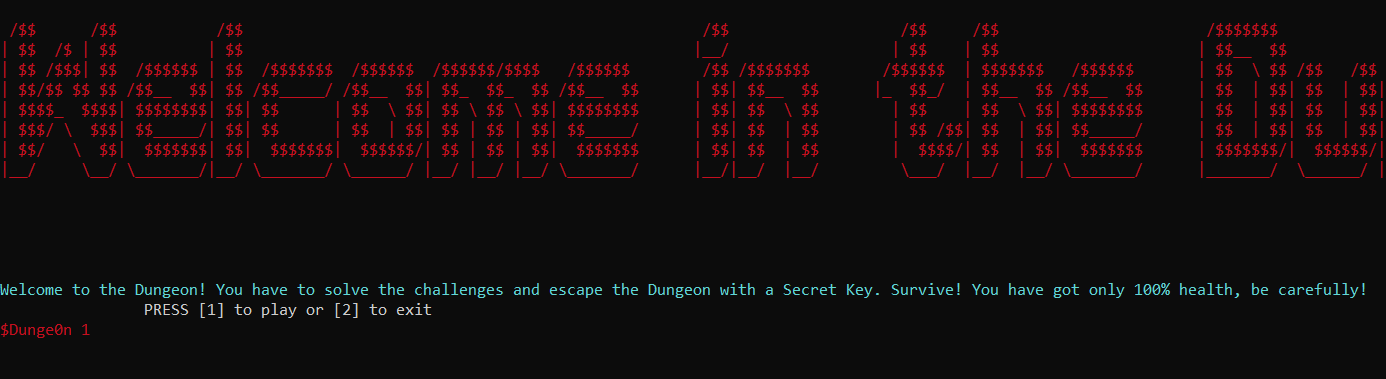
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

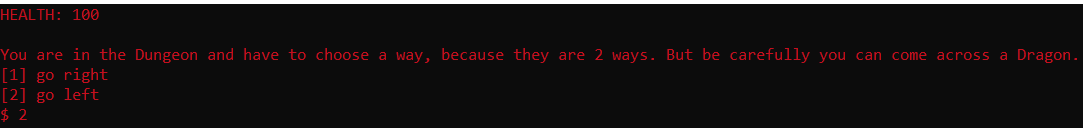
**RE CHALLENGES 2: EscapeTheDunge0n - Expl0it**

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

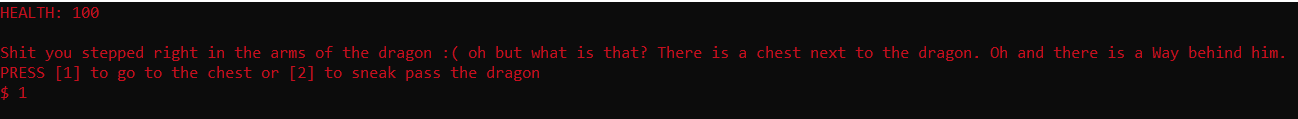
Thử chạy chương trình thì đây thuộc dạng giống game, mình chỉ việc lựa chọn hành động cần làm để vượt qua thử thách để đến cuối cùng là phần nhập Secret Key.



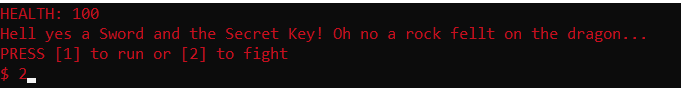
Nhập 1 để chơi.



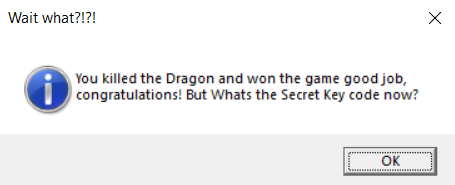
Nhập 2 để vượt qua (bằng cách thử 1 thì thua)



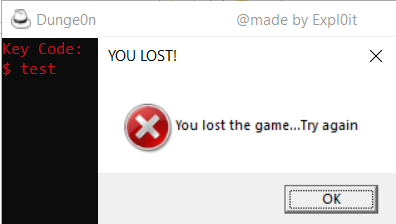
Nhập 1 để vượt qua (bằng cách thử 2 thì thua)



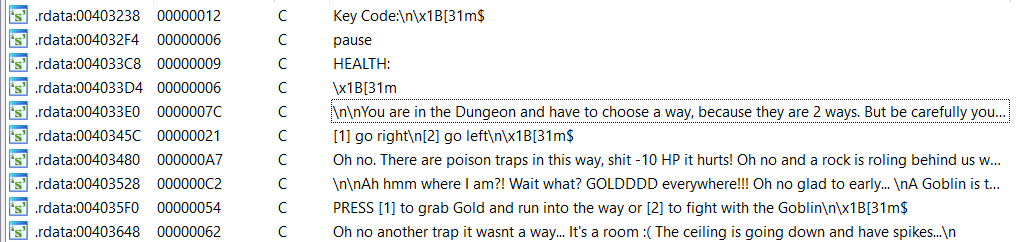
Nhập 2 để vượt qua (bằng cách thử 1 thì thua). Khi đó chương trình thông báo cần phải nhập **Secret Key code** để thắng.



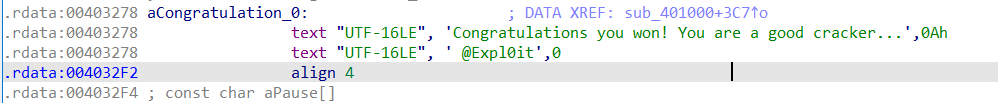
Thực hiện nhập thử code là **test** thì chương trình hiện MessageBox báo thua. Vậy nhiệm vụ của chúng ta bây giờ là đi tìm **Secret Key code** có trong file thực thi bằng phương pháp dịch ngược.



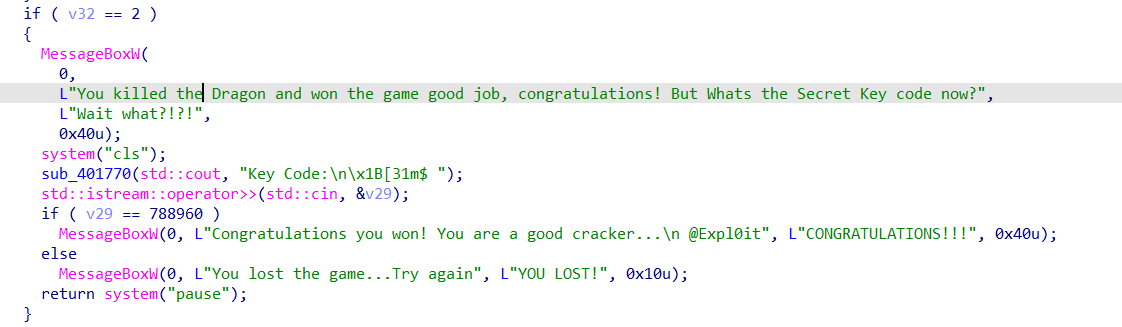
Mở file bằng IDA Pro 32-bit, ở **subview strings** thì xuất hiện các dòng miêu tả có trong trò chơi.



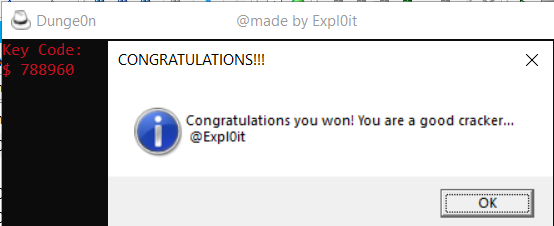
Thực hiện truy vết thì thấy các strings này nằm trong hàm **sub\_401000**.



Mở code hàm **sub\_401000**, chúng ta chỉ cần tìm đến phần code chứa phần nhập **Secret Key code**.



Quan sát có thể thấy code chúng ta nhập vào được lưu vào biến **v29**, nếu nó bằng **788960** thì một MessageBox hiện ra “**Congratulations you won! …**”. Đây chính điều chúng ta mong muốn.



Thực hiện nhập code bằng **788960** chương trình báo thành công.