# Chöông 5 : Nhaäp moân Assembly

**Muïc tieâu**

- Hieåu ngoân ngöõ maùy vaø ngoân ngöõ Assembly.
- Trình hôïp dòch Assembler.
- Lyù do nghieân cöùu Assembly.
- Hieåu caùc thaønh phaàn cô baûn cuûa Assembly
- Naém ñöôïc caáu truùc cuûa 1 CT Assembly.
- Bieát vieát 1 chöông trình Assembly.
- Bieát caùch dòch, lieân keát vaø thöïc thi 1 chöông trình Assembly.

# Giôùi thieäu ngoân ngöõ Assembly

- Giuùp khaùm phaù bí maät phaàn cöùng cuõng nhö phaàn meàm maùy tính.
- Naém ñöôïc caùch phaàn cöùng MT laøm vieäc vôùi heä ñieàu haønh vaø hieåu ñöôïc baèng caùch naøo 1 trình öùng duïng giao tieáp vôùi heä ñieàu haønh.
- Moät MT hay moät hoï MT söû duïng 1 taäp leänh maõ maùy rieâng cuõng nhö 1 ngoân ngöõ Assembly rieâng.

# Assembler

- **Moät chöông trình vieát baèng ngoân ngöõ Assembly muoán MT thöïc hieän ñöôïc ta phaûi chuyeån thaønh ngoân ngöõ maùy.**

- Chöông trình duøng ñeå dòch 1 file vieát baèng Assembly ➔ ngoân ngöõ maùy , goïi laø Assembler.

**Coù 2 chöông trình dòch:**

**MASM vaø TASM**

# Lyù do nghieân cöùu Assembly

- Ñoù laø caùch toát nhaát ñeå hoïc phaàn cöùng MT vaø heä ñieàu haønh.
- Vì caùc tieän ích cuûa noù .
- Coù theå nhuùng caùc chöông trình con vieát baèng ASM vaøo trong caùcchöông trình vieát baèng ngoân ngöõ caáp cao .

# Leänh maùy

- **Laø 1 chuoåi nhò phaân coù yù nghóa ñaëc bieät – noù ra leänh cho CPU thöïc hieän taùc vuï.**
  - **Taùc vuï ñoù coù theå laø :**
    **di chuyeån 1 soá töø vò trí nhôù naøy sang vò trí nhôù khaùc.**
    **Coäng 2 soá hay so saùnh 2 soá.**

**0 0 0 0 0 1 0 0 Add a number to the AL register**

**1 0 0 0 0 1 0 1 Add a number to a variable**

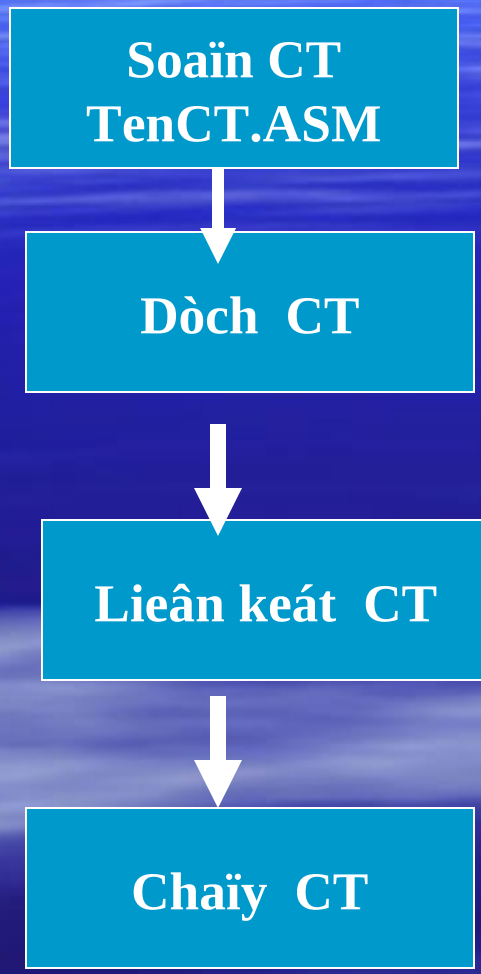
**1 0 1 0 0 0 1 1 Move the AX reg to another reg**

# Leänh maùy (cont)

- **Taäp leänh maùy ñöôïc ñònh nghóa tröôùc, khi CPU ñöôïc saûn xuaát vaø noù ñaëc tröng cho kieåu CPU .**
  - **Ex : B5 05 laø 1 leänh maùy vieát daïng soá hex, daøi 2 byte.**
  - **Byte ñaàu B5 goïi laø Opcode**
  - **Byte sau 05 goïi laø toaùn haïng Operand**

**YÙù nghóa cuûa leänh B5 05 : cheùp giaù trò 5 vaøo reg AL**

# Caùch vieát 1 chöông trình Assembly




**Duøng 1 phaàn meàm soaïn thaûo VB baát kyø ñeå soan CT Assembly nhö : NotePad, NC, maøn hình C, Pascal ...**

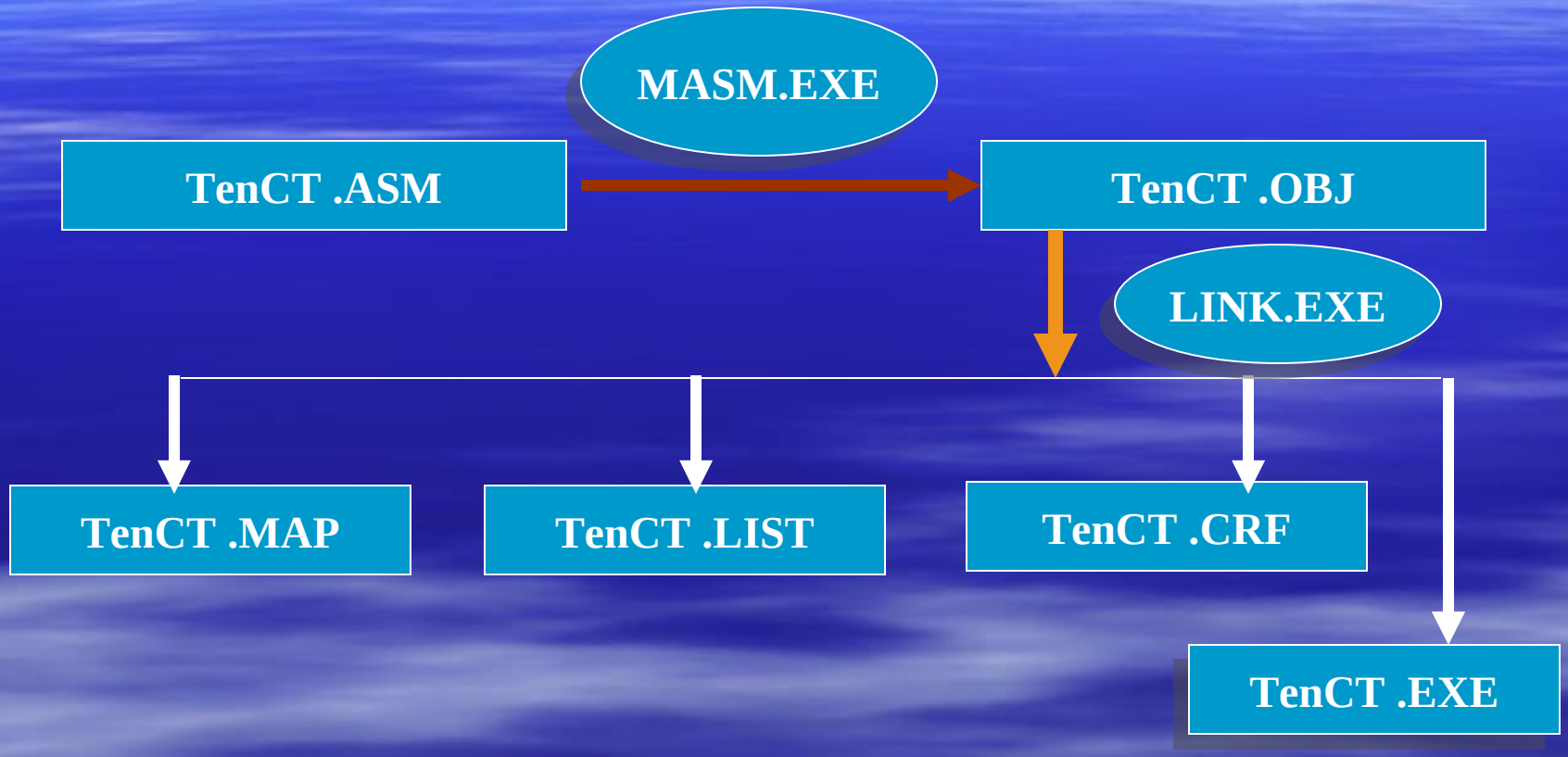
**CT coù phaàn môû roäng laø .ASM**

**duøng MASM ñeå dòch chöông trình nguoàn .ASM ➔ File Object.**

**duøng LINK ñeå lieân keát Object taïo taäp tin thöïc hieän .EXE**

**Goû teân taäp tin thöïc hieän .EXE töø daáu nhaéc DOS ñeå chaïy**

# Dòch vaø noái keát chöông trình



# Moät chöông trình minh hoaï

```
DOSSEG
.MODEL SMALL
.STACK 100h
.DATA
MES DB “HELLO WORD”,’$’
.CODE
MAIN PROC
   MOV AX, @DATA
   MOV DS, AX
   MOV DX, OFFSET MES
   MOV AH, 9
   INT 21
   MOV AH,4CH
   INT 21
   MAIN ENDP
   END MAIN
```

# Caùc file ñöôïc taïo

- Sau khi dòch thaønh coâng file nguoàn.ASM, ta coù caùc file :
- File listing : file VB , caùc doøng coù ñaùnh soá thöù töï maõ.
- File Cross reference
- File Map
- File Obj
- File EXE

# File Listing

```
Microsoft (R) Macro Assembler Version 5.10                  10/11/4
                                                            Page     1-1


                        1                       DOSSEG
                        2                       .MODEL SMALL
                        3                       .STACK 100H
                        4                       .DATA
0000  48 45 4C 4C 4F 20         5               MES DB "HELLO WORD$"
      57 4F 52 44 24            6
                        7                       .CODE
0000                    8               MAIN PROC
0000  B8 ---- R         9                       MOV AX,@DATA
0003  8E D8             10                      MOV DS, AX
0005  B4 09             11                      MOV AH,9
0007  BA 0000 R         12                      MOV DX, OFFSET MES
000A  CD 21             13                      INT 21H
000C  B4 4C             14                      MOV AH,4CH
000E  CD 21             15                      INT 21H
0010                    16              MAIN ENDP
                        17              END MAIN
♀◘Microsoft (R) Macro Assembler Version 5.10                10/11/4
```

# Map File

- Start Stop Length Name Class
- 00000H 0001FH 00020H _TEXT CODE
- 00020H 0002AH 0000BH _DATA DATA
- 00030H 0012FH 00100H STACK STACK

- Origin Group
- 0002:0 DGROUP

- Program entry point at 0000:0010

# Giaûi thích

- .model small : duøng kieåu caáu truùc <= 64 K boä nhôù cho maõ , 64K cho döõ lieäu.
- .Stack 100h : daønh 256 bytes cho stack cuûa chöông trình .
- .Data : ñaùnh daáu phaân ñoaïn döõ lieäu ôû ñoù caùc bieán ñöôïc löu tröõ.
- .Code : ñaùnh daáu phaân ñoaïn maõ chöùa caùc leänh phaûi thi haønh.
- Proc : khai baùo ñaàu 1 thuû tuïc, trong Ex naøy ta chæ coù 1 thuû tuïc Main.

# Giaûi thích (cont)

- **Cheùp ñòa chæ ñoaïn döõ lieäu vaøo thanh ghi AX.**
- **Sau ñoù cheùp vaøo thanh ghi DS**
- **Goïi haøm soá 9 cuûa Int 21h cuûa Dos ñeå xuaát chuoåi kyù töï ra maøn hình.**
- **Thoaùt khoûi CT .**
- **Main endp : ñaùnh daáu keát thuùc thuû tuïc**
- **End main : chaám döùt chöông trình**

# Caùc cheá ñoä boä nhôù

| Kieåu | Moâ taû |
|---|---|
| SMALL | Maõ leänh trong 1 ñoaïn.Döõ lieäu trong 1 ñoaïn |
| MEDIUM | Maõ leänh nhieàu hôn 1 ñoaïn.Döõ lieäu trong 1 ñoaïn |
| COMPACT | Maõ leänh trong 1 ñoaïn. Döõ lieäu nhieàu hôn 1 ñoaïn |
| LARGE | Maõ leänh nhieàu hôn 1 ñoaïn<br>Döõ lieäu nhieàu hôn 1 ñoaïn,khoâng coù maûng naøo > 64K |
| HUGE | Maõ leänh nhieàu hôn 1 ñoaïn<br>Döõ lieäu nhieàu hôn 1 ñoaïn, maûng coù theå > 64K |

# Daïng leänh


- [name] [operator] [ operand] [comment]

Nhaõn, teân bieán
Teân thuû tuïc

Maõ leänh daïng gôïi nhôù

Register, oâ nhôù
Trò, haèng

**Ex : MOV CX , 0**

**LAP : MOV CX, 4**

**LIST DB 1,2,3,4**

**Moãi doøng chæ chöùa 1 leänh vaø moãi leänh phaûi naèm treân 1 doøng**

# INT 21H

- Leänh INT soá hieäu ngaét ñöôïc duøng ñeå goïi chöông trình ngaét cuûa DOS vaø BIOS.

**Ngaét 21h**

**oán söû duïng haøm naøo cuûa INT 21h ta ñaë**
**n_number vaøo thanh ghi AH, sau ñoù goïi IN**

| Function_number | chöùc naêng |
|---|---|
| 1 | nhaäp 1 kyù töï töø baøn phím |
| 2 | Xuaát 1 kyù töï ra maø hình. |
| 9 | Xuaát 1 chuoåi kyù töï ra maøn hình |

# INT 21h (cont)

**Haøm 1 : Nhaäp 1 kyù töï**

**Input : AH =1**
**Output : AL = maõ ASCCI cuûa phím aán**
**= 0 neáu 1 phím ñieàu khieåân ñöôïc aán**

**Haøm 2 : Hieån thò 1 kyù töï ra maøn hình**

**Input : AH =2**
**DL = Maõ ASCII cuûa kyù töï hieån thò hay kyù töï ñieàu khieån**

# Thí duï minh hoïa

```
DOSSEG
.MODEL SMALL
.STACK 100H
.CODE
  MAIN PROC
    MOV AH , 2
    MOV DL , '?'
    INT 21H
    MOV AH ,1
    INT 21H
    MOV BL,AL
    MOV  AH,2
    MOV DL, 0DH
    INT 21H
    MOV DL , 0AH
    INT 21H
    MOV DL , BL
    INT 21H
    MOV AX , 4C00H
    INT 21H
    MAIN ENDP
END MAIN
```

KEÁT QUAÛ

```
? N
N
```

# Thí duï minh hoïa caùc haøm cuûa INT 21

- **In daáu ? ra maøn hình :**

  **MOV AH, 2**

  **MOV DL, ‘?’**

  **INT 21H**

- **Nhaäp 1 kyù töï töø baøn phím :**

  **MOV AH, 1**

  **INT 21H**

# Bieán

- Cuù phaùp : [teân bieán] DB | DW |.... [trò khôûi taïo]
- Laø moät teân kyù hieäu daønh rieâng cho 1 vò trí trong boä nhôù nôi löu tröõ döõ lieäu.
- Offset cuûa bieán laø khoaûng caùch töø ñaàu phaân ñoaïn ñeán bieán ñoù.
- Ex : khai baùo 1 danh saùch aList ôû ñòa chæ 100 vôùi noäi dung sau :

```
.data
    aList  db “ABCD”
```

# Bieán (cont)

**Luùc ñoù :**

| Offset | Bieán |
|---|---|
| 0000 | A |
| 0001 | B |
| 0002 | C |
| 0003 | D |

# Khai baùo bieán

| Töø gôïi nhôù | Moâ taû | Soá byte | Thuoäc tính |
|---|---|---|---|
| DB | Ñònh nghóa byte | 1 | Byte |
| DW | Töø | 2 | Word |
| DD | Töø keùp | 4 | Doubleword |
| DQ | Töø töù | 8 | Quardword |
| DT | 10 bytes | 10 | tenbyte |

# Minh hoïa khai baùo bieán

KIEÅU BYTE

- Char db ‘A’
- Num db 41h
- Mes db “Hello Word”,’$’
- Array_1 db 10, 32, 41h, 00100101b
- Array_2 db 2,3,4,6,9
- Myvar db ? ; bieán khoâng khôûi taïo
- Btable db 1,2,3,4,5
  db 6,7,8,9,10

# Minh hoïa khai baùo bieán

**KIEÅU WORD**

DW 3 DUP (?)

DW 1000h, ‘AB’, 1024

DW ?

DW 5 DUP (1000h)

DW 256*2

**DAÏNG LÖU TRÖÕ DÖÕ LIEÄU KIEÅU WORD :**

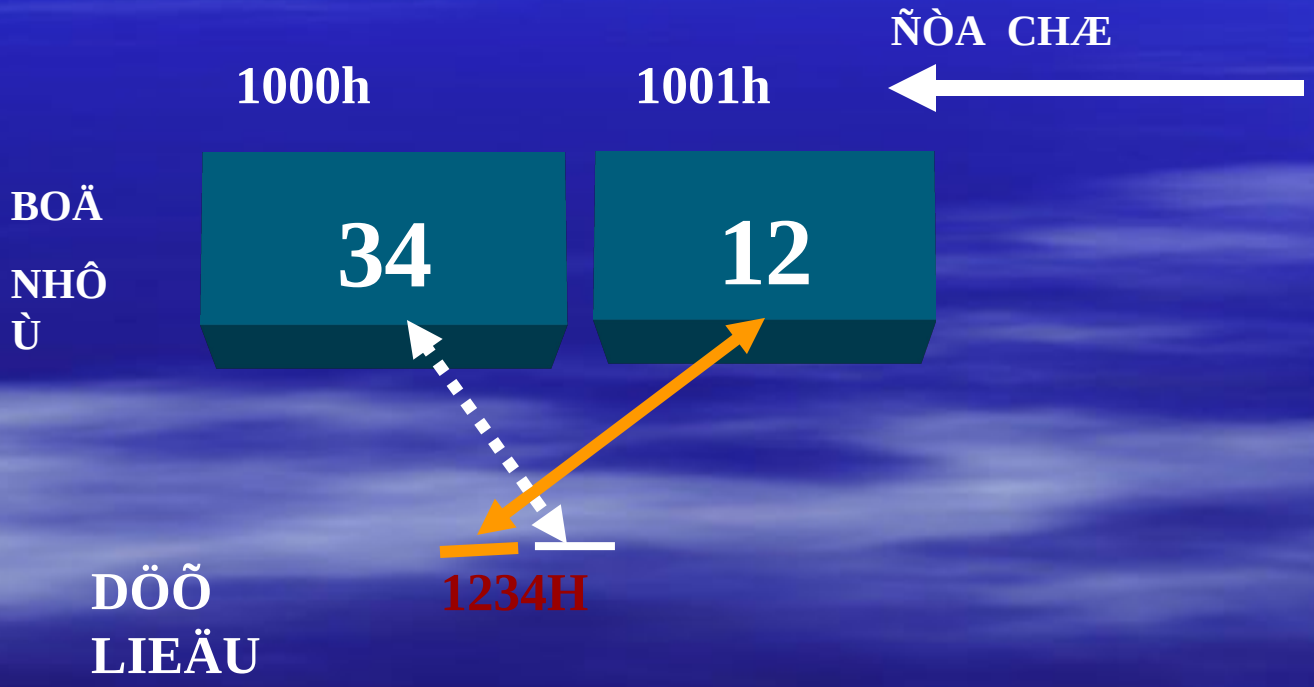
**Trình hôïp dòch ñaûo ngöôïc caùc byte trong 1 giaù trò kieåu WORD khi löu tröõ trong boä nhôù :**

**Byte thaáp löu ôû ñòa chæ thaáp  Byte cao löu ôû ñòa chæ cao**

# Minh hoïa khai baùo bieán

KIEÅU WORD

**Ex : 1234h ñöôïc löu tröõ trong boä nhôù nhö sau :**



# Toaùn töû DUP

- Laëp laïi 1 hay nhieàu giaù trò khôûi taïo.
- Ex :

```
Bmem   DB  50 Dup(?)
; khai baùo vuøng nhôù goàm 50 bytes.
  db  4 dup (“ABC”)
;12 bytes “ABCABCABCABC”
  db 4096 dup (0)
; Vuøng ñeäm 4096 bytes taát caû baèng 0
```

# Khôûi taïo bieán

- Löu yù :

Khi khôûi taïo trò laø 1 soá hex thì giaù trò soá luoân luoân baét ñaàu baèng 1 kyù soá töø 0 ñeán 9. Neáu kyù soá baét ñaàu laø A.. F thì phaûi theâm soá 0 ôû ñaàu.

- Ex :

```
 Db  A6H   ; sai
Db  0A6h   ; ñuùng
```

# Toaùn töû DUP (cont)

Amtrix dw 3 dup (4 dup (0) )

**Taïo 1 ma traän 3x4**

**Atable db 4 dup (3 dup (0), 2 dup ('X'))**

**Taïo 1 vuøng nhôù chöùa 000XX 000XX 000XX 000XX**

# Toaùn töû DUP

- **Chæ xuaát hieän sau 1 chæ thò DB hay DW**
- **Vôùi DUP ta coù theå laëp laïi 1 hay nhieàu trò cho vuøng nhôù.**
- **Raát coù ích khi laøm vieäc vôùi maûng hay chuoåi.**

# Toaùn töû ?

- Muoán khai baùo 1 bieán hay 1 maûng maø khoâng caàn khôûi taïo trò ta duøng toaùn töû ?

**Ex : MEM8 DB ? ; khai baùo 1 byte troáng trong boä nhôù**

**MEM16 DW ? ; khai baùo 2 byte troáng trong boä nhôù**

**BMEM DB 50 DUP(?)**

**; khai baùo 50 byte troáng trong boä nhôù**

# Chöông trình daïng .COM

```
CODE SEGMENT
  ASSUME  CS:CODE , DS:CODE, SS:CODE
; toaøn boä chöông trình chæ naèm trong 1 segment
Org  100h ;; chæ thò naïp thanh ghi leänh IP=100h khi
    CT ñöôïc naïp
Main proc
   mov ax,bx
 ..............
Main endp
Count db  10
.............................
Code ends
End main
```

# SUMMARY

- chöông trình Assembly goàm nhieàu doøng leänh.
- Moãi leänh phaûi vieát treân 1 doøng
- Leänh coù theå goàm [teân] [toaùn töû] [toaùn haïng]
- Caùc kyù töï phaûi ñaët trong daáu ‘ ‘ hay “ “
- DB duøng ñeå ñònh nghóa bieán kieåu BYTE
- DW duøng ñeå ñònh nghóa bieán kieåu WORD.
- Coù 2 caùch xuaát nhaäp döõ lieäu : lieân

# Caâu hoûi oân taäp

- Trong maõ maùy döôùi ñaây ñöôïc laáy töø taäp tin lieät keâ, haõy neâu yù nghóa cuûa R

5B 0021 R ADD BX, VAL1

- Neâu yù nghóa cuûa kyù hieäu hoa chæ cuûa bieán döôùi ñaây trong 1 taäp tin lieät keâ.

5B 0021 R ADD BX, VAL1

# Caâu hoûi oân taäp

- Chöông trình sau coù loãi. Haõy tìm caâu leänh naøo gaây ra loãi, giaûi thích vaø söûa laïi cho ñuùng.

```
.MODEL SMALL
.STACK 100H
.DATA
  MOV AX, VALUE1
  MOV BX, VALUE2
  INC BX, 1
  INT 21H
  MOV 4C00H, AX
  MAIN ENDP
  VALUE1    0AH
  VALUE2    1000H
  END MAIN
```

# Caâu hoûi oân taäp

- Chöông trình sau coù loãi. Haõy tìm caâu leänh naøo gaây ra loãi, giaûi thích vaø söûa laïi cho ñuùng.

```
.MODEL SMALL
.STACK 100H
.CODE
MAIN PROC
  MOV AX, @DATA
  MOV DS , AX
  MOV AX, VALUE1
   MOV AX, VALUE2
  MOV AX, 4C00H
INT 21H
MAIN ENDP
VALUE1 DB  0AH
VALUE2 DB 1000H
END MAIN
```

# Baøi taäp laäp trình

Baøi 1 : Vieát chöông trình nhaäp 1 kyù töï thöôøng , in ra kyù töï hoa töông öùng.

Baøi 2 : Vieát chöông trình hoaùn vò 2 bieán kieåu byte ñöôïc gaùn saün trò.

Baøi 3 : Vieát chöông trình taïo 1 array coù caùc phaàn töû 31h,32h,33h,34h.

Naïp töøng phaàn töû vaøo thanh ghi DL vaø xuaát noù ra maøn hình. Giaûi thích taïi sao keát xuaát treân maøn hình laø 1234.