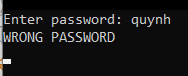
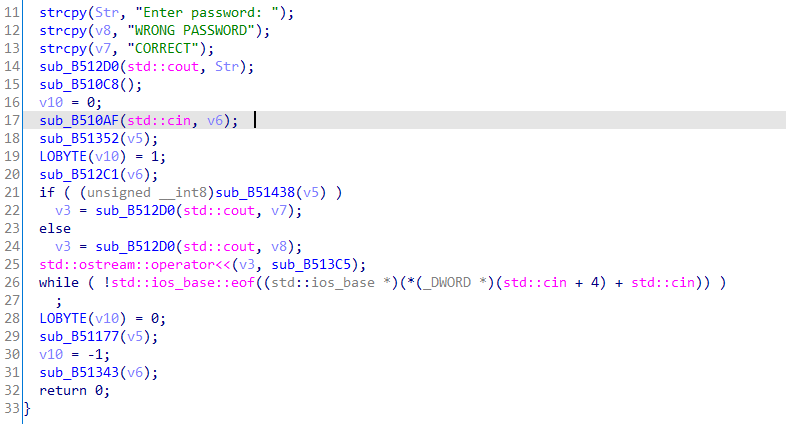
*Nguyễn Mỹ Quỳnh 19520241*

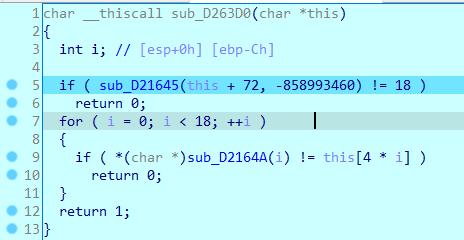
**no strings attached**

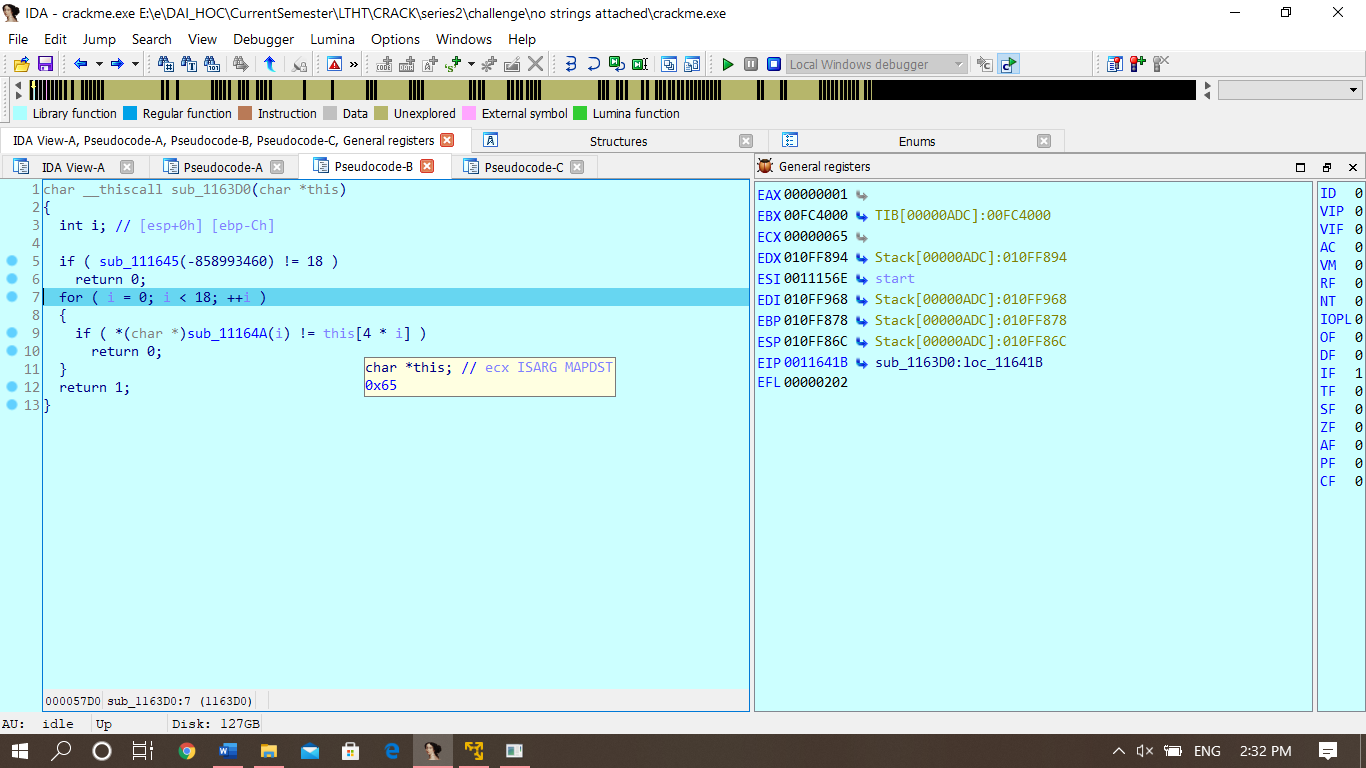
Chạy thử chương trình

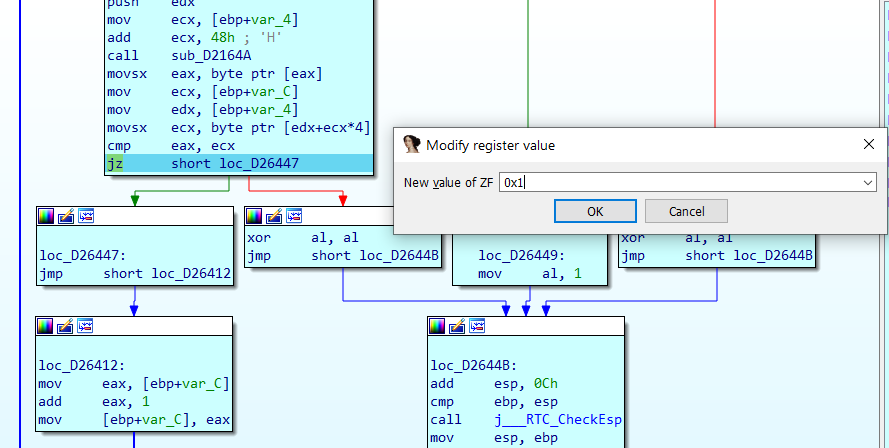


Xem mã giả của hàm main, ta thấy dòng 22 in ra chuỗi v7 “CORRECT”, vì vậy cần vào được if ở dòng 21, tức là (unsigned \_\_int8)sub\_B51438(v5) **phải =1**. Nếu nhấp vào sub\_B51438 xem code thì hơi rối ta tiến hành đặt breakpoint ở dòng 21 debug để xem kết quả cụ thể.



Thực hiện debug với input ta nhập là 12345, dòng 5 so sánh nếu kết quả trả về hàm sub\_D21645 khác 18 thì return 0 (không đúng với mong muốn như ta đã phân tích ở trên), nếu = 18 thì duyệt lần lượt 18 lần ở dòng 7. Vậy ta có thể suy đoán hàm sub\_D21645 trả về độ dài chuỗi, thật vậy sau dòng 5 quan sát kết quả hàm sub\_D21645 trả về trong thanh ghi eax, ta thấy eax=5. Vậy chuỗi input cần 18 kí tự.

Tiếp đến câu lệnh for ở dòng 7, với mỗi i ta thấy \*(char \*)sub\_11164A(i) trả về kí tự thứ i trong chuỗi input ta nhập (quan sát eax), còn this[4 \* i] ta có thể thấy được khi debug xong dòng 9 bằng cách trỏ vào. Tóm lại, dòng for thực hiện so sánh từng kí tự trong chuỗi nhập vào với this[4 \* i](quan sát trực tiếp khi debug, kết hợp sửa cờ để vượt qua các lần lặp for)



Làm tương tự đến hết chuỗi ta nhận biết được chuỗi input cần nhập là encrypted-c-string

Kiểm tra:

