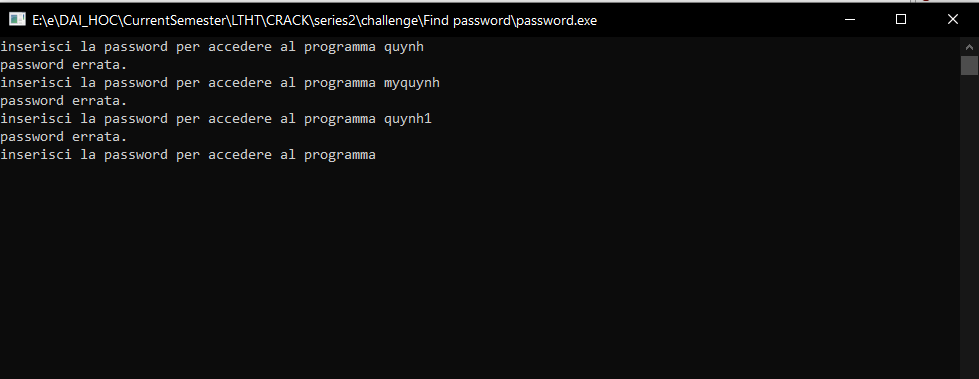
*Nguyễn Mỹ Quỳnh 19520241*

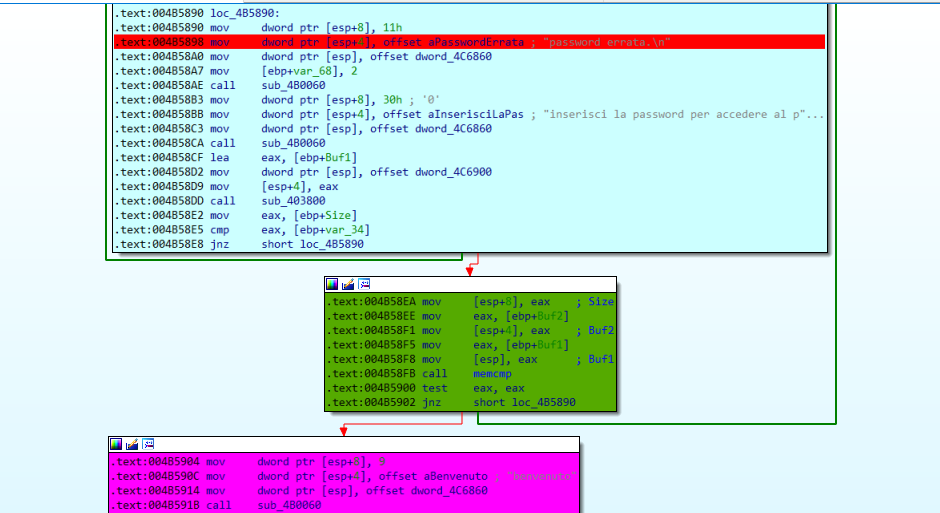
**Find password**

Chạy thử chương trình thì thấy chương trình yêu cầu nhập password đến khi đúng thì thôi.

****

Mở IDA shift+f12 tìm chuỗi, ta thấy ngoài chuỗi “password errata.” thông báo pass sai còn có chuỗi "benvenuto" (google dịch nghĩa chào mừng). Vì vậy ta tiến hành tìm nơi có gọi chuỗi 

Ta thấy để đến được khối hàm gọi chuỗi "benvenuto" màu hồng thì kết quả so sánh trong khối màu xanh lá phải cho kết quả bằng nhau, để đến được khối xanh lá kết quả khối ngay phía trên cũng phải cho kết quả bằng nhau.Tiến hành debug từ khối xanh dương như hình



Debug ta thấy:

+ Lần nhập đầu luôn sai.

+ Lần nhập thứ hai sẽ so sánh 6 và độ dài chuỗi ta nhập vào đúng thì nhảy đến khối xanh lá, khối xanh lá tiếp tục so sánh chuỗi nhập vào với “djejie”, nếu bằng thong báo "benvenuto".

Kiểm tra:

