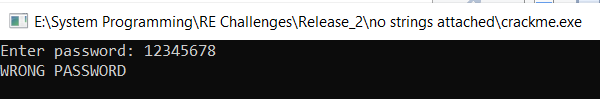
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

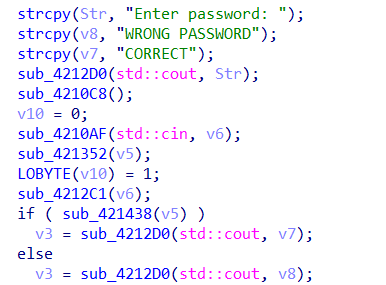
**RE CHALLENGES 2: No strings attached**

|  |  |  |  |
| --- | --- | --- | --- |
| **Giảng viên hướng dẫn** | **Phạm Văn Hậu** | | **ĐIỂM** |
| **Sinh viên thực hiện 1** | **Trần Đức Lương** | **19521815** |  |

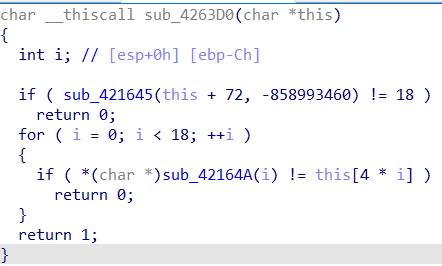
Đây là file exe PE 32-bit. Thử chạy chương trình với password nhập vào là **12345678** thì chương trình báo sai “**WRONG PASSWORD”.** Ý tưởng của bài này cũng là đi tìm password đúng để chạy chương trình thành công.



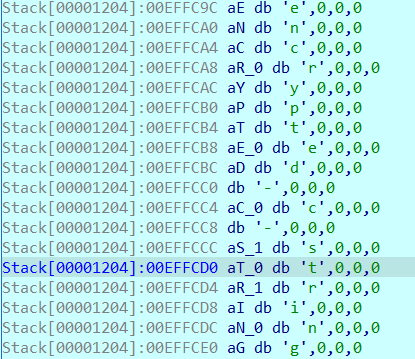
Mở file bằng IDA Pro, thực hiện mở hàm main để phân tích code.



Nhìn vào hình trên, chúng ta có thể quan sát thấy password chúng ta nhập vào lưu ở v6 và để chương trình cout ra chuỗi v7, tức là “**CORRECT**” thì giá trị trả về của hàm **sub(421438(v5))** phải bằng **1**. Thực hiện truy xuất hàm đó thì chương trình dẫn đến hàm **sub\_4263D0()** (hàm này cũng phải return về 1).



Ở hàm này chỉ ra rằng, chúng ta phải nhập vào password dài 18 ký tự, và tiếp theo để hàm này trả về 1 thì từng kí tự của password phải bằng **this[4\*i]** (với i chạy từ 0 đến 17). Debug chương trình thì thấy giá trị của this như hình dưới. Có thể thấy **this[0] = ‘e’**, **this[4] = ‘n’**, …. Tương tự như thế suy ra password cần tìm dài 18 ký tự là: “**encrypted-c-string**”.



Thực hiện chạy chương trình với password là “**encrypted-c-string**”, chương trình báo đúng.

