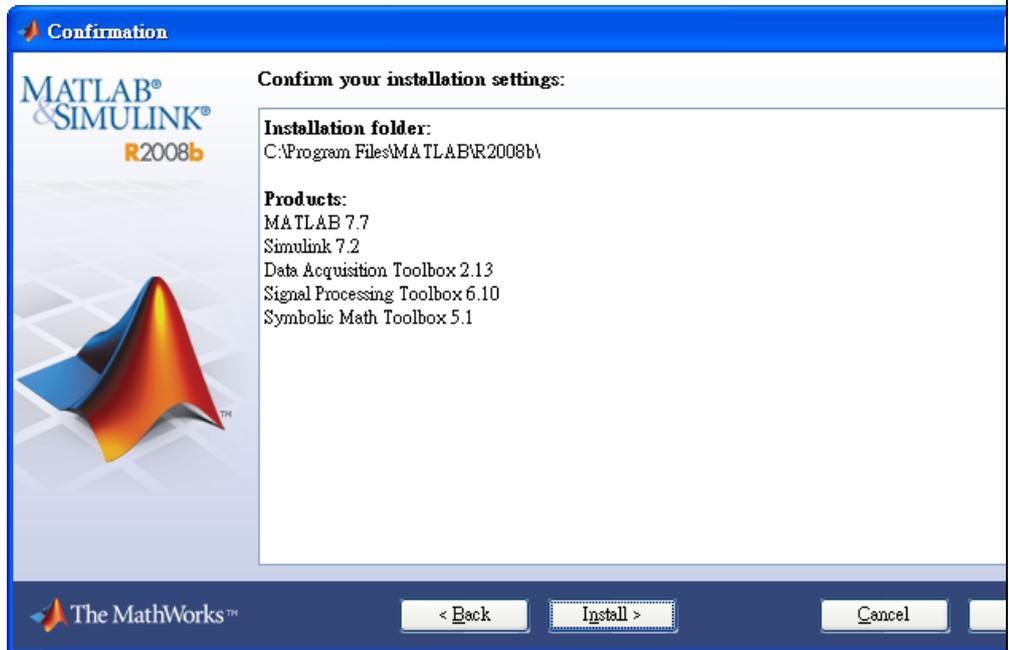
Step19

選擇成功後  
即可按 next

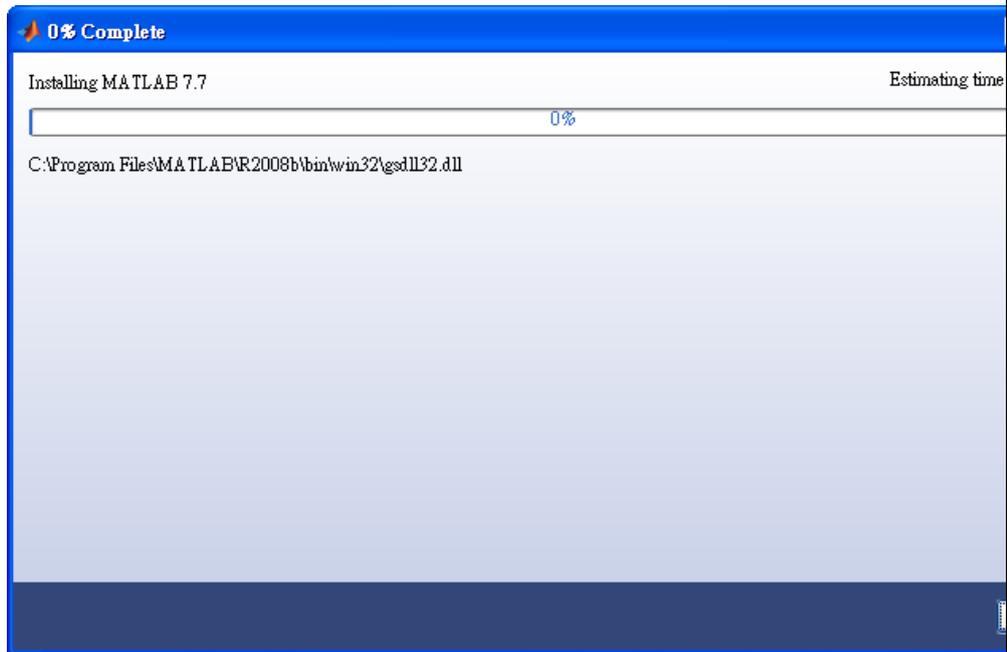


Step20

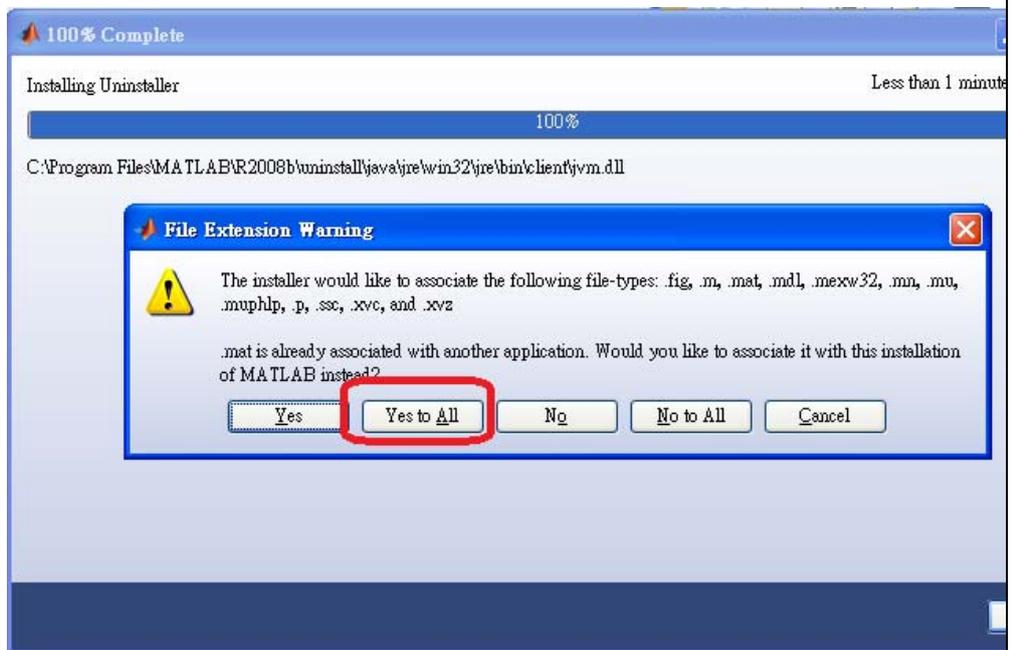
選擇 Install



Step21 等待一些時間安裝

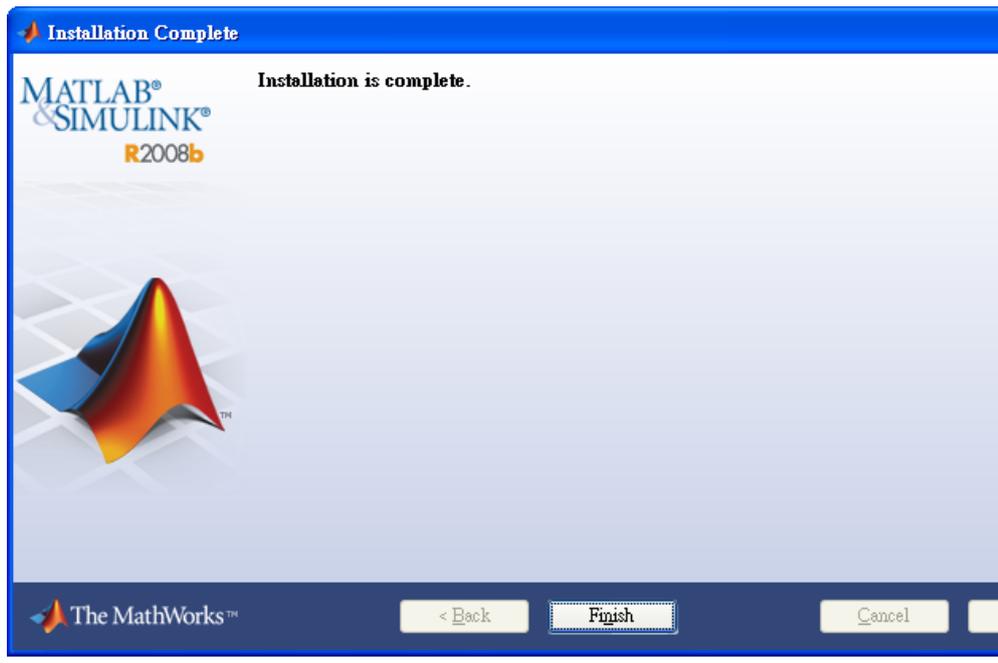


Step22 選擇 Yes to All



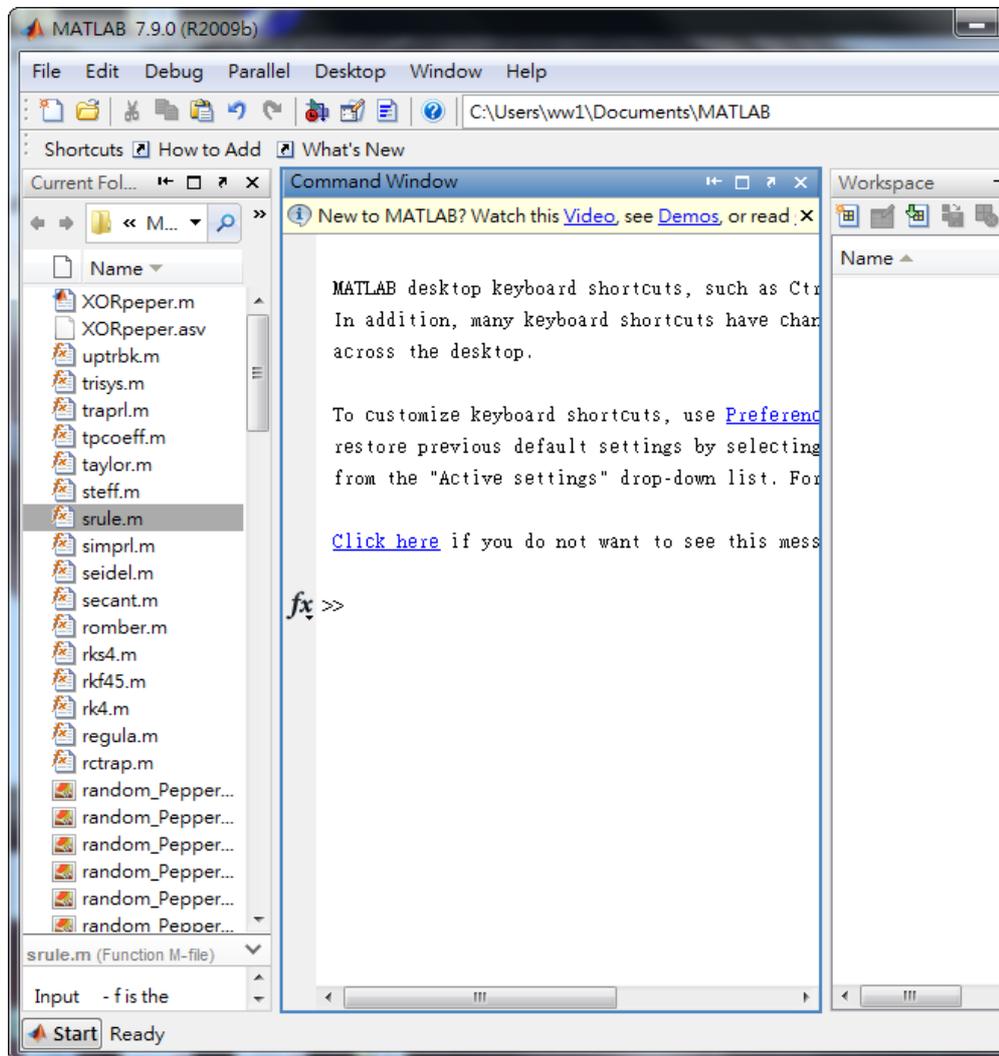
Step23

點選 Finish

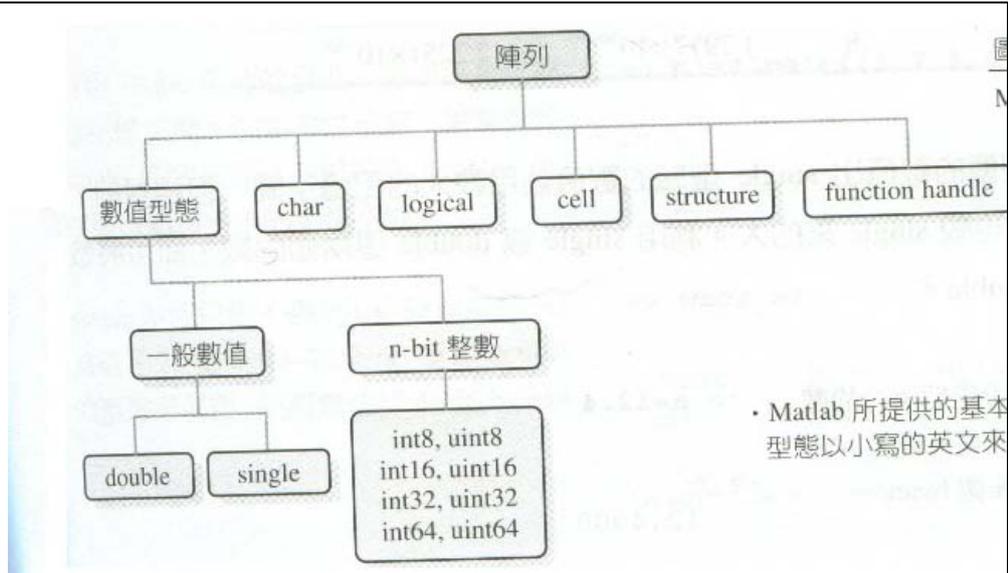


## 2. AES 會用到的基本指令

Step1 打開 matlab 介面



Step2



將要下的指令打在 command window  
普通陣列初始

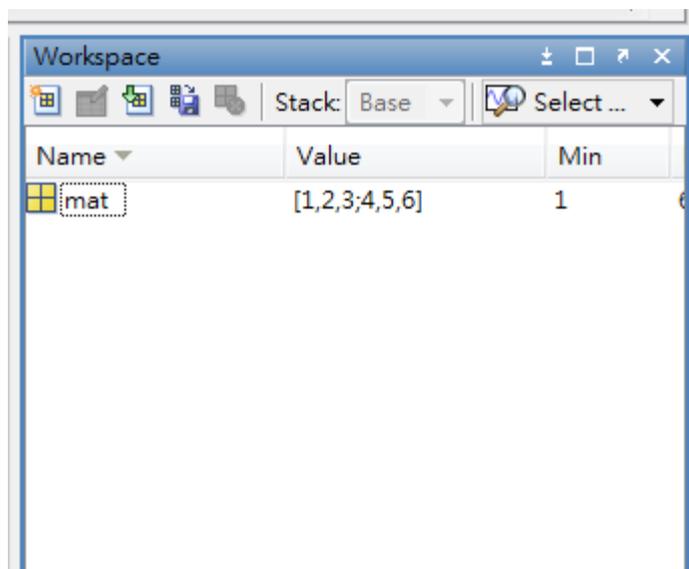
```
>> mat=[1 2 3;
        4 5 6;];
mat=[1 2 3;
     4 5 6;]

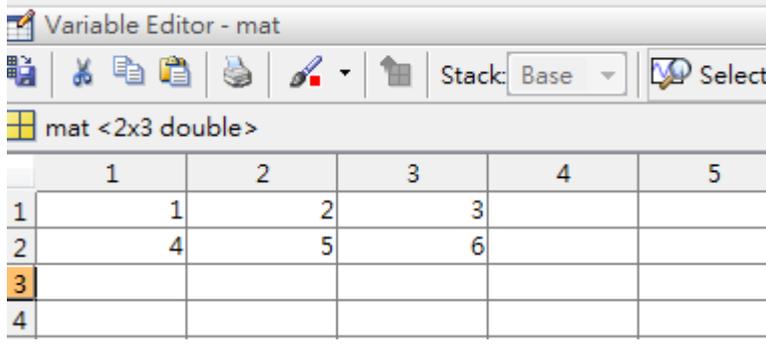
mat =

     1     2     3
     4     5     6
```

Step3

可以看到宣告的變數或陣列



Step4	<p>可以直觀的看到陣列的數值</p>  <p>The screenshot shows the MATLAB Variable Editor window for a variable named 'mat'. The variable is a 2x3 double matrix. The values are displayed in a grid with columns labeled 1 through 5 (though only 3 columns have data) and rows labeled 1 through 4 (though only 2 rows have data). The values are: Row 1: 1, 2, 3; Row 2: 4, 5, 6. The third row is highlighted in orange.</p>
Step5	<p>觀察數值</p> <pre data-bbox="363 701 558 936"> &gt;&gt; mat(1,2)  ans =      2 </pre>
Step6	<p>存入數值</p> <pre data-bbox="363 1037 678 1272"> &gt;&gt; storage=mat(1,2)  storage =      2 </pre>
Step7	<p>觀察列 or 排的數值</p>

```

>> mat(1,1:2)

ans =

     1     2

>> mat(1,1:end)

ans =

     1     2     3

>> mat(1,:)

ans =

     1     2     3

>> mat(:,2)

ans =

     2
     5

```

Step8 陣列-cell 的應用  
陣列初始

```

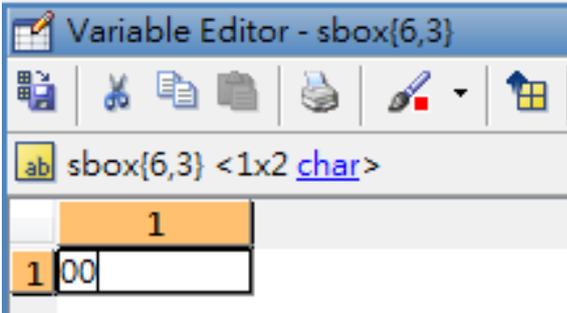
C{1}=(1:2);
C{2}=(1);
C{3}=(1:3);

```

Step9 每格的裡面的 size 可以不同

 C <1x3 cell>

	1	2	3
1	[1,2]	1	[1,2,3]

Step10	<p>可應用在 s-box</p> <pre>sbox={     '63' '7c' '77' '7b' 'f2' '6b' '6f' 'c5' '30' '01' '67' '2b' 'fe' 'd7' 'ab     'ca' '82' 'c9' '7d' 'fa' '59' '47' 'f0' 'ad' 'd4' 'a2' 'af' '9c' 'a4' '72     'b7' 'fd' '93' '26' '36' '3f' 'f7' 'cc' '34' 'a5' 'e5' 'f1' '71' 'd8' '31     '04' 'c7' '23' 'c3' '18' '96' '05' '9a' '07' '12' '80' 'e2' 'eb' '27' 'b2     '09' '83' '2c' '1a' '1b' '6e' '5a' 'a0' '52' '3b' 'd6' 'b3' '29' 'e3' '2f     '53' 'd1' '00' 'ed' '20' 'fc' 'b1' '5b' '6a' 'cb' 'be' '39' '4a' '4c' '58     'd0' 'ef' 'aa' 'fb' '43' '4d' '33' '85' '45' 'f9' '02' '7f' '50' '3c' '9f     '51' 'a3' '40' '8f' '92' '9d' '38' 'f5' 'bc' 'b6' 'da' '21' '10' 'ff' 'f3     'cd' '0c' '13' 'ec' '5f' '97' '44' '17' 'c4' 'a7' '7e' '3d' '64' '5d' '19     '60' '81' '4f' 'dc' '22' '2a' '90' '88' '46' 'ee' 'b8' '14' 'de' '5e' '0b     'e0' '32' '3a' '0a' '49' '06' '24' '5c' 'c2' 'd3' 'ac' '62' '91' '95' 'e4     'e7' 'c8' '37' '6d' '8d' 'd5' '4e' 'a9' '6c' '56' 'f4' 'ea' '65' '7a' 'ae     'ba' '78' '25' '2e' '1c' 'a6' 'b4' 'c6' 'e8' 'dd' '74' '1f' '4b' 'bd' '8b     '70' '3e' 'b5' '66' '48' '03' 'f6' '0e' '61' '35' '57' 'b9' '86' 'c1' '1d     'e1' 'f8' '98' '11' '69' 'd9' '8e' '94' '9b' '1e' '87' 'e9' 'ce' '55' '28     '8c' 'a1' '89' '0d' 'bf' 'e6' '42' '68' '41' '99' '2d' '0f' 'b0' '54' 'bb };</pre>
Step11	<p>要是在一般普通的陣列只會看到 0</p> <pre>sbox(6,3)  ans =      '00'</pre>
Step12	 <p>The screenshot shows the MATLAB Variable Editor window titled 'Variable Editor - sbox{6,3}'. The variable 'sbox{6,3}' is shown with a value of '00'. The editor displays a grid where the first row contains the number '1' and the first column contains the number '1', with the cell at the intersection containing the value '00'.</p>
Step13	<p>型態跟數值的取出</p> <p>()- 取出型態</p> <p>{}-取出數值</p>

	<pre>&gt;&gt; sbox(6,3)  ans =      '00'  &gt;&gt; sbox{6,3}  ans =      00</pre>
Step14	<p>取出每個位元的方法</p> <pre>&gt;&gt; sbox{4,1}  ans =      04  &gt;&gt; sbox{4,1}(1,1)  ans =      0  &gt;&gt; sbox{4,1}(1,2)  ans =      4  &gt;&gt; sbox{4,1}(1,1:end)  ans =      04</pre>
Step15	<p>迴圈的宣告(九九乘法表)</p> <pre>&gt;&gt; clear &gt;&gt; for i=1:9     for j=1:9         mutil(i,j)=i*j;     end end</pre>

Step16

Variable Editor - mutil

Stack: Base No valid plots for: mutil(9,...)

mutil <9x9 double>

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	10	12	14	16	18
3	3	6	9	12	15	18	21	24	27
4	4	8	12	16	20	24	28	32	36
5	5	10	15	20	25	30	35	40	45
6	6	12	18	24	30	36	42	48	54
7	7	14	21	28	35	42	49	56	63
8	8	16	24	32	40	48	56	64	72
9	9	18	27	36	45	54	63	72	81
10									

Step17 If...else 範例

```
>> dog=15; pig=51;
>> if (pig<dog)
    pig=0;
else
    dog=0;
end
```

Workspace:

Name	Value
pig	51
dog	0

Step18 處理各式資料型態

n-bit 整數可分為有號 (signed) 與無號 (unsigned) 兩種，所謂的有號，是指整數可有正負數的存在，而無號則只容許正數。無論是有號或無號整數，依其大小可分為 8、16、32 與 64 個位元 (bits) 的整數，如下表所列：

表 2.5.2 n-bit 整數型態

資料型態	說明	位元組	最大值	最小值
int8	8-bit 整數	1	127	-128
uint8	8-bit 無號整數	1	255	0
int16	16-bit 整數	2	32767	-32768
uint16	16-bit 無號整數	2	65535	0
int32	32-bit 整數	4	2147483647	-2147483648

	<pre> &gt;&gt; 10/4  ans =      2.5000  &gt;&gt; a=fix(ans) %無條件捨去  a =       2  &gt;&gt; b=uint8(ans) %四捨五入  b =       3 </pre>
Step19	<pre> 16,10,2 進位換算  'ab'  a=hex2dec(ans)%16進位轉成10進位  b=dec2bin(a)%10進位轉成2進位  c=bin2dec(b)%2進位轉成10進位  ans =  ab  a =      171  b =  10101011  c =  171  </pre>

Step20

bitxor 的應用

```
>> clear
a='1a';
b='02';
a=uint8(hex2dec(a)) %轉成10進位 且要int型態
b=uint8(hex2dec(b)) %轉成10進位 且要int型態
c=bitxor(a,b) %a,b一定要10進位
d=dec2hex(c) %最後擺放回去要記得轉回16進位
```

```
a =
    26

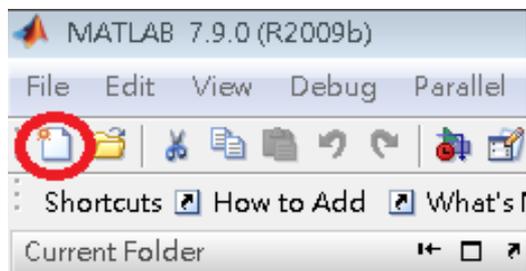
b =
     2

c =
    24

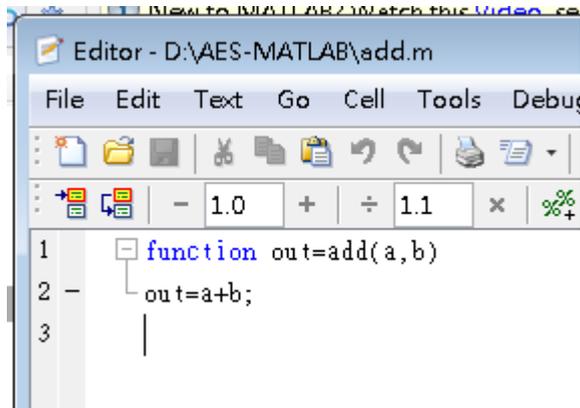
d =
    18
```

Step21

製作 function 首先要開啟新檔 (M-file)

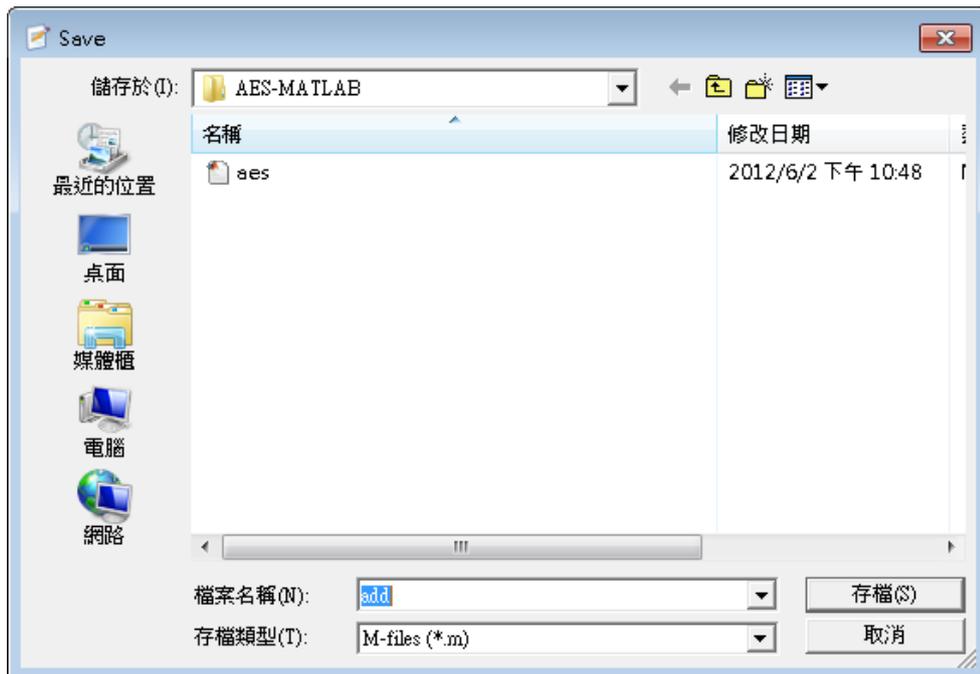


Step22 先把要打的內容先輸入完  
最後在第一行加上 function

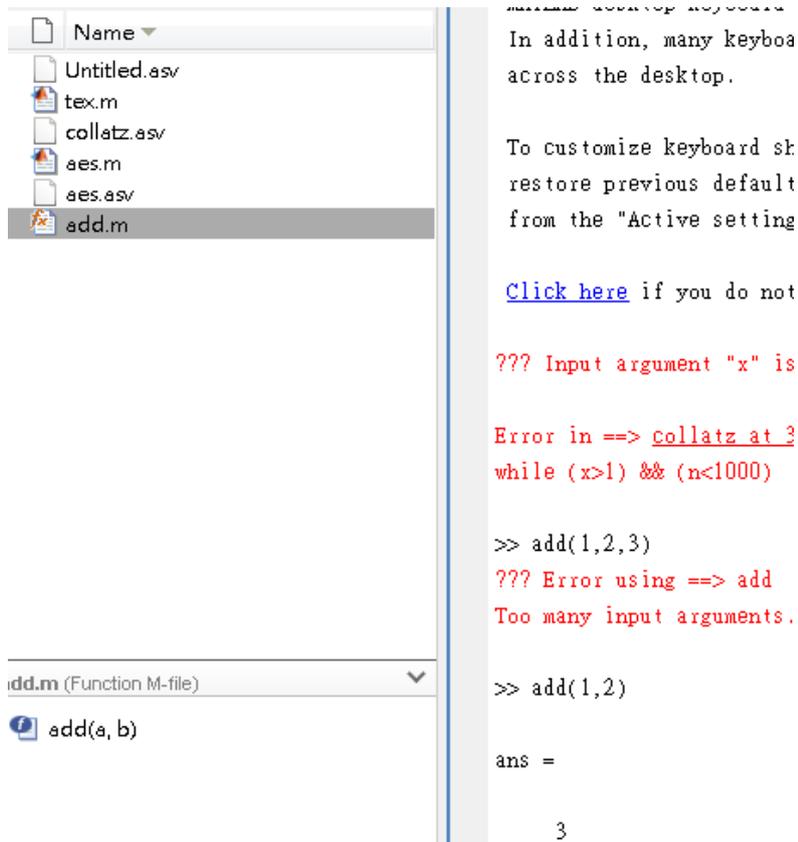


```
Editor - D:\AES-MATLAB\add.m
File Edit Text Go Cell Tools Debug
- 1.0 + ÷ 1.1 × %
1 function out=add(a,b)
2 -   out=a+b;
3   |
```

Step23 存檔時 檔名要注意



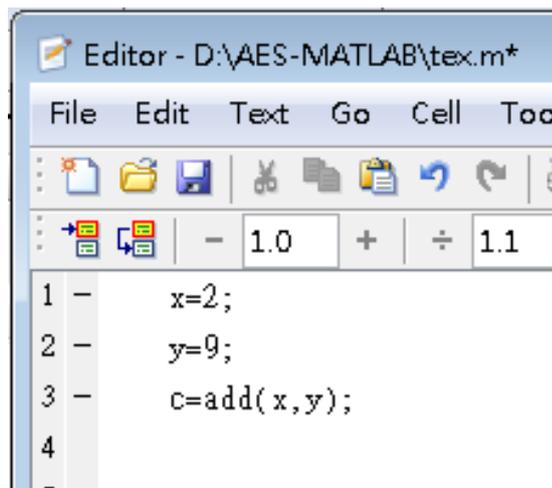
Step24 可看到建立的 function



The screenshot shows the MATLAB IDE interface. On the left, a file browser displays a list of files: 'Untitled.asv', 'tex.m', 'collatz.asv', 'aes.m', 'aes.asv', and 'add.m'. The 'add.m' file is selected. Below the file browser, the 'add.m' file is open, showing the function definition: `add(a, b)`. On the right, the command window displays the following text:

```
??? Input argument "x" is  
Error in ==> collatz at 3  
while (x>1) && (n<1000)  
  
>> add(1,2,3)  
??? Error using ==> add  
Too many input arguments.  
  
>> add(1,2)  
  
ans =  
  
3
```

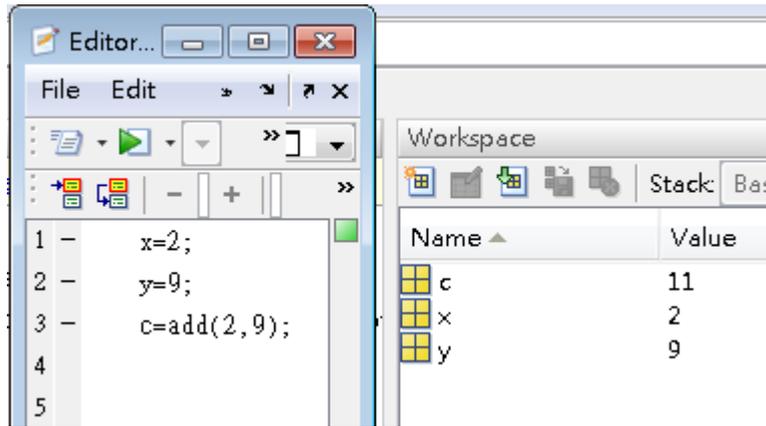
Step25 呼叫使用



The screenshot shows a MATLAB editor window titled 'Editor - D:\AES-MATLAB\tex.m\*'. The window has a menu bar with 'File', 'Edit', 'Text', 'Go', 'Cell', and 'Too'. Below the menu bar is a toolbar with various icons. The editor area shows the following code:

```
1 - x=2;  
2 - y=9;  
3 - c=add(x,y);  
4  
5
```

Step26



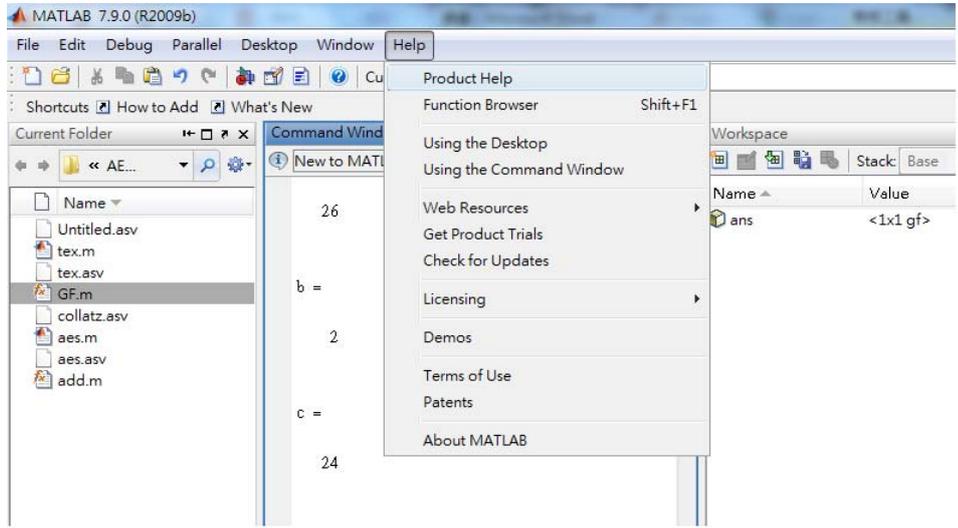
Step27

GF(2^8) 乘法 ( <http://sna.csie.ndhu.edu.tw/~cnyang/Matlab/gf28.m> )

```
>> gf28(2,135)  
  
ans =  
  
    19  
  
>> gf28(3,110)  
  
ans =  
  
    178  
  
|
```

Step1

Help -> Product Help



Step2

The screenshot shows the MATLAB Help window for the 'xor' function. The left pane shows search results for 'xor'. The main pane displays the following information:

**xor**  
Logical exclusive-OR

**Syntax**  
`C = xor(A, B)`

**Description**  
C = `xor(A, B)` performs an exclusive OR operation on the corresponding elements of arrays A and B. The resulting element C(i, j, ...) is logical true (1) if A(i, j, ...) or B(i, j, ...), but not both, is nonzero.

A	B	C
Zero	Zero	0
Zero	Nonzero	1
Nonzero	Zero	1
Nonzero	Nonzero	0

**Examples**

Step3

The screenshot shows the MATLAB 7.9.0 (R2009b) interface. The Command Window contains the following code and output:

```

26
b =
    2
c =
    24
  
```

The Help menu is open, showing options such as Product Help, Function Browser (Shift+F1), Using the Desktop, Using the Command Window, Web Resources, Get Product Trials, Check for Updates, Licensing, Demos, Terms of Use, Patents, and About MATLAB.

Step4

The screenshot shows the MATLAB Function Browser for the 'xor' function. The list of functions includes:

- `xor`: Logical exclusive-OR
- `xor (fixedpoint)`: Logical exclusive-OR
- `bitxor`: Bitwise XOR
- `bsxfun`: Apply element-by-element...
- `findobj`: Locate graphics objects wit...
- `streamparticles`: Plot stream particles
- `opengl`: Control OpenGL rendering
- `polybool (map)`: Set operations on polygon...
- `crc.generator (comm)`: Construct CRC generator o...
- `crc.detector (comm)`: Construct CRC detector ob...
- `seqgen.pn (comm)`: Construct default PN sequ...
- `commsrc.pn (comm)`: Create PN sequence gener...

At the bottom, it says "All products".

Step5

Step6

```
>> xor(0,1)

ans =

     1
```

## 4. VPN

Step1

<http://net.ndhu.edu.tw/netservice-teach/2.html>  
住校外的人一定要登入 VPN 才能使用學校的 Matlab

### 問題與練習：

1. 輸入成 5 個數字，呼叫函式，回傳 1\*2 cell 類型的陣列，[1 1]為五數相加與五數相乘，[1 2]為五個數值中的最大值。

### 總結測驗：

1. 以 MATLAB 實作出 AES (6/22 驗收)。