Lab 3 - Matryoshka

SUMMARY:

Test your understanding of reverse engineering 32-bit Windows binaries where the source code is not available. Analyze the binary and determine the five (5) passwords required to get the program to print "**success**".

REQUIREMENTS:

The student is required to research and determine the five passwords needs to get the supplied program to print "**success**". Each password must be entered successfully to be prompted for the next password. Once all five (5) passwords have been entered successfully, the program will print "**success**". If any password is entered incorrectly, program execution will terminate. The student is required to create a key generator program that will print all the passwords needed to successfully run the program. Be warned that each password is progressively tougher to crack and that not all password values are static.

WHAT TO SUBMIT:

Email me a link to the GitHub repository where your code resides.

COLLABORATION:

This is a group assignment and students make work in groups of up to three (3) students. The knowledge gained in determining each password can be shared, but each student is expected to turn in their own key generator program.

GRADING:

Grades are assigned based on meeting the requirements for each password. 200 points total. Password 1 is worth 30 points. Password 2 is worth 30 points. Password 3 is worth 40 points. Password 4 is worth 50 points. Password 5 is worth 50 points. Partial credit is given if a password is incorrect but the concepts are close. Placing your commented IDA database file in your Git repository allows we to give partial credit more readily, but is not required.

DUE:

11:59 P.M. March 17, 2017