HW3 Solutions

Student: Yanhan Lin

Q1.

According to the slides on lecture, change assembly code of CRACKME.exe, which is change CMP EAX, EBX to CMP EAX, EAX. Therefore, no matter what serial I input is, the result will show message of ‘Great work, mate! Now try the next CrackMe’ .

Q2.

To understand what does assembly code mean, I reviewed the assembly code involving function call of messageboxA and code about how serials generated. After reviewing, The Crackme check the name we input, if it includes numbers or other symbols return failure message. It checks the word letter by letter, and then calculate their ASCII code from 65 to 90, which means all of letters are uppercase there. Then the binary code of name will XOR with 5678. The result of this calculation will XOR with 1234. The final result is the answer we want. For example,

YANHAN = Y + 2A + 2N + H = 89 + 65 * 2 + 2 * 78 + 72 = 447.

447 0000 0001 1011 1111
XOR 5678 0101 0110 0111 1000
0101 0111 1100 0111
XOR 1234 0001 0010 0011 0100
0100 0101 1111 0011 = 17907

same as SHIFU, YUJIE, YIMING. Results has been posted on Canvas.