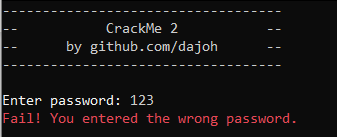
*Nguyễn Mỹ Quỳnh 19520241*

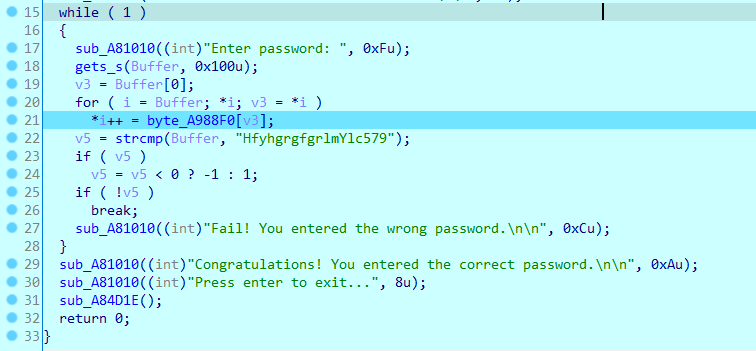
**CrackMe2 - Classical cipher**

Chạy thử chương trình

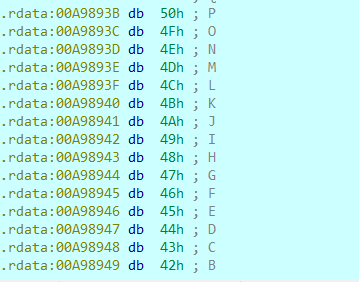


HfyhgrgfgrlmYlc579

Xem mã giả của chương trình ta thấy chương trình yêu cầu nhập pass cho đến khi nào đúng thì thông báo "Congratulations! You entered the correct password.” Ta thấy để đến được dòng 29 thì lệnh break ở dòng 26 cần được thực hiện, vậy v5 phải bằng 0. Từ dòng 22 ta thấy v5=0 khi chuỗi buffer bằng chuỗi "HfyhgrgfgrlmYlc579". Buffer là chuỗi ta nhập vào và được biến đổi ở dòng 20, 21 trước khi đem so sánh. Cụ thể dòng 20, 21 duyệt từng kí tự chuỗi buffer và lấy đó làm index để truy xuất phần tử tương ứng trong byte\_A988F0 và gán giá trị phần tử đó lại trong buffer.



Với kí tự đầu tiên v3 trong buffer ta cần tìm v3 sao cho byte\_A988F0[v3] = ‘H’



Nhấp vào byte\_A988F0 để xem ta thấy H ở vị trí 83 = 0x53 (tra bảng ASCII ta thấy đó là kí tự S).

Làm tương tự với các kí tự còn lại của buffer ta suy ra được chuỗi buffer là “SubstitutionBox420”

Kiểm tra:

