NAME: **ALPHA:**

SY485J: Lab 8: Bringing Down the House

Go to http:/courses.cyber.usna.edu/~debels/SY485J/Code/Lab8. There is one executable, blackjack. You will be analyzing several vulnerabilities in blackjack and making yourself a millionaire. You are free to use any of the techniques we've discussed in this class. Turn in this Lab Worksheet (both sides) in the submit system giving the answers to the following 6 questions along with your bank file, showing a balance of at least $1 million. This lab is **due November 7, 2019 by 0955**.

1. (20 points) What is the secret key used to generate the HMAC for the bank file?

2. (20 points) What are the contents of the message that is signed?

3. (10 points) What are the steps you took to change your bank balance to $1,000,000?

4. (10 points) Turn in (via soft or hard copy) your bank file with a balance of $1,000,000. The bank file **must** have the correct authentication HMAC.

NAME: **ALPHA:**

5. (20 points) There is at least one buffer overflow vulnerability in the blackjack code.
    a. Where is it?

    b. How could an attacker take advantage of this to modify a bank balance?

    c. What could the programmer have done to eliminate this buffer overflow?

6. (20 points) What are two anti-reversing techniques that could be used to thwart the attacks you described/performed above (defeating authentication and buffer overflow attacks)?