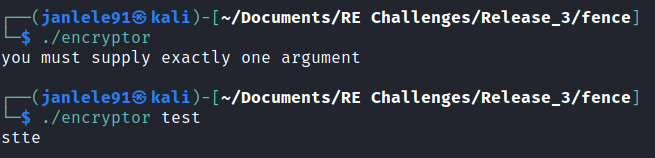
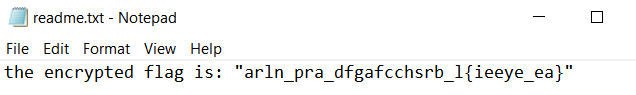
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

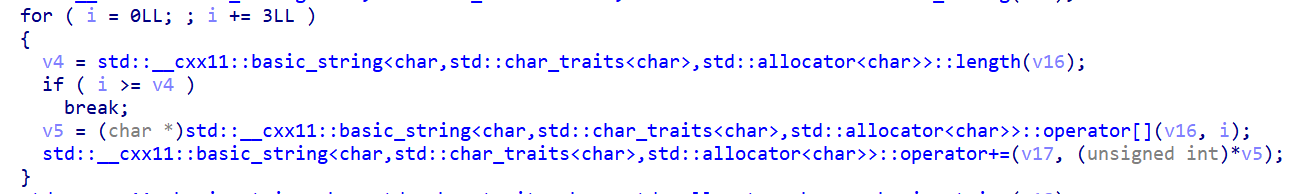
**RE CHALLENGES 3: Fence**

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

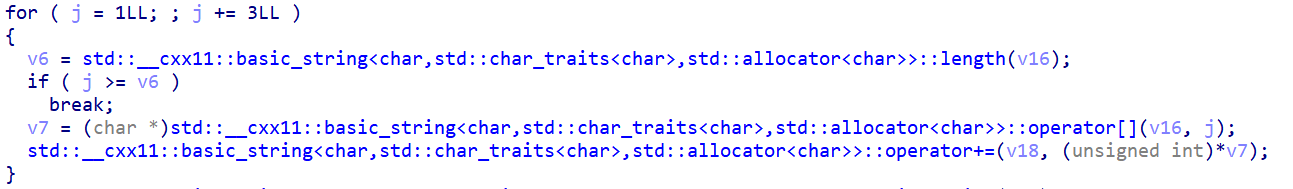
Đây là file thực thi ELF 64-bit. Thực hiện chạy thử chương trình với không tham số đầu vào thì thấy chương trình báo cần thêm đúng 1 tham số. Với tham số đầu vào ***“test”*** chương trình cho ra chuỗi ***“stte”***. Như vậy nhiệm vụ của chương trình encryptor này là encrypt chuỗi tham số đầu vào. (Có thể nghe tên encryptor là đã đoán được.)

Ta mở file ***readme.txt*** được cung cấp thì thấy flag cần tìm bị encrypt thành chuỗi ***“arln\_pra\_dfgafcchsrb\_l{ieeye\_ea}”***. Nhiệm vụ của chúng ta là dựa vào quy luật encrypt của chương trình encryptor để decrypt chuỗi này.

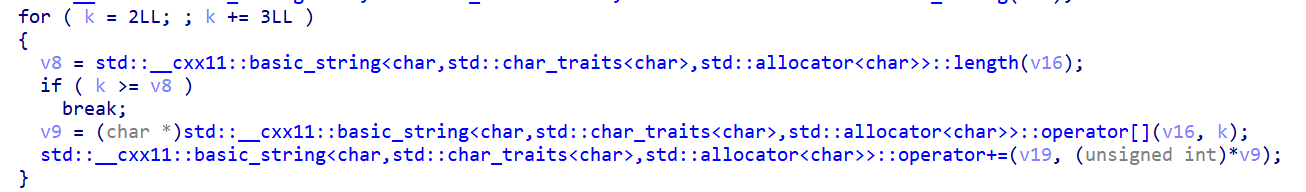
Mở file **encryptor** bằng IDA Pro để thực hiện quá trình dịch ngược. Mở hàm **main**, bắt đầu phân tích:



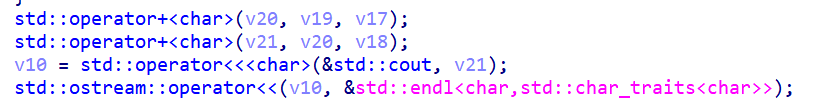
* Vòng for đầu tiên: Chương trình thực hiện nối những kí tự ở vị trí i, với i%3 == 0 thành một chuỗi và lưu vào chuỗi v17.



* Vòng for thứ 2: Chương trình thực hiện nối những kí tự ở vị trí i, với i%3 == 1 thành một chuỗi và lưu vào chuỗi v18.



* Vòng for thứ 3: Chương trình thực hiện nối những kí tự ở vị trí i, với i%3 == 2 thành một chuỗi và lưu vào chuỗi v19.



Khi đó với chuỗi nhập vào, chương trình sẽ in ra chuỗi được encrypt với dạng v19+v17+v18. Như vậy, với chuỗi flag ***“arln\_pra\_dfgafcchsrb\_l{ieeye\_ea}”*** đã bị encrypt, ta sẽ decrypt dựa trên quy luật encrypt trên và được kết quả là ***“flag{railfence\_cyphers\_are\_bad\_}”***. Đây chính là flag chúng ta cần tìm.

