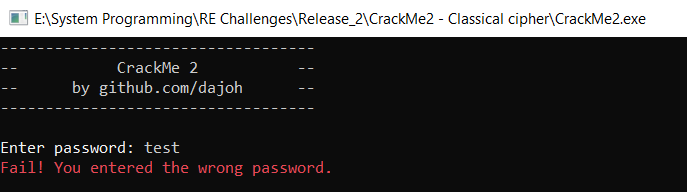
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

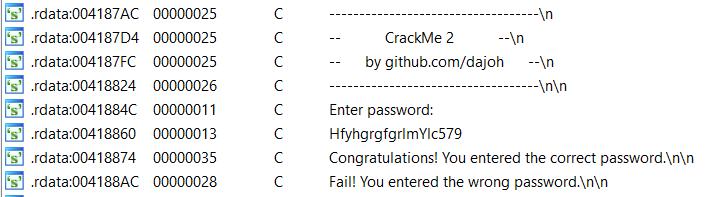
**RE CHALLENGES 2: CrackMe2 - Classical cipher**

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

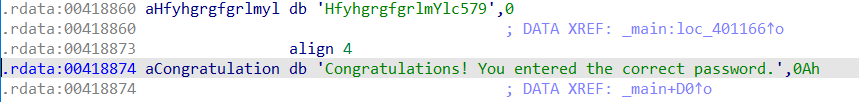
Đây là file thực thi PE 32-bit. Thử chạy chương trình với password là **test** thì chương trình báo thất bại như hình dưới. Ý tưởng bài này là đi tìm password nhập vào đúng thì sẽ thành công.



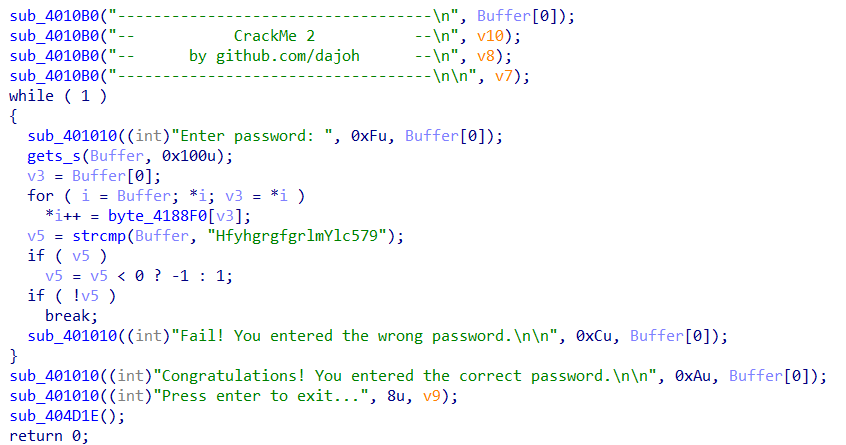
Mở file bằng IDA Pro bắt đầu dịch ngược, mở **subview strings** thì thấy dòng “**Congratulations! …**” chính là mục tiêu chúng ta cần hướng đến.



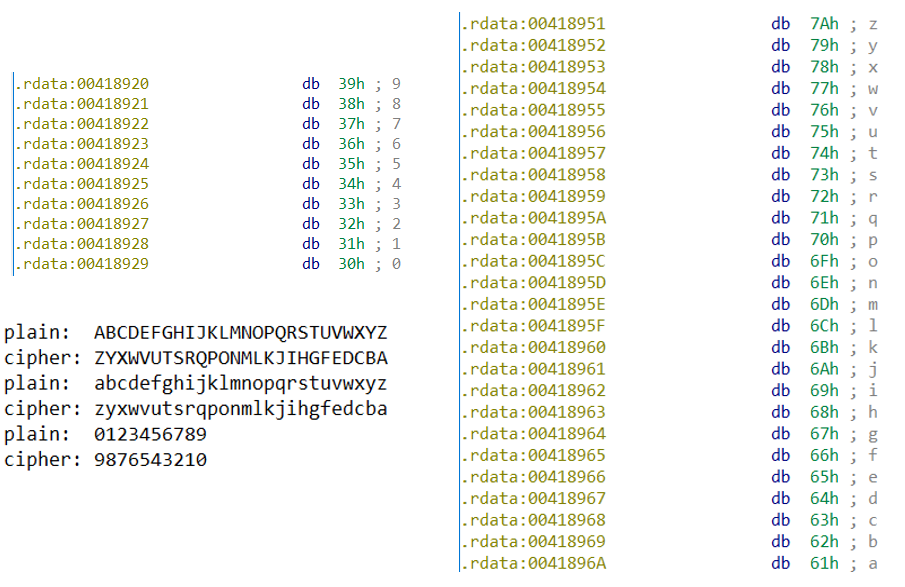
Thực hiện truy vết string trên thì thấy nó nằm ở trong hàm **main**.



Mở hàm **main** và bắt đầu phân tích code.



Ở đây biến **Buffer** là mảng char lưu password mà chúng ta nhập vào. Để in ra được dòng chữ thành công, chúng ta phải nhập password sao cho giá trị **v5 = 0** để break ra khỏi vòng while, trong đó **v5** chính là giá trị trả về của hàm **strcmp** giữa **Buffer** và chuỗi “**HfyhgrgfgrlmYlc579**”. Như vậy, chuỗi Buffer sau khi chạy qua vòng for phải bằng “**HfyhgrgfgrlmYlc579**”. Ở vòng for, chương trình thực hiện đổi từng kí tự của **Buffer** nhờ vào mảng **byte\_4188F0**. Kiểm tra mảng **byte\_4188F0** thì thấy nó giống với một số thuật toán mã hóa cổ điển, cụ thể hoán vị vị trí của các kí tự theo chiều ngược nhau. Ví dụ như kí tự ‘a’ sẽ thành kí tự ‘z’ hay kí tự ‘0’ sẽ thành kí tự ‘9’(hình dưới).



Có thể hiểu rằng “HfyhgrgfgrlmYlc579” chính là ciphertext của Buffer sau khi được mã hóa theo cách trên. Bằng cách giải mã ngược lại theo công thức trên hình, ta được Buffer chính bằng “SubstitutionBox420”. Đây chính là password chúng ta cần tìm.