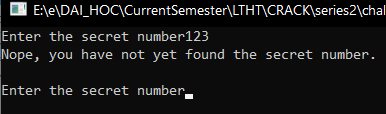
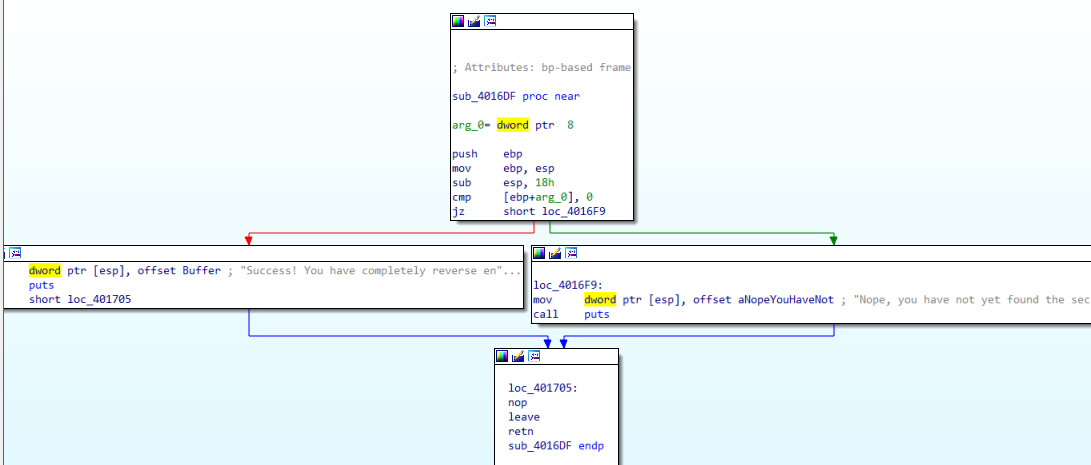
*Nguyễn Mỹ Quỳnh 19520241*

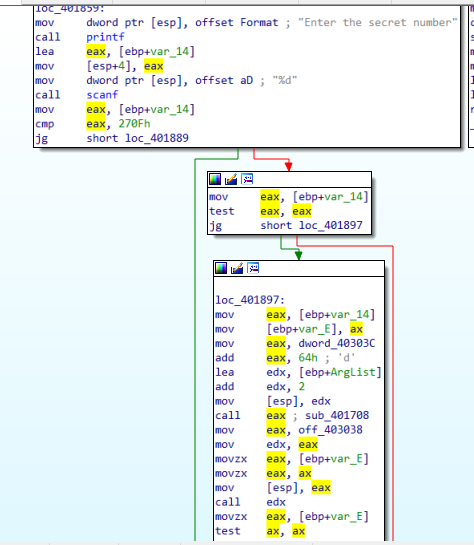
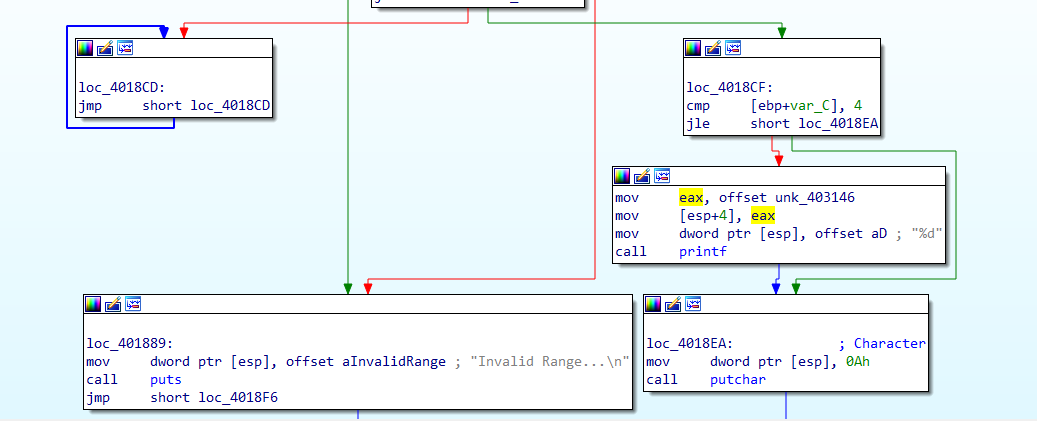
**FindMySecret**

Chạy thử chương trình

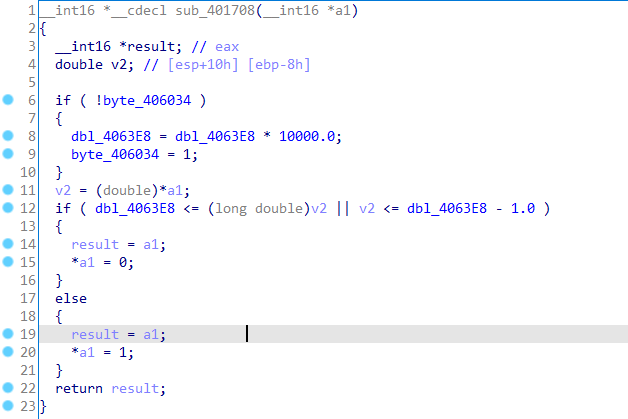


Shift f12 để tìm chuỗi mong muốn. Ta đến nơi gọi chuỗi "Success! You have completely reverse en"... Ta thấy hàm sub\_4016DF nhận tham số đầu vào và so sánh với 0 nếu tham số đó khác 0 thì in ra chuỗi ta mong muốn.

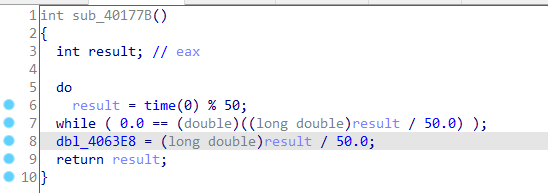
Truy vết xem hàm nào gọi hàm sub\_4016DF (off\_403038) thì ta đến được hình dưới. Tại đây ta thấy secret number được lưu trong thanh ghi eax, sau đó đem so sánh với giá trị 270Fh= 9999, nếu lớn hơn 9999 hoặc nhỏ hơn bằng 0 thì chương trình sẽ jump đến label loc\_401889 và in chuỗi “Invalid Range…” ra màn hình. Vì vậy 🡺 0 < Secret number <= 9999. Trước khi gọi hàm sub\_4016DF (off\_403038) thông qua lệnh call edx, chương trình thực hiện lệnh call eax ; sub\_401708 kết hợp debug ta thấy đây chính là tham số truyền cho hàm sub\_4016DF.



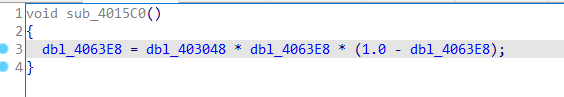
Nhảy vào hàm sub\_401708, ta thấy Nếu double secret number => double dbl\_4063E8 hoặc secret number <=( double dbl\_4063E8 – 1) thì sẽ thất bại(trả về 0 không thỏa những gì ta đã phân tích ở trên). Vì vậy ta sẽ tiến hành tìm secret number thỏa điều kiện trên.



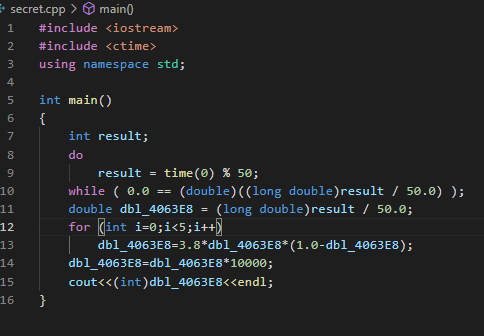
Debug tìm hiểu dbl\_4063E8 ta thấy dbl\_4063E8 được tính từ time(0) - thời gian hiện tại, theo như hình dưới



Tiếp theo debug ta thấy đoạn code này thực thi 4 lần



Viết chương trình c++ tương ứng để tính dbl\_4063E8 và chạy cùng lúc với FileMySecret.exe



Kiểm tra:

