

BÁO CÁO BÀI TẬP

Môn học: Cơ chế hoạt động của mã độc

Kỳ báo cáo: Buổi 01 (Session 01)

Tên chủ đề: Ôn tập ngôn ngữ Assembly & Chèn mã vào tập tin PE

GV: Nguyễn Hữu Quyền

Ngày báo cáo: 19/03/2023

Nhóm: 1

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.N21.ATCL

STT	Họ và tên	MSSV	Email
1	Lê Viết Tài Mẫn	20521593	20521593@gm.uit.edu.vn
2	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn
3	Nguyễn Hùng Thịnh	20521963	20521963@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Câu hỏi 01	100%	Thịnh
2	Câu hỏi 02	100%	Thiết
3	Câu hỏi 03	100%	Thịnh
4	Câu hỏi 04	100%	Mẫn, Thiết
5	Câu hỏi 05	100%	Mẫn, Thiết

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Viết một đoạn chương trình tìm số nhỏ nhất trong 3 số (1 chữ số) a,b,c cho trước.

- Ý tưởng: Đối với bài này sẽ có 3 section: section .data để khai báo chuỗi thông báo và các chữ số a, b, c cho trước, section .bss để khai báo biến smallest vì biến này có thể thay đổi giá trị trong quá trình thực thi, section .text là phần chính chạy chương trình, bao gồm thuật toán tìm số nhỏ nhất trong 3 số cho trước.

+ section .text

```

1 section .text
2     global _start                ;must be declared for using gcc
3
4 _start:                          ; the label for the program entry point
5     mov ecx, [a]
6     cmp ecx, [b]
7     jl check_c                  ; Nếu a < b, chuyển sang so sánh a vs c
8     mov ecx, [b]                ; Nếu b < a, đưa b vào ecx
9
10    ; So sánh a vs c nếu a < b
11    ; Hoặc so sánh b vs c nếu b < a
12 check_c:
13     cmp ecx, [c]                ; Nếu giá trị trong %ecx < c, smallest = giá trị trong %ecx
14     jl _exit
15     mov ecx, [c]                ; Nếu giá trị trong c < %ecx, smallest = c
16
17 _exit:
18     mov [smallest], ecx
19
20     ;print message
21     mov eax, 4
22     mov ebx, 1
23     mov ecx, msg
24     mov edx, len
25     int 0x80                    ; interrupt
26
27     ;print the smallest number
28     mov eax, 4                  ; sys_write system call
29     mov ebx, 1                  ; stdout file descriptor
30     mov ecx, smallest           ; Đưa giá trị của smallest vào %ecx
31     mov edx, 8                  ; Hiển thị kết quả với độ dài 8 bits
32     int 0x80                    ; interrupt
33
34     ;exit program
35     mov eax, 1                  ; sys_exit system call
36     mov ebx, 0                  ; no error
37     int 0x80                    ; interrupt

```

+ section .data

```

38
39 ~ section .data                ; section .data khai báo các biến tĩnh
40     msg db "The smallest number is " ; Khai báo chuỗi msg
41     len equ $ - msg            ; Tính độ dài chuỗi msg
42     a db '5'                  ; Khai báo a = 5
43     b db '4'                  ; Khai báo b = 4
44     c db '2'                  ; Khai báo c = 2

```

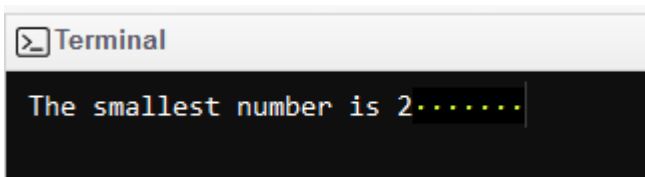
+ section .bss

```

45
46 ~ section .bss                ; section .bss khai báo các biến có thể thay đổi giá trị
47     smallest resb 2           ; Khai báo biến smallest để chứa min

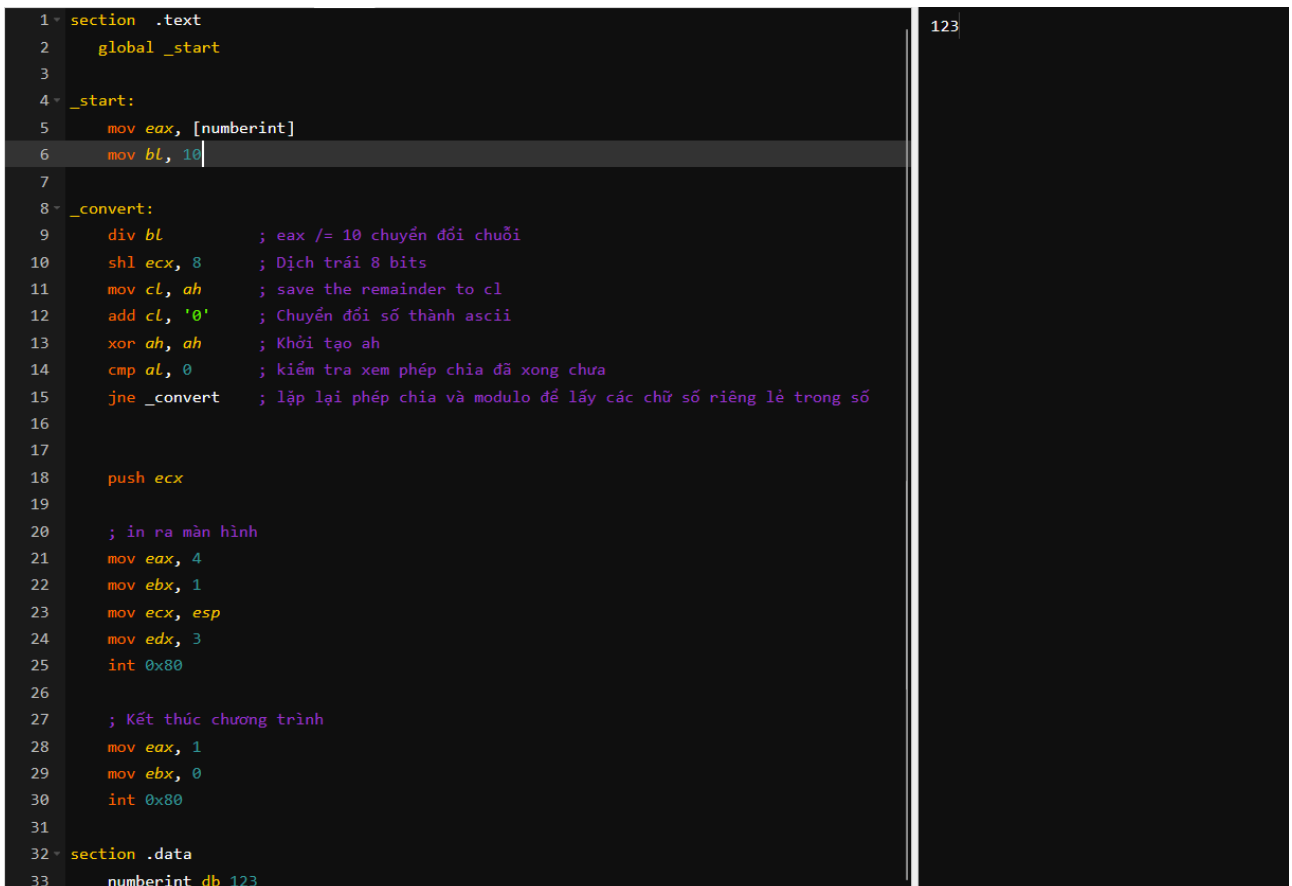
```

- Kết quả khi chạy chương trình:



2. Viết chương trình chuyển đổi một số (number) 123 thành chuỗi '123'. Sau đó thực hiện in ra màn hình số 123.

- Ý tưởng: Dùng vòng lặp để chuyển số sang chuỗi.



3. Cải tiến chương trình yêu cầu 1 sao cho tìm số nhỏ nhất trong 3 số bất kỳ (nhiều hơn 1 chữ số)

- Ý tưởng: tương tự bài 1, tuy nhiên, số a, b, c là 3 số bất kỳ cho phép nhập từ bàn phím, ngoài ra thay đổi resb thành 10 để có nhiều byte biểu diễn số nhiều hơn 1 chữ số.

+ section .text

```
1 section .text
2     global _start                ;must be declared for using gcc
3
4 _start:                          ; the label for the program entry point
5     ; Nhập số a
6     mov eax, 4
7     mov ebx, 1
8     mov ecx, msgInput
9     mov edx, lenInput
10    int 0x80
11
12    mov eax, 3
13    mov ebx, 2
14    mov ecx, a
15    mov edx, 5
16    int 0x80
17
18    ; Nhập số b
19    mov eax, 4
20    mov ebx, 1
21    mov ecx, msgInput
22    mov edx, lenInput
23    int 0x80
24
25    mov eax, 3
26    mov ebx, 2
27    mov ecx, b
28    mov edx, 5
29    int 0x80
30
```

```
31 ; Nhập số c
32 mov eax, 4
33 mov ebx, 1
34 mov ecx, msgInput
35 mov edx, lenInput
36 int 0x80
37
38
39 mov eax, 3
40 mov ebx, 2
41 mov ecx, c
42 mov edx, 5
43 int 0x80
44
45 ;;;;;;;;;;;;;;
46
47 mov ecx, [a]
48 cmp ecx, [b]
49 jl check_c ; Nếu a < b, chuyển sang so sánh a vs c
50 mov ecx, [b] ; Nếu b < a, đưa b vào ecx
51
52 ; So sánh a vs c nếu a < b
53 ; Hoặc so sánh b vs c nếu b < a
54 check_c:
55 cmp ecx, [c] ; Nếu giá trị trong %ecx < c, smallest = giá trị trong
    %ecx
56 jl _exit
57 mov ecx, [c] ; Nếu giá trị trong c < %ecx, smallest = c
58
59 _exit:
60 mov [smallest], ecx
```

```

61
62     ;print message
63     mov eax, 4
64     mov ebx, 1
65     mov ecx, msg
66     mov edx, len
67     int 0x80                ; interrupt
68
69     ;print the smallest number
70     mov eax, 4                ; sys_write system call
71     mov ebx, 1                ; stdout file descriptor
72     mov ecx, smallest        ; Đưa giá trị của smallest vào %ecx
73     mov edx, 8                ; Hiển thị kết quả với độ dài 8 bits
74     int 0x80                ; interrupt
75
76     ;exit program
77     mov eax, 1                ; sys_exit system call
78     mov ebx, 0                ; no error
79     int 0x80                ; interrupt
80

```

+ section .data

```

81 ▾ section .data                ; section .data khai báo các biến tĩnh
82     msg db "The smallest number is " ; Khai báo chuỗi msg
83     len equ $ - msg            ; Tính độ dài chuỗi msg
84
85     ; Khai báo chuỗi yêu cầu người dùng nhập 3 số a, b ,c
86     msgInput db "Enter a number: "
87     lenInput equ $ - msgInput
88
89

```

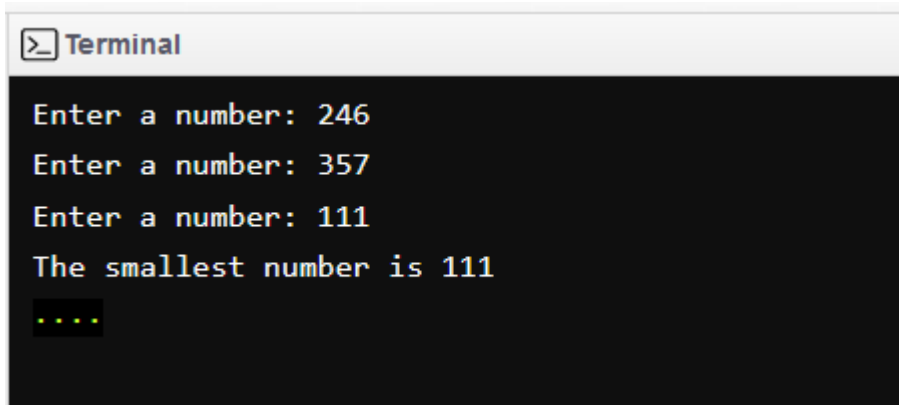
+ section .bss

```

90 ▾ section .bss                ; section .bss khai báo các biến có thể thay đổi giá trị
91
92     a resb 10
93     b resb 10
94     c resb 10
95     smallest resb 10           ; Khai báo biến smallest để chứa min

```

- Kết quả:



```
Terminal
Enter a number: 246
Enter a number: 357
Enter a number: 111
The smallest number is 111
...
```

4. (Chèn file PE) Thực hiện lại các bước trên thay đổi phần Text là MSSV
5. (Chèn file PE) Bằng cách không tạo thêm vùng nhớ mở rộng vào tập tin PE, tận dụng vùng nhớ trống để chèn chương trình cần chèn trên tập tin Notepad và calc.

Xem video demo Câu 4, Câu 5 tại đây:

<https://drive.google.com/drive/folders/1spApjiiLdtuOjkYqvW3qGKpRo4IeU15e?usp=sharing>

Em cảm ơn thầy vì đã xem

HẾT!

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).
Ví dụ: [NT101.K11.ANTT]-Session1_Group3.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT