تعريف المتغيرات بلغة التجميع :

يتم تعريف المتغيرات في قطعة البيانات **(.data)** وبالصيغة التالية :

.data

اسم المتغير نوعه البياني القيمة الابتدائية

Example:

```
   .data
 x   byte  5
y   word  ?
```

ملاحظات:

١. يستخدم الرمز ؟ لحجز مكان في الذاكرة دون إعطاء قيمة ابتدائية للمتغير .

٢. اسم المتغير يجب إن لا يكون اسم احد المسجلات

(CS,DS,SS,ES,EAX,EBX,EDX,ECX,DT,ST)

٣. اسم المتغير يجب إن لا يكون واحدة من الكلمات المحجوزة الموجودة في اللغة .

ملاحظة :

الأنواع البيانية بلغة التجميع(**Assembly**) :

1.	**byte**	**al**	**bl**	**cl**	**dl**	**ah**	**bh**	**ch**	**dh**
2.	**word**	**ax**	**bx**	**cx**	**dx**				
3.	**dword**	**eax**	**ebx**	**ecx**	**edx**				

مثال : اكتب برنامج يقوم بنقل محتوى متغير من نوع **word** إلى المسجل **ax** علما إن قيمة المتغير تساوي **6** .

```
1  Include Irvine32.inc
2      .data
3      x word 6
4      .code
5      main proc
6      mov ax,x
7      call dumpregs
8      exit
9      main endp
10     end main
```

```
C:\Windows\system32\cmd.exe
EAX=763D0006  EBX=7FFDF000  ECX=00000000  EDX=00301005
ESI=00000000  EDI=00000000  EBP=0027FF6C  ESP=0027FF64
EIP=0030101B  EFL=00000246  CF=0  SF=0  ZF=1  OF=0  AF=0  PF=1
Press any key to continue . . .
```

واجـــــب :

س١: اكتب برنامج لتعريف متغيرين من نوع word قيمة المتغير الأول تساوي 6 وقيمة المتغير الثاني تساوي 8 ، المطلوب تبديل محتوى المتغيرين دون استخدام إيعاز xchg .

س٢: اكتب برنامج لتعريف متغيرين من نوع byte احدهما يحتوي على القيمة 6 والاخر يحتوي على القيمة 8 ، المطلوب نقل محتويات المتغير الأول مسجل dl ونقل محتويات المتغير الثاني إلى المسجل dh ثم إبدال محتويات المسجلين مع بعضهما .

مـثال : اكتب برنامج يقوم بخزن القيمة 10 في المسجل al ومن ثم نقله إلى متغير اسمه var.

```
Include irvine32.inc
.data
    Var   byte  ?
.code
   Main proc
       Mov   al , 10
        Mov   var  ,  al
     Exit
    Main endp
End main
```

في المثال أعلاه تم نقل القيمة من المسجل al إلى متغير var والذي يعتبر مكان في الذاكرة إي إننا لا نستطيع استخدام الإيعاز(call dumpregs) لطباعة محتواه لذلك نحتاج إلى استخدام إيعاز أخر يستخدم لطباعة محتوى المتغير وهذا الإيعاز هو (call dumpmem) ، ويتم ذلك بثلاث خطوات :

١- نحتاج الوصول إلى عنوان المتغير (var) نستخدم الصيغة الآتية:

```
Mov  esi,offset  var
```

ملاحظة:

المسجلات المسؤولة عن المواقع(index) هي **(ebp,esi,edi)**

٢- المتغير ممكن إن يحتوي على قيمة واحدة أو أكثر لذلك نحتاج إلى استخدام المسجل ecx لمعرفة عدد القيم التي يحتويها المتغير ، ويكتب بالصيغة الآتية :

```
Mov ecx , عدد القيم
```

أو نستخدم الدالة الجاهزة (lengthof) وتكتب بالصيغة الآتية:

```
Mov  ecx ,lengthof  var
```

٣- حجم المتغير يجب يوضع في المسجل ebxإذا كان النوع البياني byte نضع الرقم 1
وإذا كان النوع البياني word نضع الرقم 2 وإذا كان النوع البياني dword نضع الرقم 4
ويكتب بالصيغة الآتية :

```
Mov ebx,1
Mov ebx,2
Mov ebx,4
```

أو نستخدم الدالة الجاهزة (typeof) لمعرفة حجم المتغير وتكتب بالصيغة الآتية :

```
Mov ebx,typeof var
```

بعد إكمال الثلاث خطوات السابقة نستخدم الايعاز *call dumpmem*.

فيما يلي حل السؤال السابق مع التنفيذ :

```
al Scope)
 1   Include Irvine32.inc
 2         .data
 3         var byte ?
 4         .code
 5         main proc
 6         mov al,10h
 7         mov var,al
 8         mov esi,offset var
 9         mov ecx,1
10         mov ebx,1
11         call dumpmem
12         exit
13         main endp
14         end main
```

```
C:\Windows\system32\cmd.exe
Dump of offset 00B45000
-------------------------------
10
Press any key to continue . . .
```

واجـب : اكتب برنامج لنقل القيمة 7 إلى المتغير اسمه var من نوع wordوطباعة على الشاشة التنفيذ.