Josh Levy – EECS349 HW3 part 1

1) The modified executable in contained in this repo, called CRACKEDME.EXE. I changed the instruction where the program compares the username hash to the password hash, from 'CMP EAX, EBX' to 'CMP EAX, EAX'. As a result, this check always passes and the entered login is always considered valid.

2) The executable hashes both the username and password entered to calculate which values are valid.

   For a username, only letters are allowed in the name. The letters are changed to all capitals, and their ascii character codes are added together. The result is then XOR'ed with the hex value 5678.

   A valid password can be constructed with just numbers. The executable first converts the string of the entered password to a hex number with the same numeric value. It then XOR's this with the hex value 1234.

   To get the password for a given name, find the hashed value for the username. We can then invert the password hashing to get a valid password. To do this, XOR your username hash with the value 1234. This undoes the XOR in the password hashing. You can then use any tool to determine the base 10 representation of the resulting number (I used the built in windows calculator app in programmer mode). This gives the following name/password pairs:

   Josh – 17784
   Shifu – 17715
   Yujie – 17866
   Yiming – 17793

   Using any of these pairs will result in a valid login on the original file.