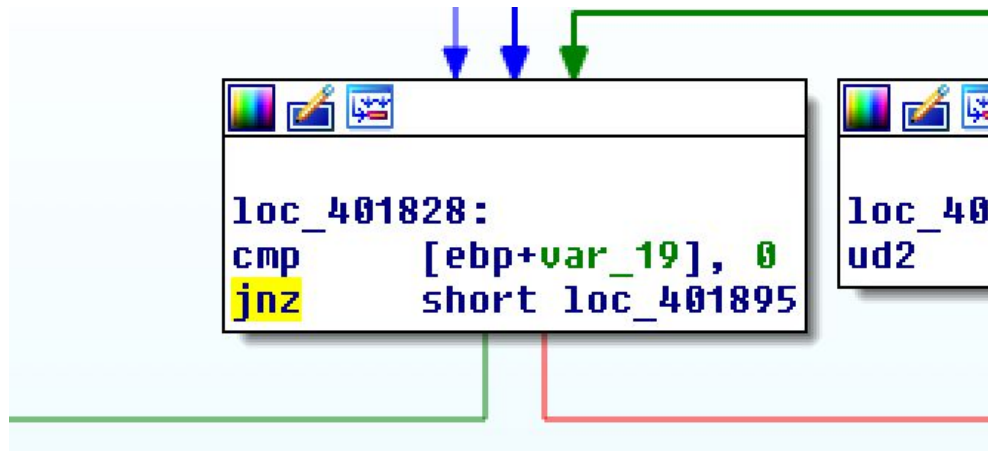


Song Yang (sy540)
Xin Yang (xy213)
Zhuohang Li (zl299)

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.

```
call    ___main
mov     [ebp+var_19], 0
lea     eax, [ebp+var_166]
mov     ecx, eax
call    ZNSaIcEC1Ev : std::
```

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

```
.text:00401828
.text:00401828 cmp     [ebp+var_19], 0
.text:0040182C jz      short loc_401895
.text:0040182E mov     dword ptr [esp+4], offset aYo
.text:00401836 mov     dword ptr [esp], offset __ZSt
.text:0040183D mov     [ebp+var_1E8], 4
```

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

The screenshot shows a debugger window with two panes. The top pane displays assembly code with the following instructions:

```

.text:00401895 loc_401895:                ; CODE XREF: _main+E6fj
.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

```

The bottom pane shows a console window titled "C:\Documents and Settings\cai\Desktop\chess.exe". The console output is as follows:

```

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

```

The console window also shows a list of memory addresses on the left side, including 004017E0, 004017F0, 00401800, 00401810, 000000C0, 7C800000, 77C10000, 7C810072, Debugge, and 40000000.