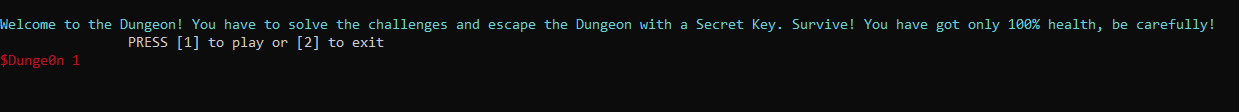
*Nguyễn Mỹ Quỳnh 19520241*

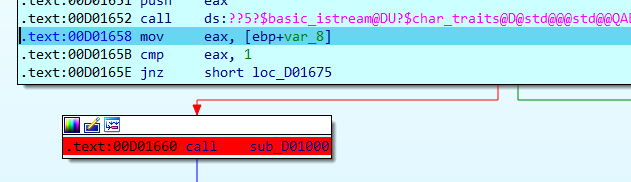
**EscapeTheDunge0n - Expl0it**

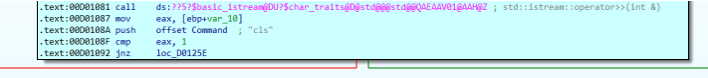
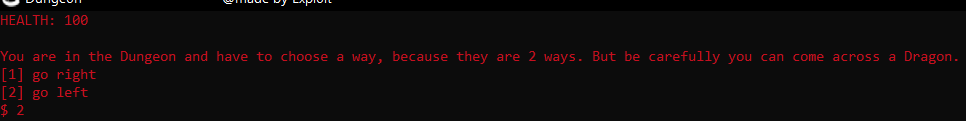
Sau khi chạy thử vài lần, ta thấy: đầu tiên nhập 1 để bắt đầu game, tiếp đó chương trình yêu cầu nhập 1 hoặc 2 trong các bước để điều khiển game để giết rồng, sau đó cần nhập Key để win game.

Tiến hành debug để thấy rõ các bước:

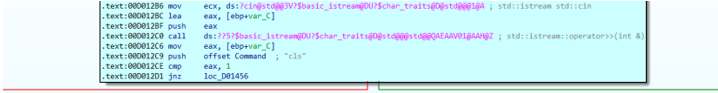
+ Sau khi nhập 1 để play game, chương trình gọi hàm sub\_D01000.

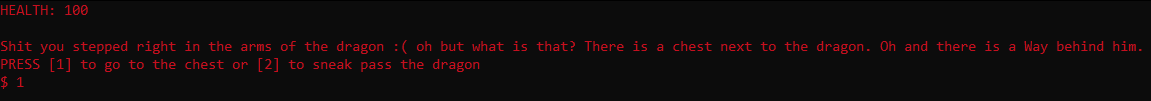


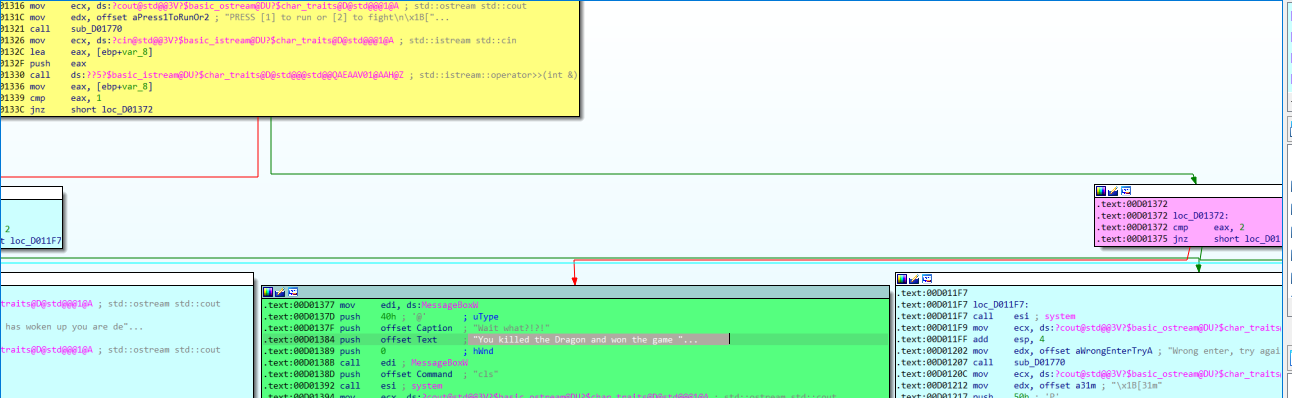


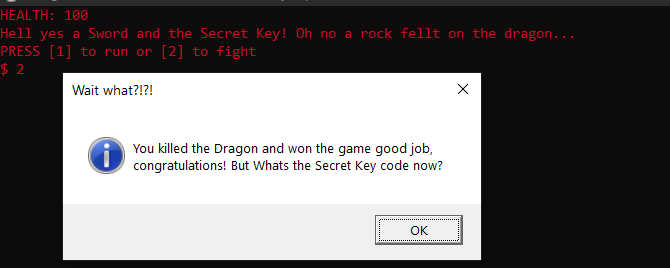
+ Tiếp theo debug tại đây nếu nhập 1 sẽ nhảy tới khối có “Oh - no” nên ta nhập 2

+ Tiếp theo debug tại đây nếu nhập khác 1 sẽ nhảy tới loc\_D01456 dẫn tới "Wrong enter, try again!\n " hoặc "Shit the dragon has woken up you are de"... nên ta nhập 1.





+ Tiếp theo ta cần đến khối màu xanh lá có chứa chuỗi "You killed the Dragon and won the game "... ở khối màu vàng so sánh nếu ta nhập khác 1 nhảy đến khối hồng, khối hồng so sánh nếu ta nhập bằng 2 nhảy đến khối màu xanh. Vậy nhập 2



+ Tiếp theo key nhập vào được so sánh với 0x0c09E0(hex) = 788960

Vậy ta nhập key tương ứng 