CSC 110 – Lab 8
Digital Forensics Algorithms

Names: _____

Introduction
The purpose of this lab is to understand some algorithms that are useful for digital forensics and to practice implementing parts of these algorithms in Python.

Exercises

1) In class we looked at several simple algorithms to compute a digital signature. As a review, answer the following questions:

    a) What is the purpose of a digital signature in a digital forensics investigation?

    b) Why was the checksum algorithm that we looked at in class NOT a good digital signature algorithms for use in a digital forensics investigation?

Instructor Initials: _____

2) Write a checksum algorithm that creates a 16-bit checksum instead of an 8-bit checksum. Use the code we wrote in class as a starting point.

   Test your program with the following strings and record the checksum for each:

   ELVIS

   LIVES

   REBA

   BARE

   Explain the results.

Instructor Initials: _____

3) Python has a function for computing an MD5 digital signature, which can be used in a digital forensics investigation. Take a look at this Python program that uses the MD5 function:

   http://www.cs.uri.edu/~cingiser/csc110/labs/md5_sig.py

   What is the name of the Python library in which the MD5 hash function is found?

4) Now let's use this program to compute an MD5 signature.

- Create a text file and include at least 5 lines of text in the file.
- Save the text file in the same place where you saved the `md5_sig.py` program, and close the file.
- Run the `md5_sig.py` program. When it asks for a file to hash, enter the name of the text file you created.
- What is the MD5 digital signature that is created?

- Make a copy of the text file that you created by right-clicking on the file and choosing Copy (or Duplicate on a Mac). Change the name of the copy to a new name.
- Run the `md5_sig.py` program, this time on the copy of the text file you created.
- What is the MD5 digital signature that is created? Explain the results.

- How does this copying process you just went through relate to the process used in a digital forensics investigation?

- Open the duplicate text file again, and add a line of text to the end of the file, and then close the file.
- Run the `md5_sig.py` program on the file again. What is the MD5 digital signature? Explain this result.

- How does what you have seen here relate to what an investigator might see when working on digital evidence?

Instructor Initials: _____

Challenge Problems

1) We have the algorithm for converting a binary number into decimal implemented in Python. For this challenge problem, write a Python program that converts a decimal number into binary.

Instructor Initials: _____

2) Write a Python function to convert a hexadecimal number (stored as a string) into a decimal number (integer).

Instructor Initials: _____