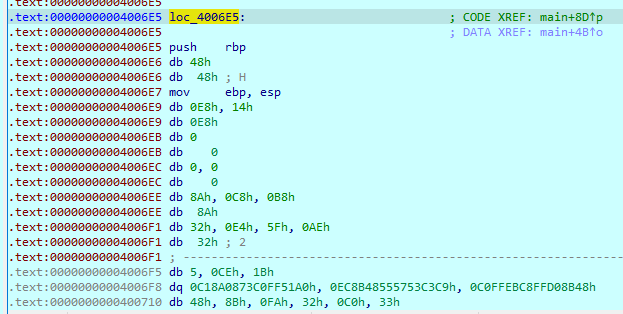
One for all:

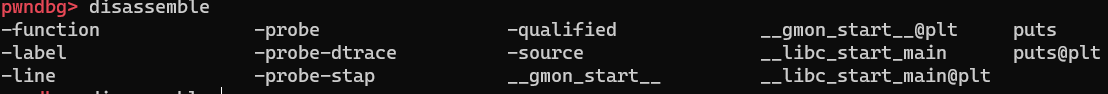
SetIP qua các đk return -1, đặt bp tại cmp instruction, loop qua 30 lần check kí tự đc flag:

Crackmexxx:

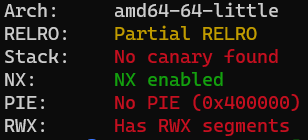


Lúc e thử skip vòng for và đặt bp tại call loc\_4006E5() thì run lỗi nên e đoán loop trên để decrypt code. Rồi e đặt bp tại call loc\_4006E5() để xem

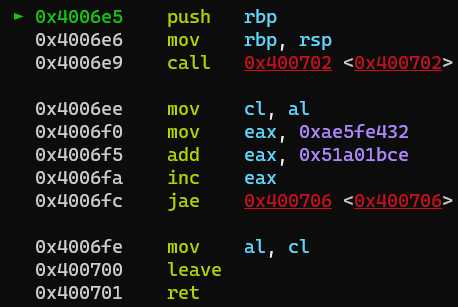


☹  
e chuyển sang dùng pwndbg  


Nhung ko thấy có main()

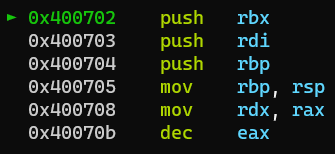
May bài này ko có pie  


Vào ida xem addr rồi đặt bp tại call loc\_4006E5()  
dùng pwndbg debug  
Vao loc\_4006E5()



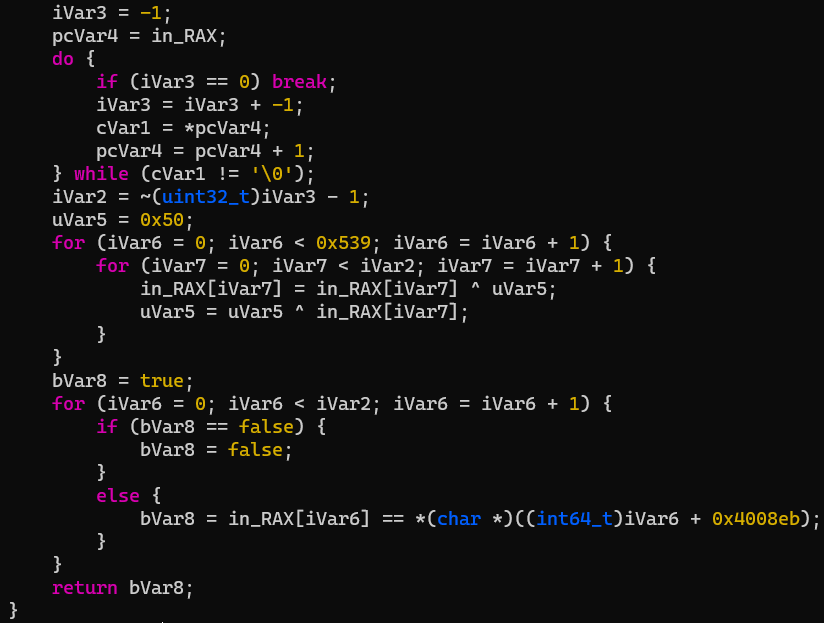
Kqua tra ve la tu ham 0x400702() ->al

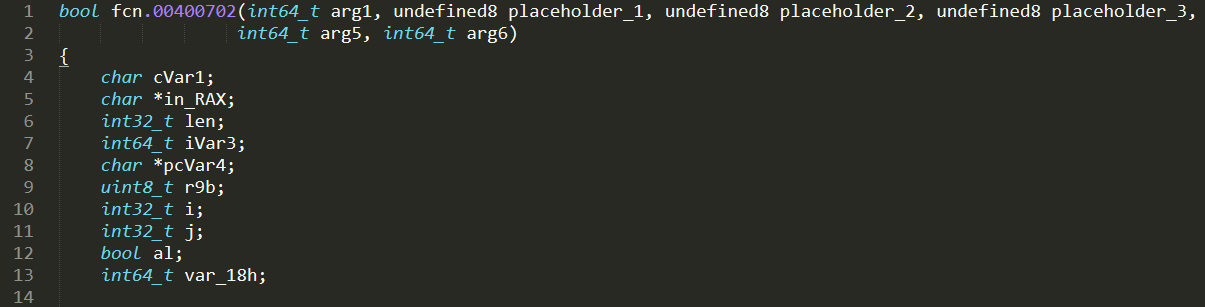
Jae [jump if above or equ] se ko dc thuc thi

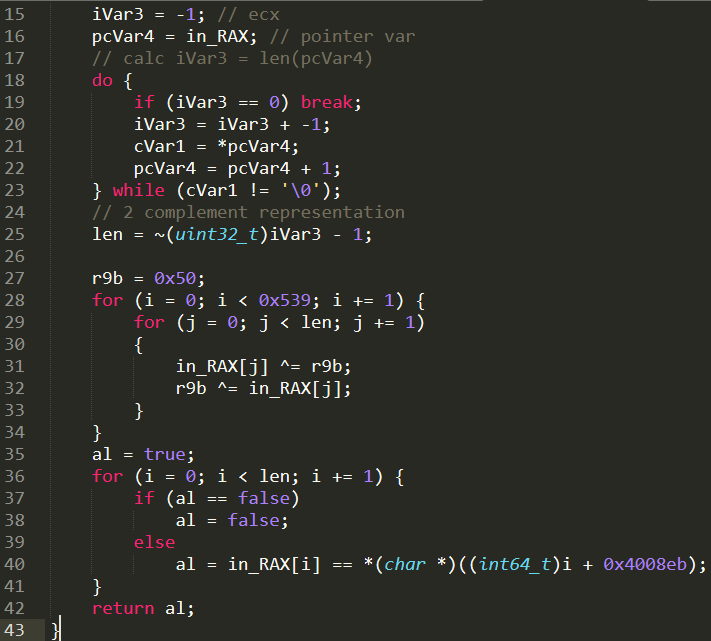


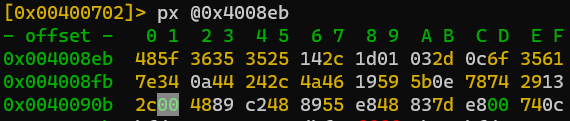
Step den dec eax  


Dung r2ghidra-radare2









* Len flag = 33

