Assignment 2: Cracking Passwords and Extracting Stego Message

Total Points: 40

Due: October 16, 2017 (Monday) at 11:55 PM

Hello! Today is the day for a new mission. Our officers (after obtaining a proper warrant, of course) seized a server from StarTrekker Inc. We suspect that this company may have been distributing copyrighted materials, illegally. Our mission today is to find those copyrighted materials on this server and verify that they are actually copyrighted. After thorough investigation, we have discovered a folder containing numerous *ZIP* files. We believe all the files we are looking for have been compressed into these *ZIP* files. The problem is that these *ZIP* files are password-protected, so we cannot simply access them. Obviously, our task is supposed to be difficult! Luckily, however, we are able to unearth a database table that contains *ZIP* filenames and their corresponding password hashes.

Accsss info

Filename	Password
Jkirk.zip	9aeaed51f2b0f6680c4ed4b07fb1a83c
Lmccoy.zip	172346606e1d24062e891d537e917a90
Cchapel.zip	fa5caf54a500bad246188a8769cb9947

Some investigative leads:

- The data stored in *Password* column are *MD5* hashes of the actual passwords.
- The *Access Info* table has a constraint that only accepts all lowercase alphabetic (a to z) characters of length five as passwords. (Sample password: tempo. Too easy to crack, right? Yay!)
- We highly suspect that there are going to be pictures compressed in **two** of these *ZIP* files. If we find a **Watermarked** picture, we conclude that it is copyrighted.
- The knowledge in **Steganography** and **Watermarking** using *Least Significant Bit* will be very helpful.

Further instructions:

1. Write a program in Python 2.7 to crack all the passwords from hashes. You will most likely have to brute-force them.
2. Using cracked passwords, un-compress the *ZIP* files to inspect their content.
3. The picture in a *ZIP* file containing only one picture is probably **watermarked**.
4. Write another program in Python 2.7 to extract the *watermarked copyright notice* from that picture.
5. Installing a *Python Image Library* (released only for Python 2.7 and below) and using the *Image* module will make your task about 71.4534% easier.

Bonus: One of the pictures in another *ZIP* file also has a hidden message. You will be rewarded five points bonus in this assignment, if you successfully extract it.

Submission Guidelines:

1. Save all the passwords you crack into a *passwords.txt* file along with their corresponding *ZIP* filenames.
2. Save both Python Programs (password_cracker.py, message_extractor.py).
3. Create a "*Read Me.pdf*" file containing:
    a. Your name
    b. A detailed paragraph explaining all the steps you went through to complete this assignment.
    c. The watermark notice you extracted and name of the picture file you extracted it from.
    d. The hidden message you found (if bonus challenge attempted).
4. Compress all these files into a single *ZIP* file. Name your *ZIP* file "*LastName_Assignment_2.zip*" and upload it to **Moodle**.

DISCLAIMER: By submitting this assignment, you agree that you are solely responsible if you use the idea used in this assignment outside of the scope of this course. In simple words, do NOT attempt cracking others' passwords or do anything illegitimate!