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

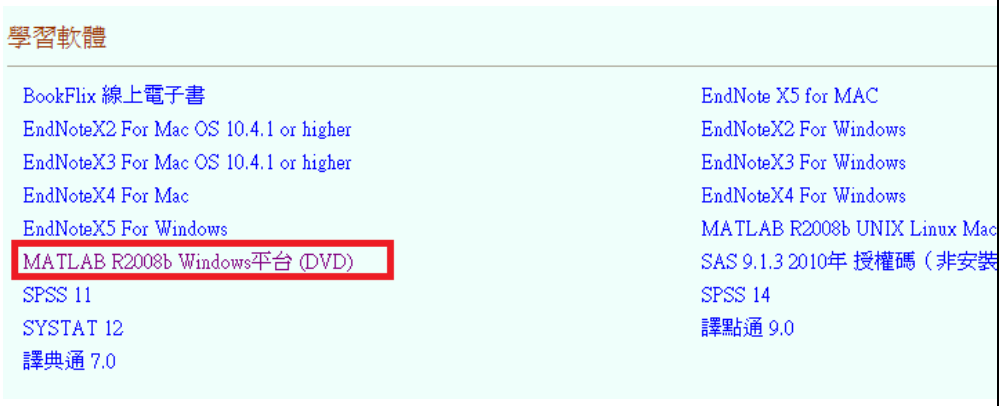
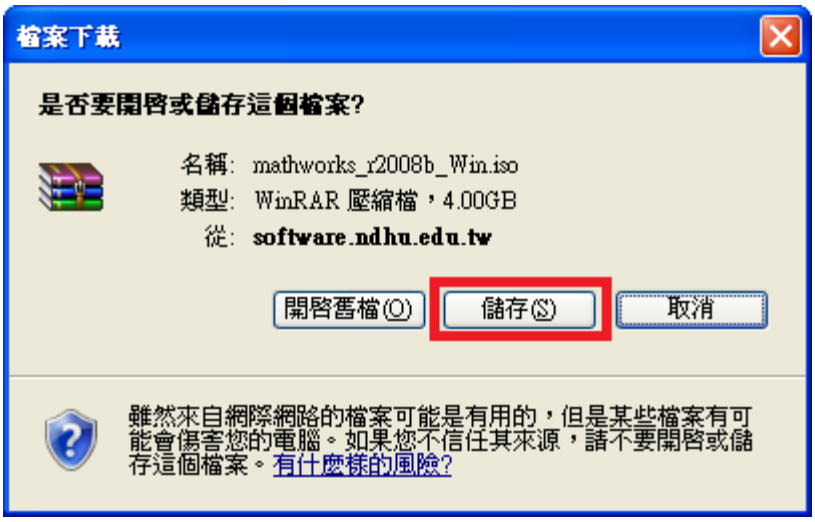
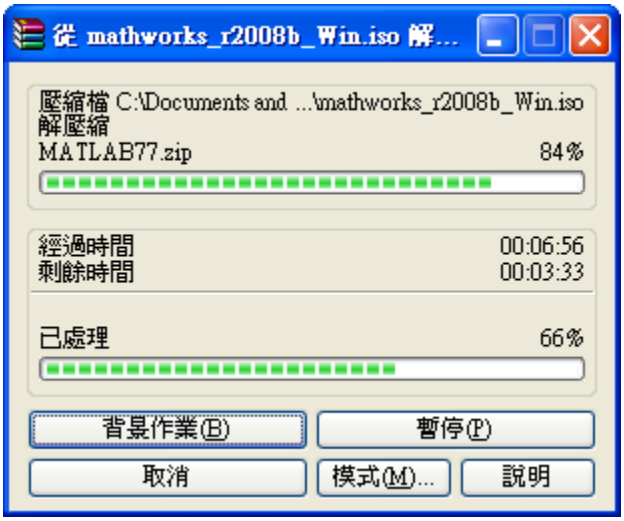
-了解 AES 理論與成因

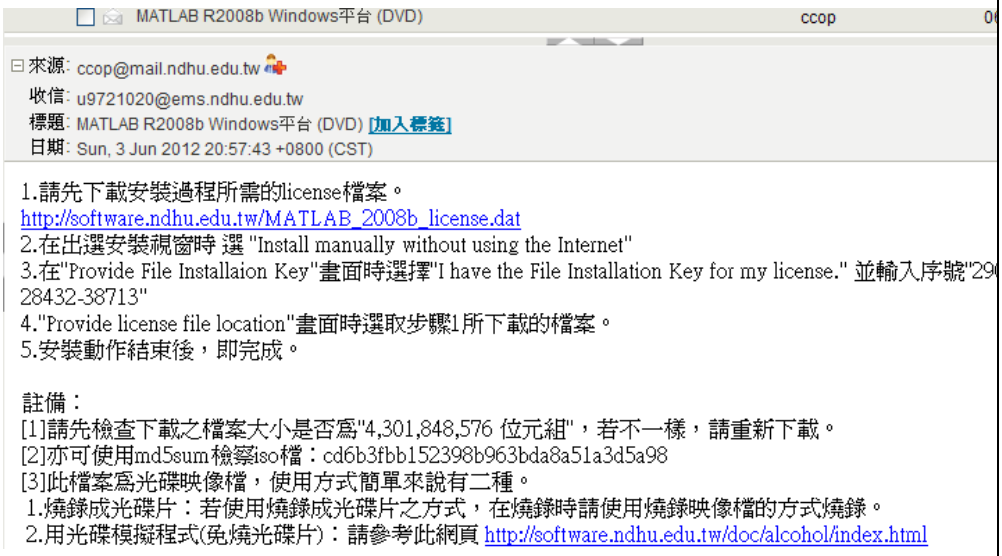
-使用 Matlab 實作

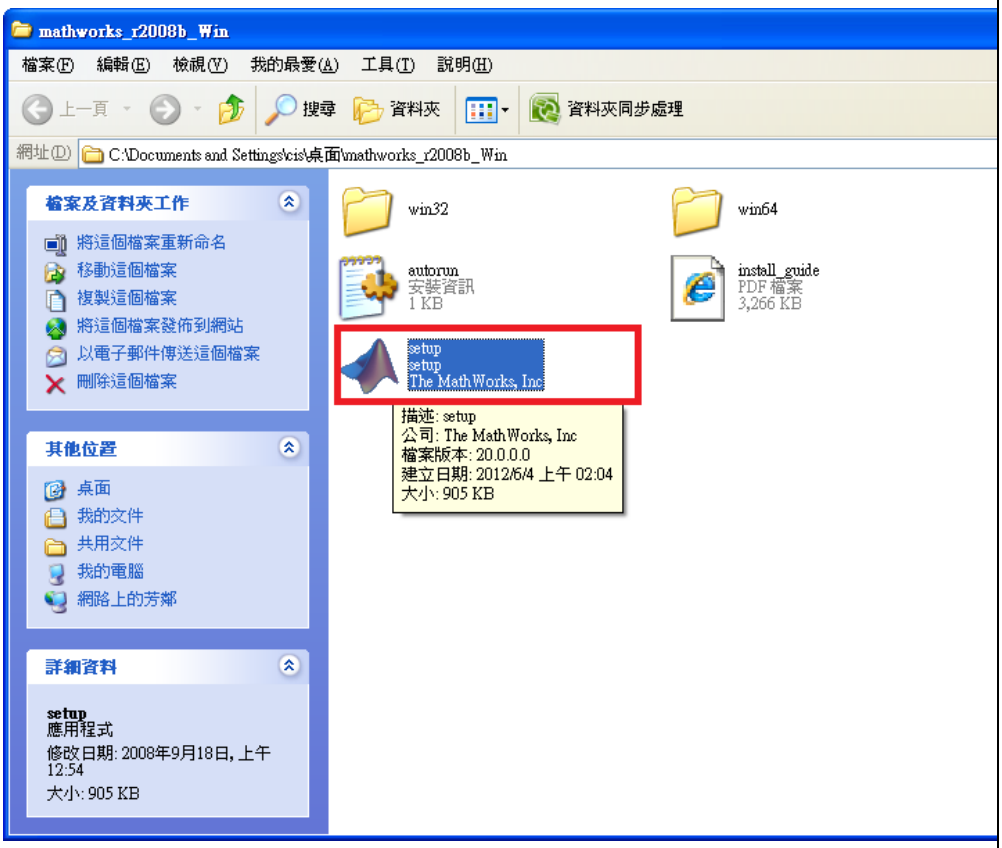
1.安裝 MATLAB

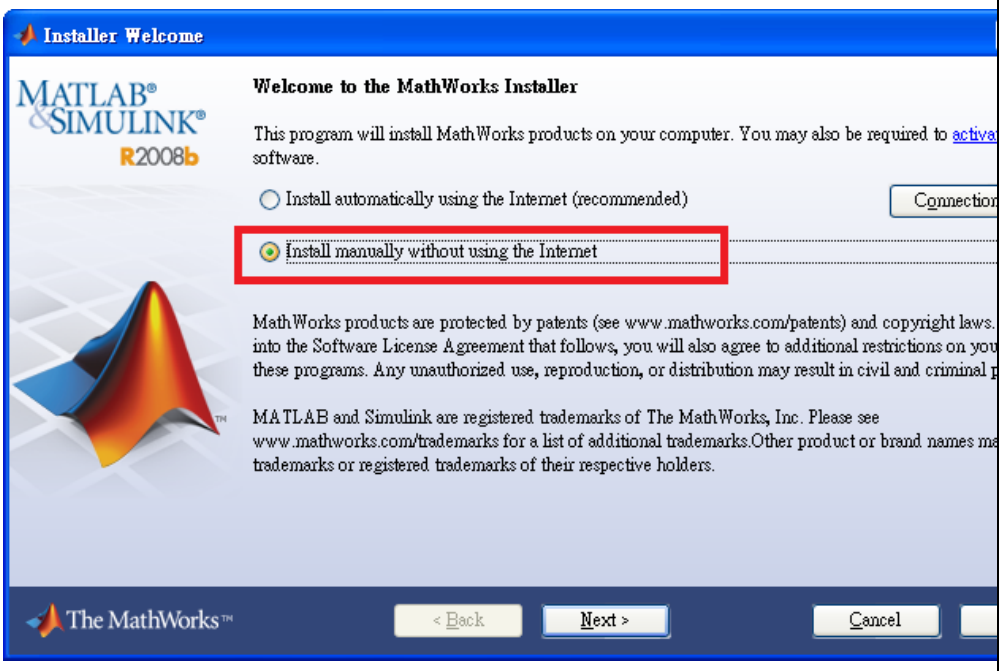
Step1	進入資網資中心的首頁 http://www.inc.ndhu.edu.tw/bin/home.php 相關服務 -> 一般服務 -> 校園授權軟體 

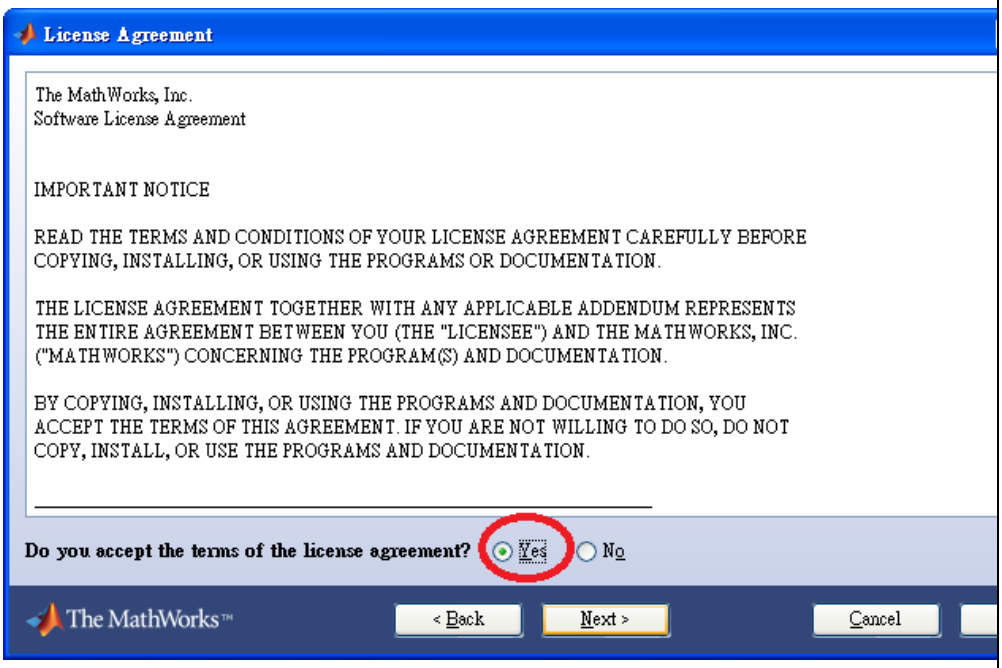
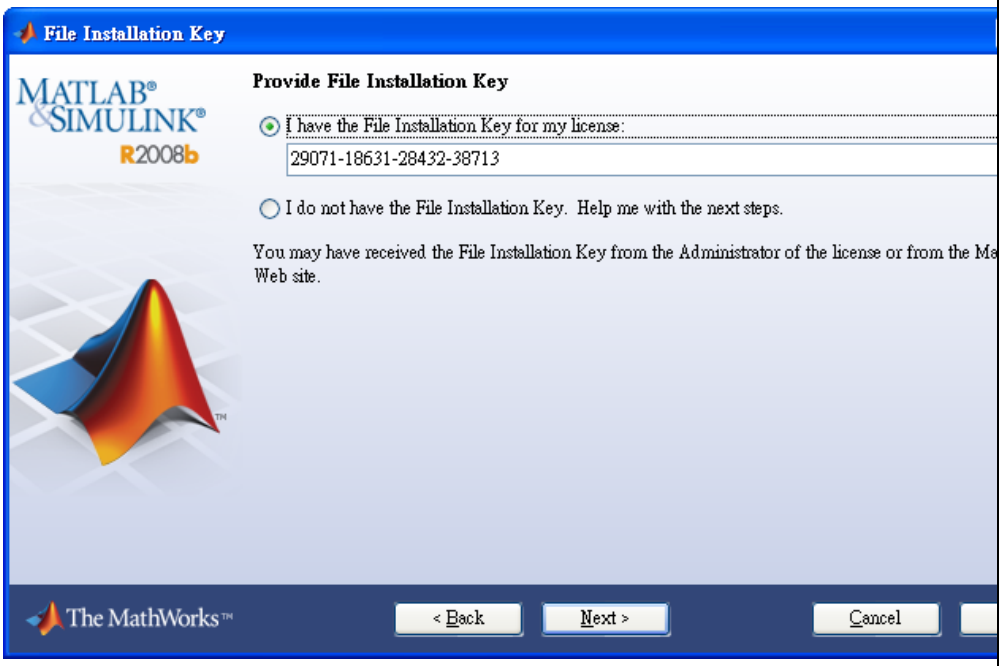
Step2	點選 下載校園授權軟體 
Step3	依照資網中心的規則去輸入帳號密碼 再點選登入 

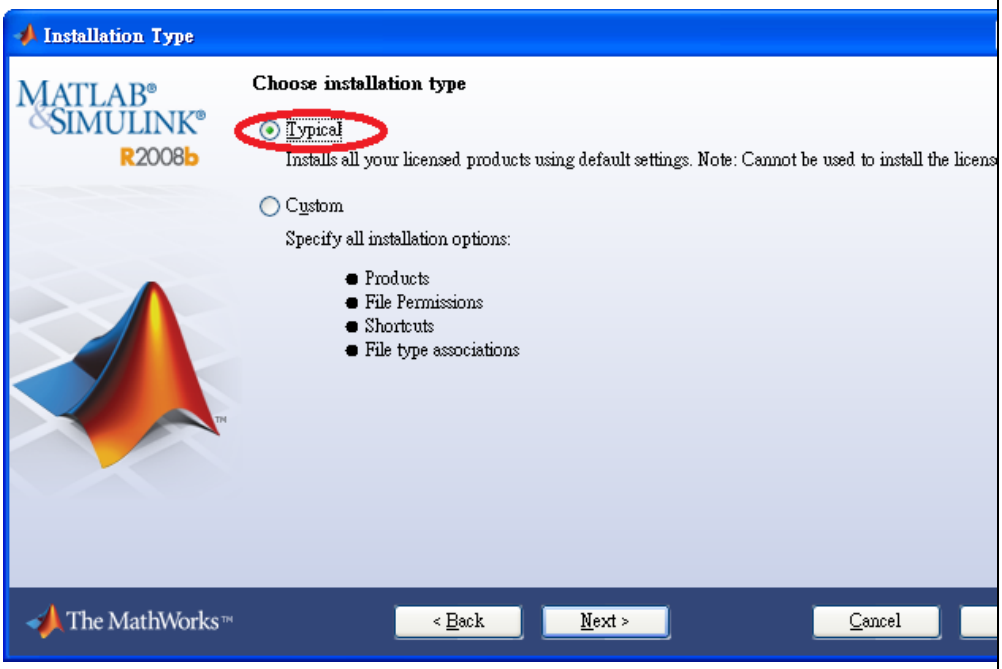
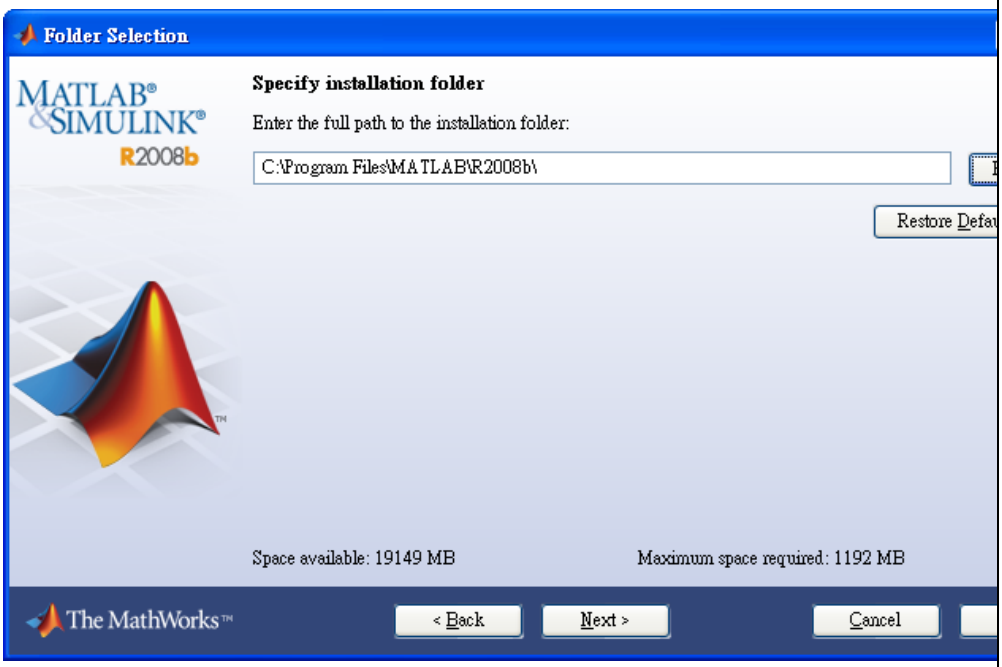
Step4	請點選學習軟體底下的MATLAB R2008b Windows 平台 (DVD) 
Step5	點選儲存 
Step6	需要一點點時間等待 先去學校信箱收認證信 

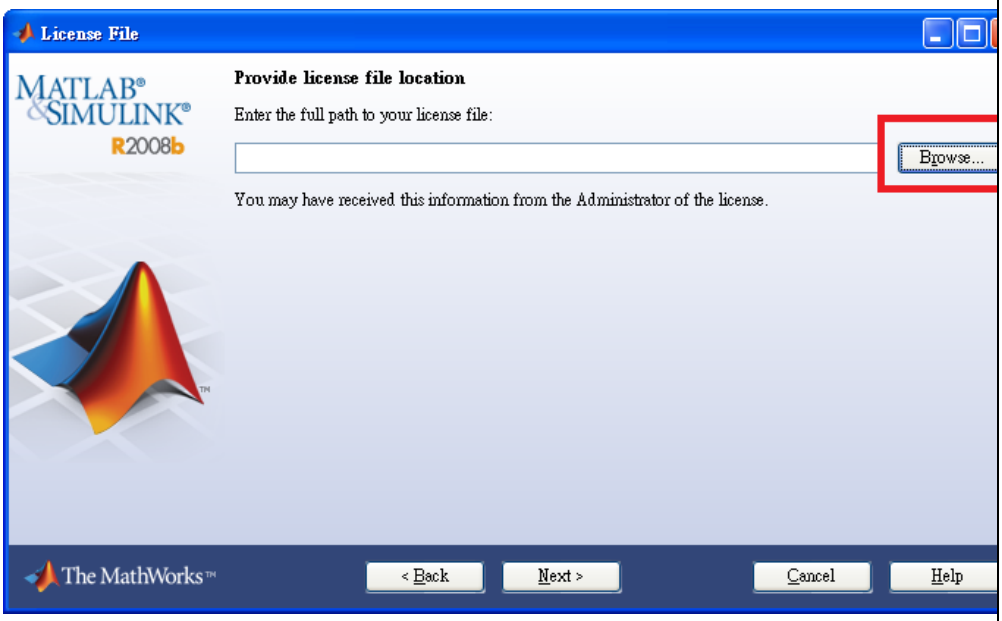
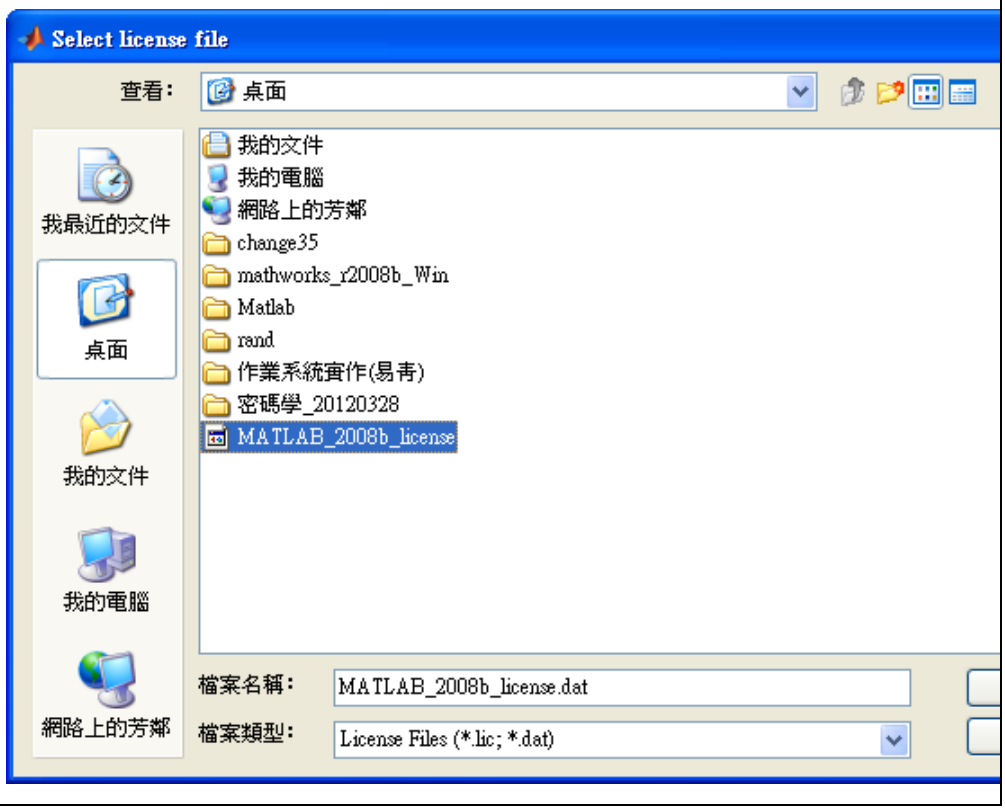
Step7	進入信箱會收到資網中心的信 
Step8	將信中第一點所需的檔案下載下來 對著網址點右鍵 -> 另存目標 放到你記得的位子即可 先暫時把此檔案擱著 最後認證才會使用到 

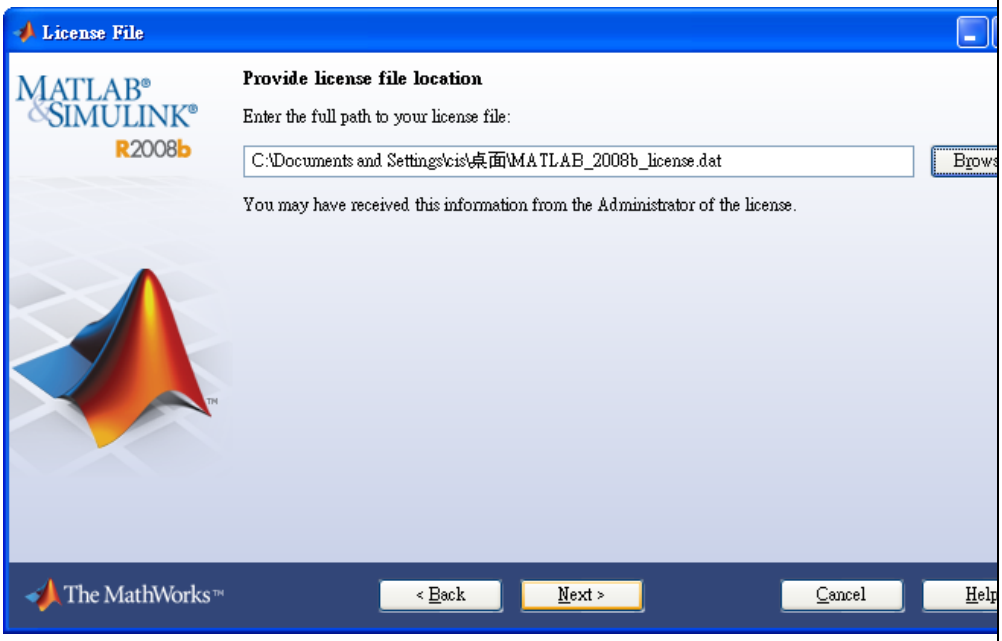
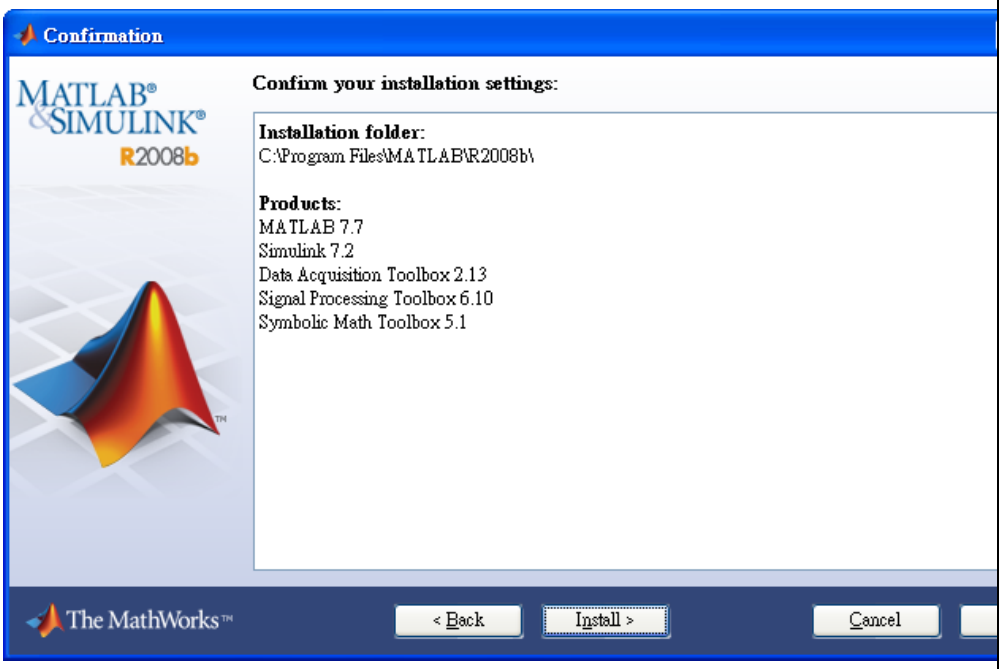
Step9	從資網中心下載完 MATLAB R2008b 的檔案後 對此檔案點右鍵 -> 將檔案解壓縮出來 
Step10	對 setup 點兩下 

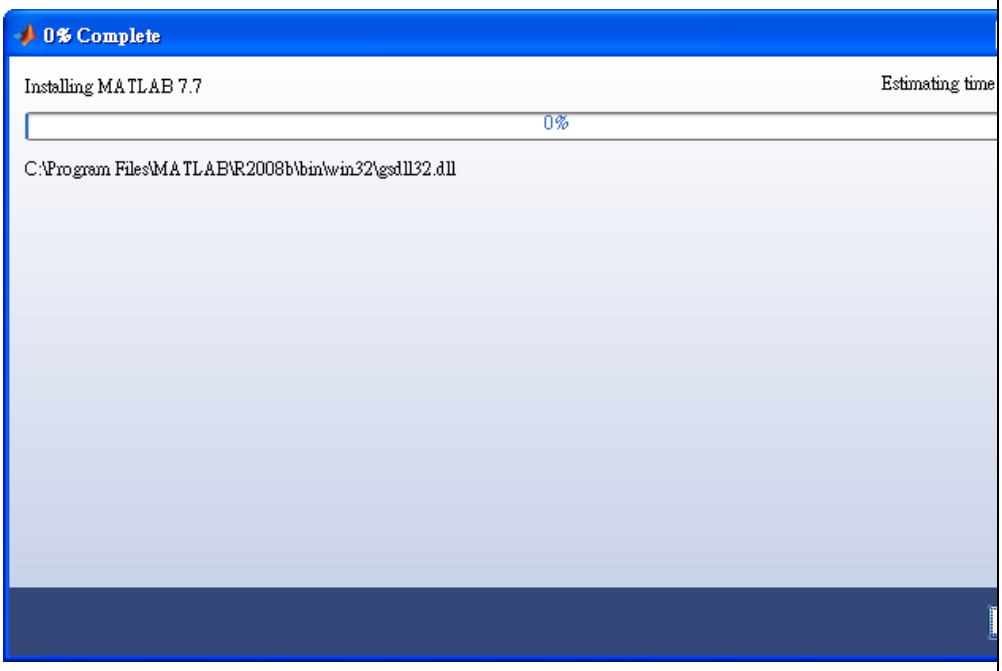
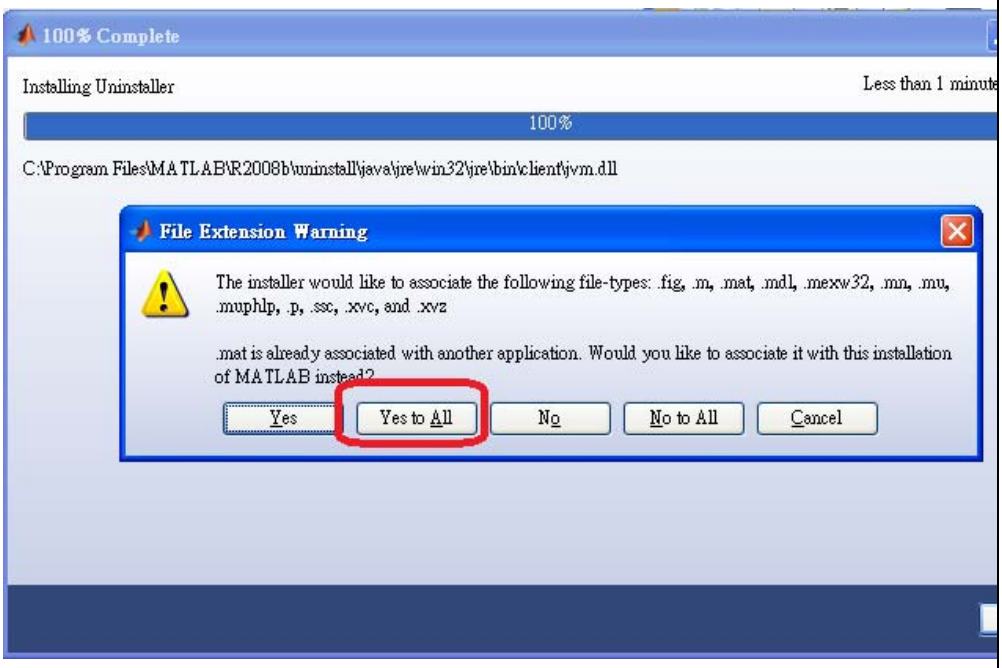
Step11	等待一會兒 
Step12	點選"Install manually without using the Internet" 即可按 next 

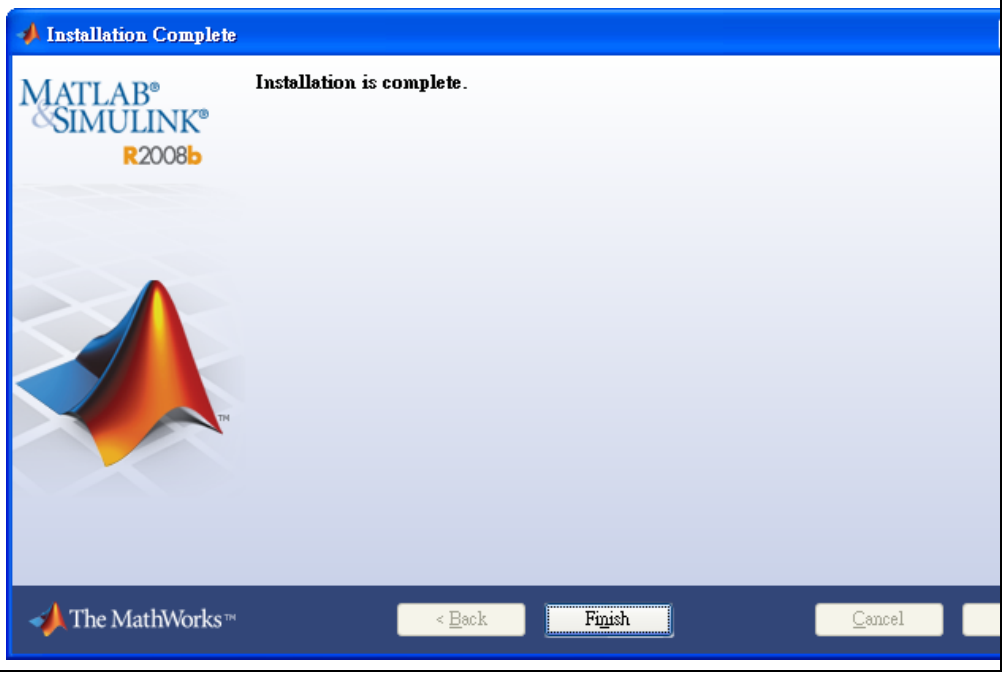
Step13	點選 yes 即可按 next 
Step14	選擇"I have the File Installation Key for my license." 並輸入序號"29071-18631-28432-38713" (學校的認證信有提供序號) 即可按 next 

Step15	選擇 Tyical 即可按 next 
Step16	選擇安裝路徑 即可按 next 

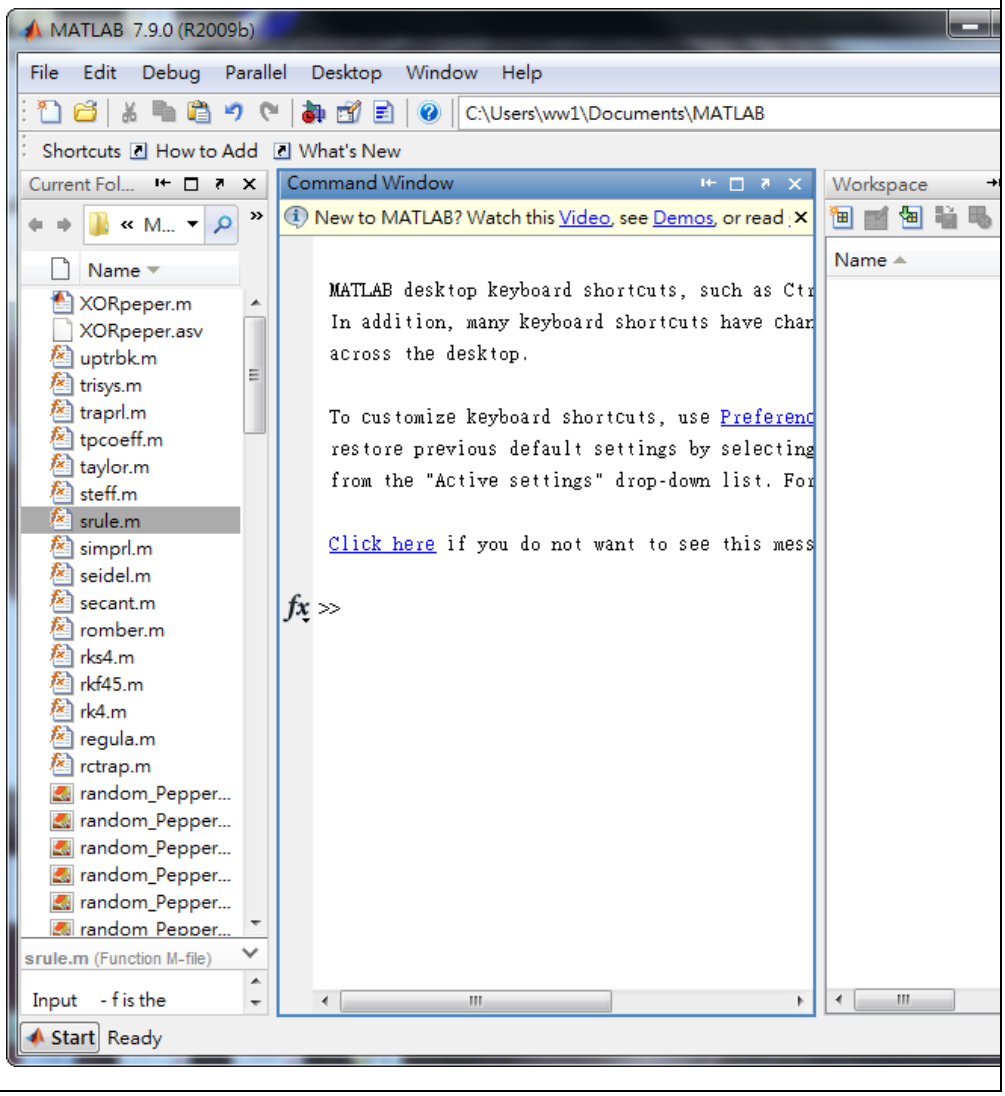
Step17	點選 Brown 
Step18	選擇在 Step8 所下載的認證的檔案 

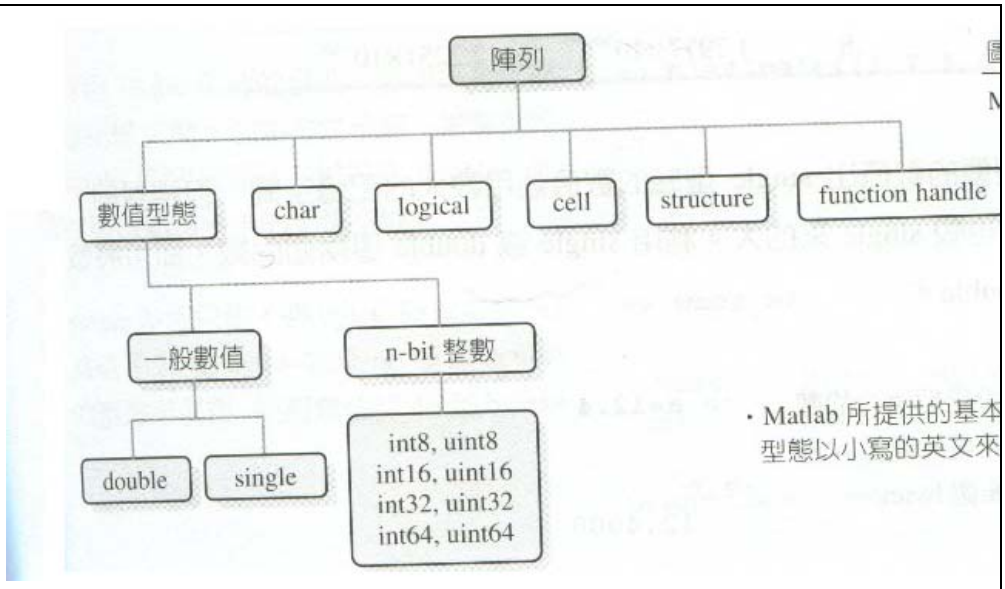
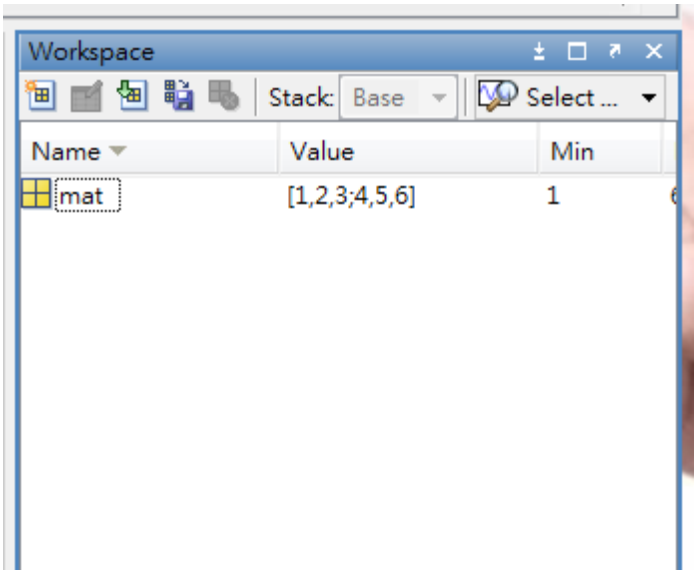
Step19	選擇成功後 即可按 next 
Step20	選擇 Install 

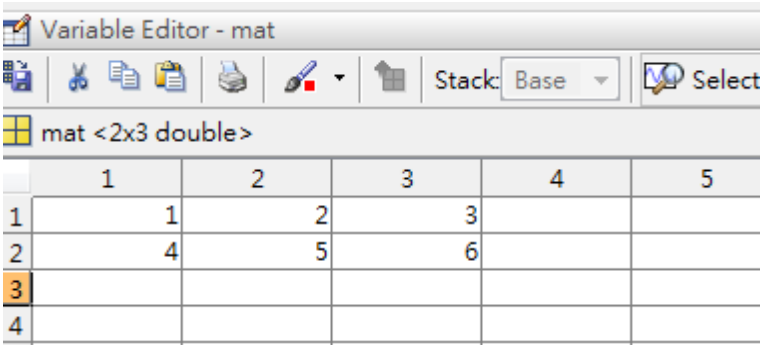
Step21	等待一些時間安裝 
Step22	選擇 Yes to All 

Step23	點選 Famish 

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 cpmmand 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	可以直觀的看到陣列的數值 
Step5	觀察數值 `>> mat(1,2)` `ans =` `2`
Step6	存入數值 `>> storge=mat(1,2)` `storge =` `2`
Step7	觀察列 or 排的數值

```
>> 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

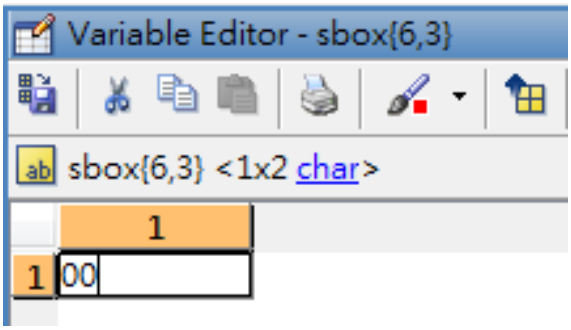
```
C{1}=(1:2);
C{2}=(1);
C{3}=(1:3);
```

Step9

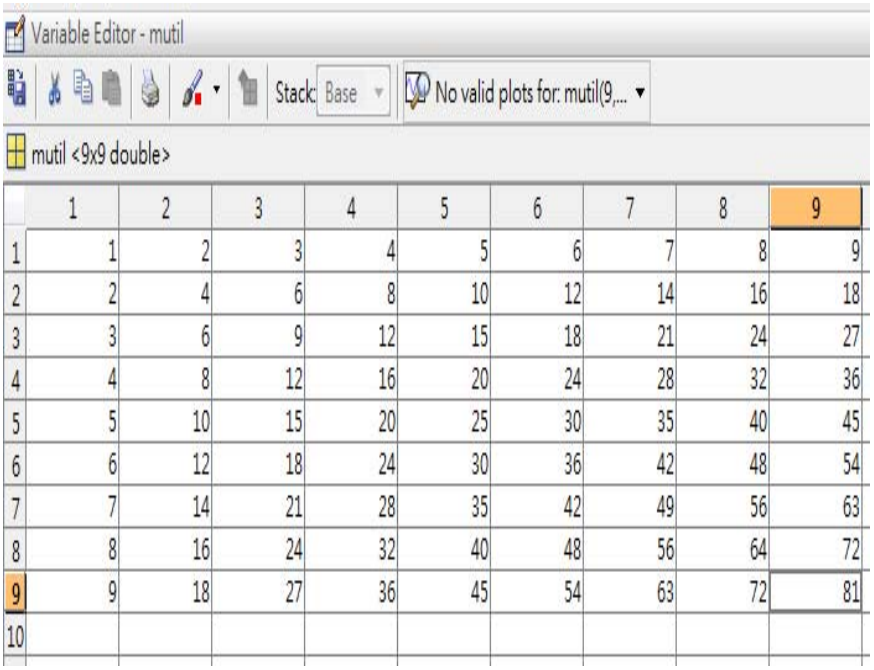
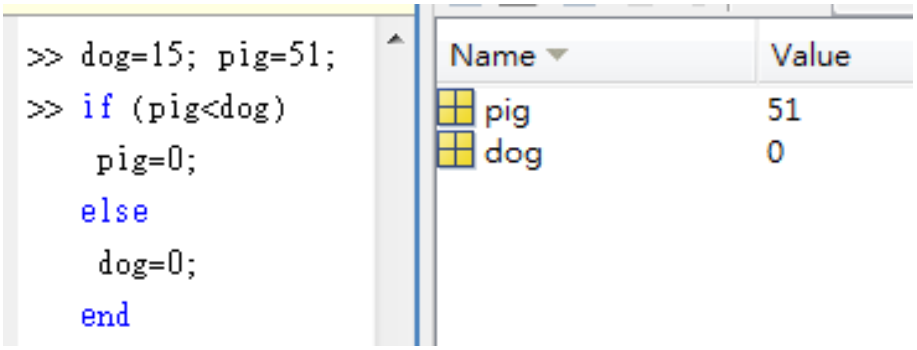
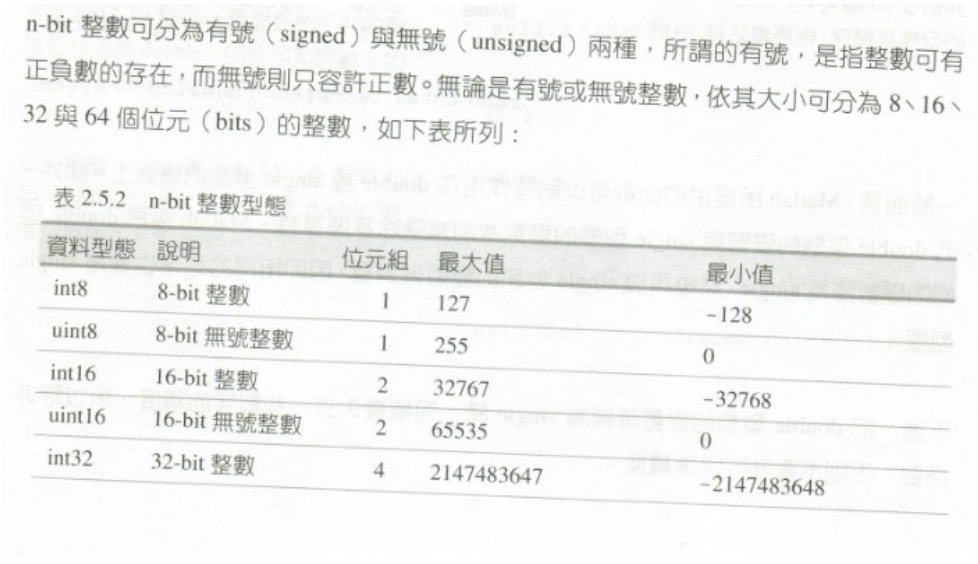
每格的裡面的 size 可以不同

C <1x3 cell>

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

Step10	可應用在 s-box 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' };
Step11	要是在一般普通的陣列只會看到 0 sbox(6,3) ans = '00'
Step12	
Step13	型態跟數值的取出 ()- 取出型態 {}-取出數值

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

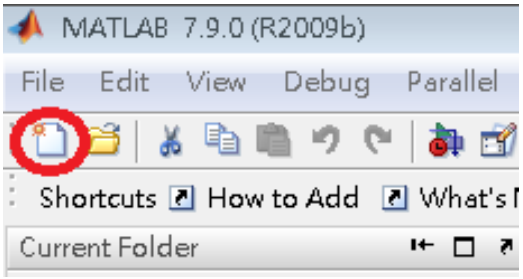
Step16	
Step17	If...else 範例 
Step18	處理各式資料型態 

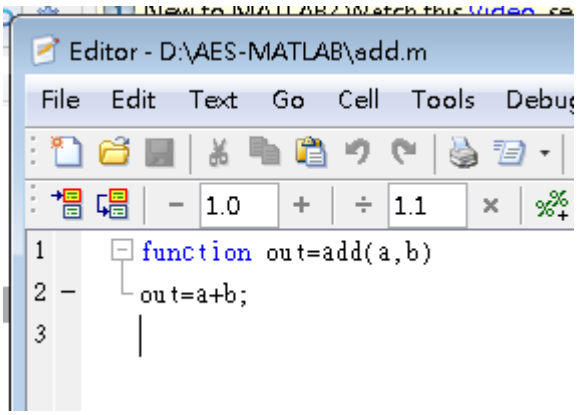
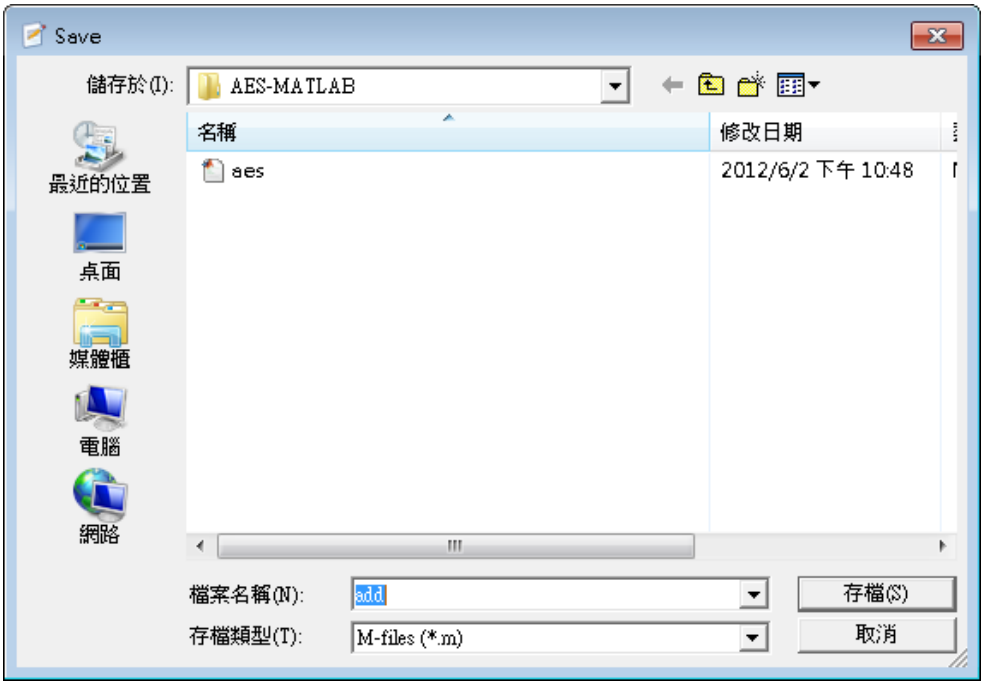
n-bit 整數可分為有號（signed）與無號（unsigned）兩種，所謂的有號，是指整數可有正負數的存在，而無號則只容許正數。無論是有號或無號整數，依其大小可分為 8、16、32 與 64 個位元（bits）的整數，如下表所列：

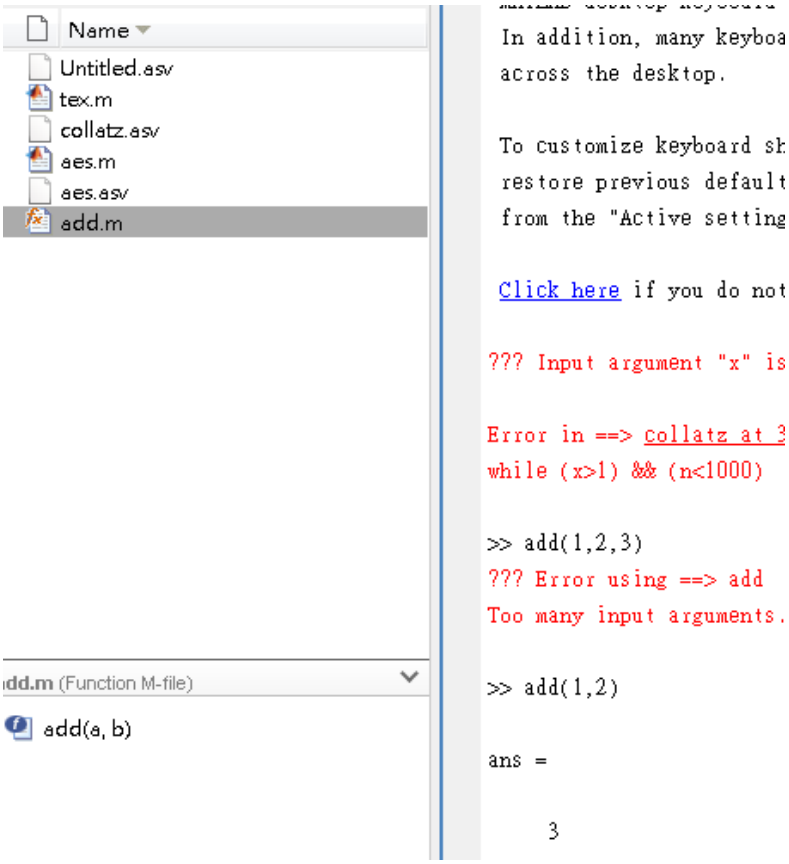
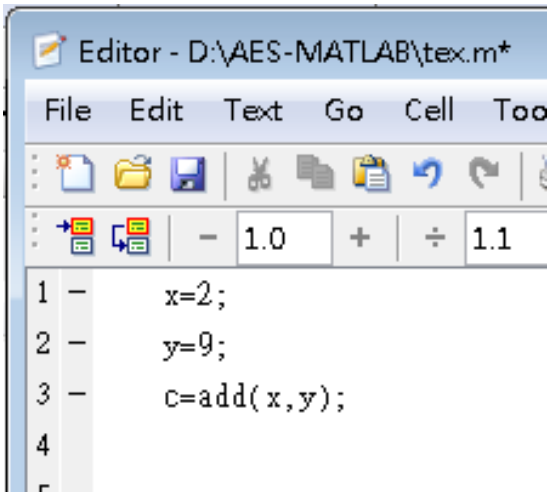
表 2.5.2 n-bit 整數型態

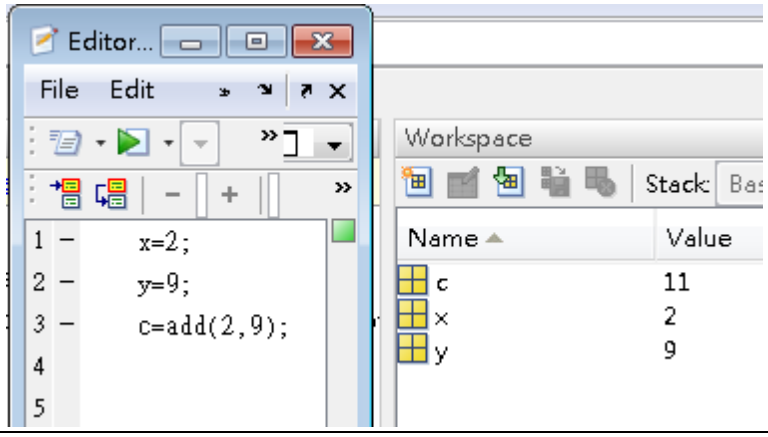
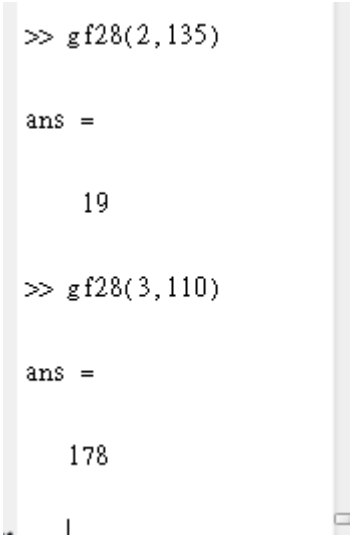
資料型態	說明	位元組	最大值	最小值
int8	8-bit 整數	1	127	-128
uint8	8-bit 無號整數	1	255	0
int16	16-bit 整數	2	32767	-32768
uint16	16-bit 無號整數	2	65535	0
int32	32-bit 整數	4	2147483647	-2147483648

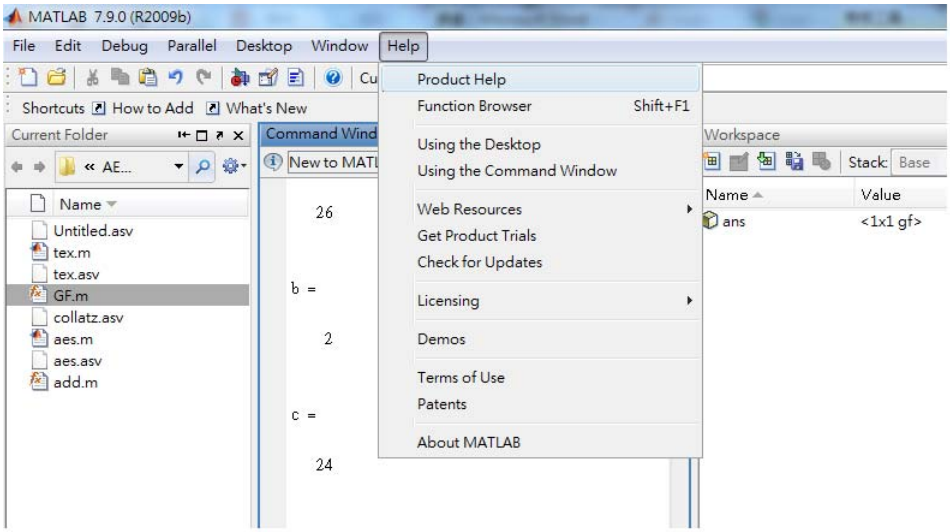
	>> 10/4 ans = 2.5000 >> a=fix(ans) %無條件捨去 a = 2 >> b=uint8(ans) %四捨五入 b = 3
Step19	16 ,10,2 進位換算 'ab' a=hex2dec(ans)%16進位轉成10進位 b=dec2bin(a)%10進位轉成2進位 c=bin2dec(b)%2進位轉成10進位 ans = ab a = 171 b = 10101011 c = 171

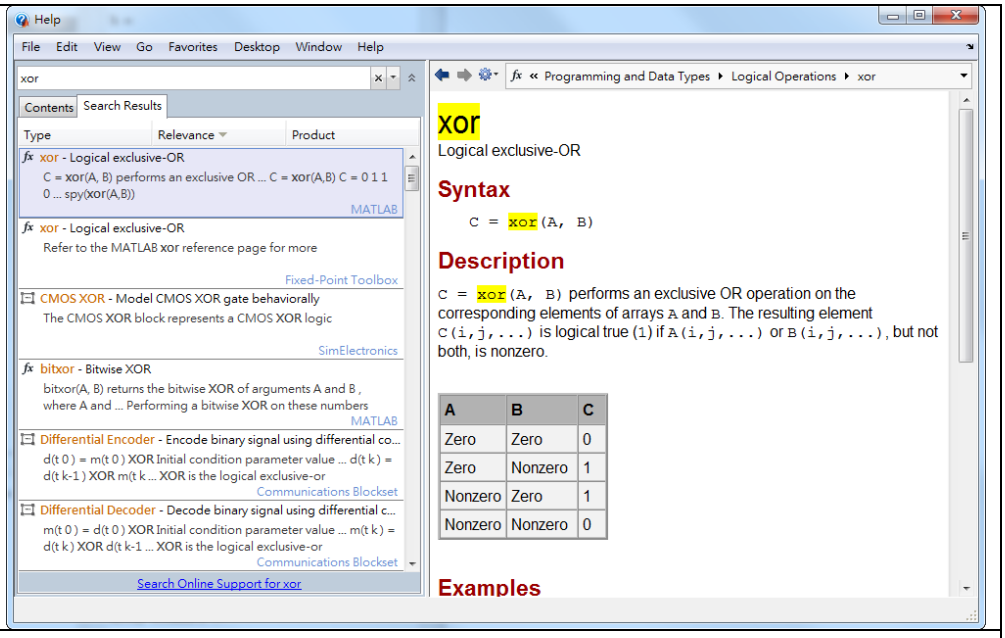
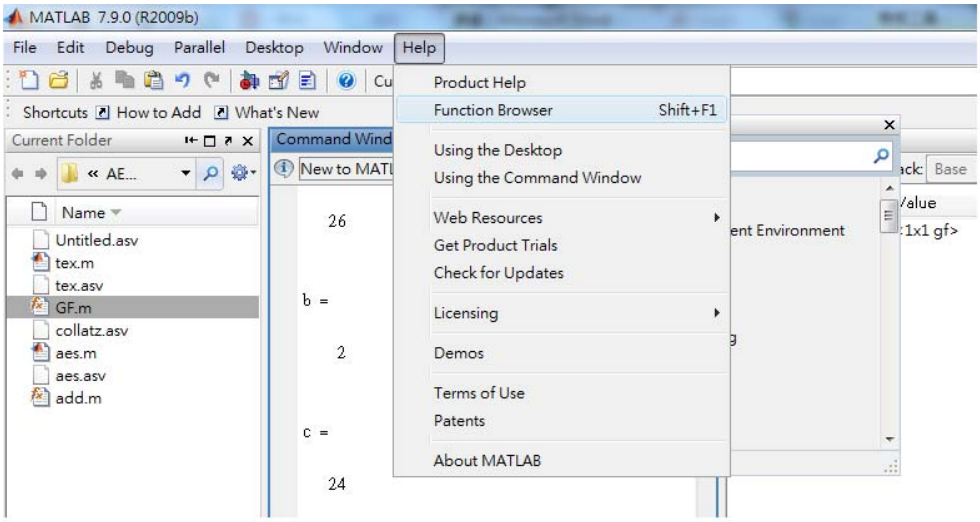
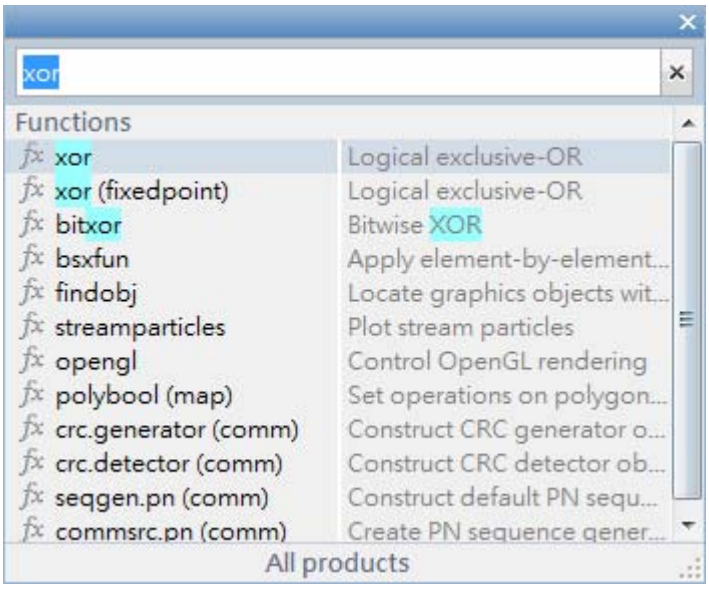
Step20	bitxor 的應用 `>> clear` `a='1a';` `b='02';` `a=uint8(hex2dec(a)) %轉成10進位 且要int型態` `b=uint8(hex2dec(b)) %轉成10進位 且要int型態` `c=bitxor(a,b) %a,b一定要10進位` `d=dec2hex(c) %最後擺放回去要記得轉回16進位` `a =` `26` `b =` `2` `c =` `24` `d =` `18`
Step21	製作 function 首先要開啟新檔 (M-file) 

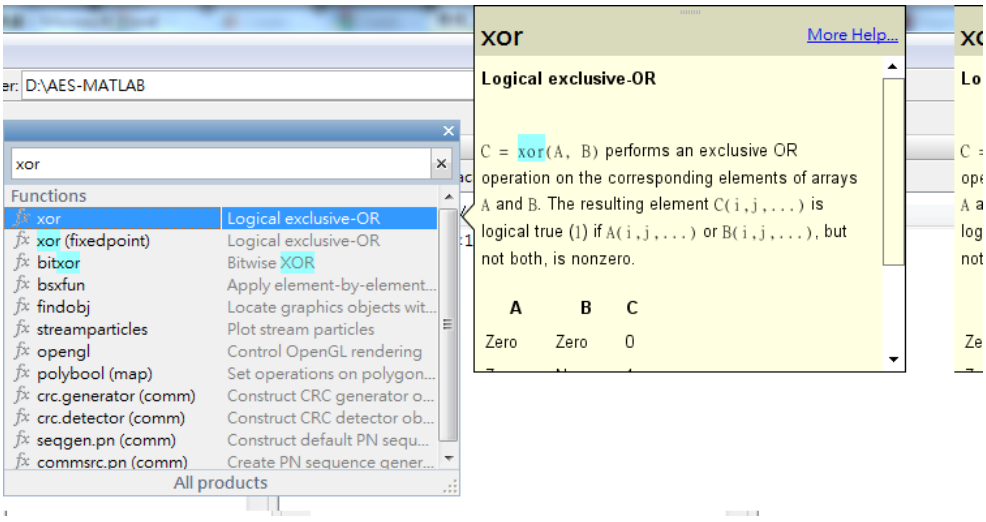
Step22	先把要打的內容先輸入完 最後在第一行加上 function 
Step23	存檔時 檔名要注意 

Step24	可看到建立的 function 
Step25	呼叫使用 

Step26	
Step27	GF(2^8) 乘法（ http://sna.csie.ndhu.edu.tw/~cnyang/Matlab/gf28.m ） 

Step1	Help -> Product Help 

Step2	
Step3	
Step4	

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)。