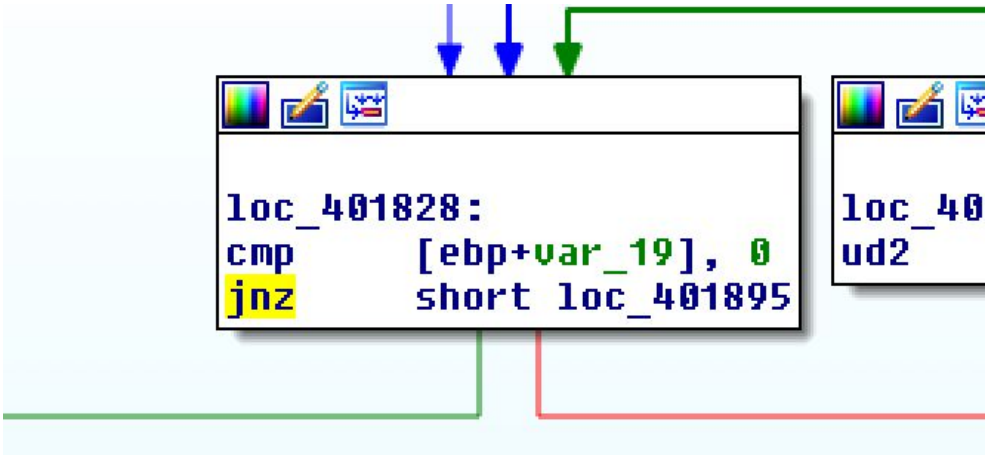
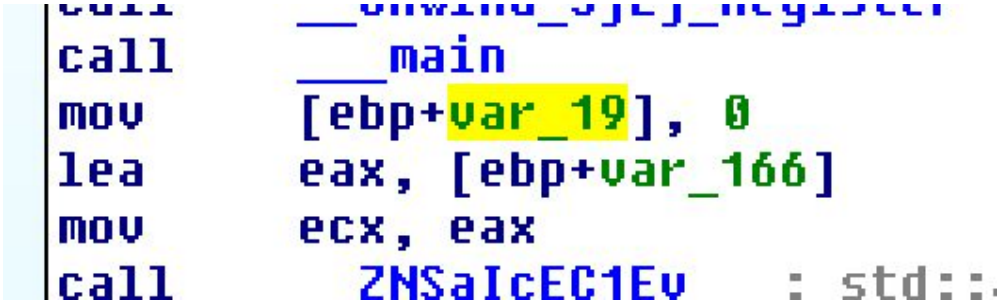
Song Yang (sy540)
Xin Yang (xy213)
Zhuohang Li (zl299)

Homework7

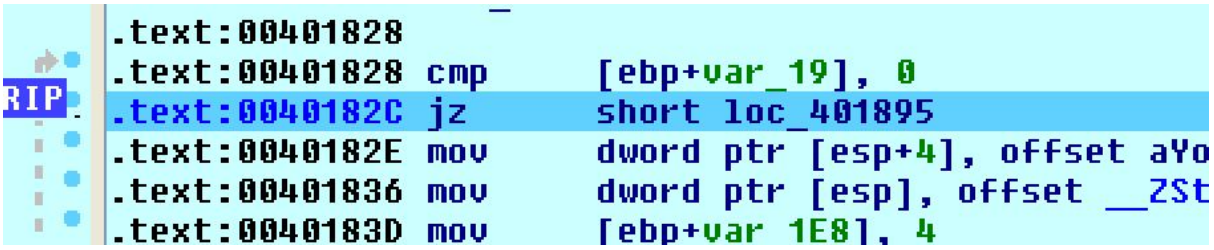
1.We first found that before the program goes into the password section, it will compare var_19 with 0, if they are equal, then let user input password.



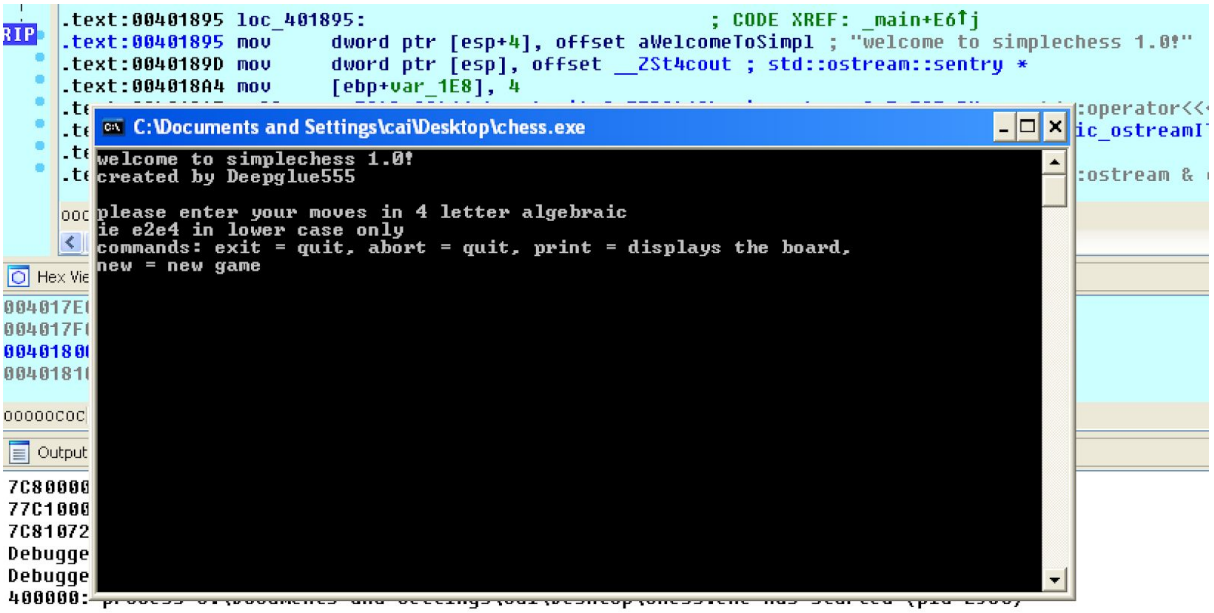
var_19 is initially assigned with 0, so every time the program runs it will ask for password.



So to get rid of the password, we can simply change this instruction from “jnz short loc_401895” to “jz short loc_401895”:



And we run the program again. This time, we are able to play the game without typing the password.


.text:00401895 loc_401895: ; CODE XREF: _main+E6↑j
.text:00401895 mov dword ptr [esp+4], offset aWelcomeToSimpl ; "welcome to simplechess 1.0!"
.text:0040189D mov dword ptr [esp], offset __ZSt4cout ; std::ostream::sentry *
.text:004018A4 mov [ebp+var_1E8], 4
C:\Documents and Settings\cai\Desktop\chess.exe
welcome to simplechess 1.0!
created by Deepglue555
please enter your moves in 4 letter algebraic
ie e2e4 in lower case only
commands: exit = quit, abort = quit, print = displays the board,
new = new game
Hex Vie
Output