**CIS 313 – Cryptography – Hashing Exercise**

**Name: James Chad Ballay**

The objective of this exercise is to allow you to explore hashing algorithms. Answer all questions.

1. Download the latest version of the Windows binary MD5 zipped file from the following link:

<https://github.com/jessek/hashdeep/releases/tag/v4.4>.

Note1 : If this link doesn’t work, search for MD5. You only need to download and use the md5deep program.

Note2: These instructions require you to use Windows DOS commands. If you’re not familiar with this, see the tutorial at <http://idcontent.bellevue.edu/content/id/CIT/CIS/607/Windows%20DOS%20Tutorial/html/>.

Note3: This program may generate a warning that you are running a 32 bit program on a 64 bit system. This is only a warning and the program will still work. The generated hash will follow the warning.

1. Create a folder on your c: drive using your last name as the label. Example mkdir c:\*sampson*.
2. Unzip the zipped file into the c:\*yourlastname* folder.
3. Open up Word and enter the following text:

Now is the time for all good men to come to the aid of their country.

Save as c:\*yourlastname*\md5deep-4.4\Country1.doc.

1. Open up a command window and navigate (cd) to c:\*yourlastname*\md5deep-4.4
2. Obtain the hash for Country1.doc by typing **md5deep Country1.doc** at the command prompt and pressing **Enter**. Record the entire hash in the space provided below.

**Hash from file:** \_\_\_ 8534eaefbe350e214cbcaa11f9d81f4b\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NOTE: Each of the programs has a 32 bit and a 64 bit version. While you can run the 32 bit version on a 64 bit OS you will get a warning. The 64 bit versions of the programs have a 64 at the end of them. For example, md5deep and md5deep64

1. MD5 has the capability of hashing from keyboard input as well as from file input. To illustrate, in the command window, type in md5deep and press enter. Type in “Now is the time for all good men to come to the aid of their country.” (without the quotes), press enter, hit CTRL+Z, then press enter. The hash of your text should appear. Record the entire hash in the space provided below:

**Hash from command line:**\_\_\_ f1f798aa8f3305109ae440087f73cfd8\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Compare the length of both hashes (in number of characters or bits) and contents and record your findings below. Are the hash values the same or different? Explain why.

\_Length is the same. This is because it outputs a 32 character hexadecimal string with two spaces at the end. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. This utility comes with a number of hashing generators, all of which are in the same directory as md5 and SHA256. Each one produces different output. Complete the following question for SHA1, SHA256, whirlpooldeep and tigerdeep.
2. SHA1deep hash of abcdef-123:

**Hash from command line:**\_\_\_\_\_ 6320dc54aa431d1b9266467e82f9442c33d6b9f9 \_\_\_\_\_\_\_\_\_

**Number of characters:** \_\_\_\_\_\_43. (40 hexadecimal with 3 spaces.)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. SHA256deep hash of abcdef-123:

**Hash from command line:** a1586648199e7e6f09ef9452100613dcd6674d1c203eb3ca203529dba2383e9e

**Number of characters:** \_\_67. (64 hexadecimal with 3 spaces.)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Whirlpooldeep hash of abcdef-123:

**Hash from command line:**\_ e4d09683c9b98302f69f94bb20648b084d163bb29c68ac285822419c3f38e67537afef66d0159f681152e7735965e76193d1bf497384fb672e6f3ad4b6192444

**Number of characters:** \_\_131. (128 chars and 3 spaces.)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Tigerdeep hash of abcdef-123:

**Hash from command line:**\_\_ f651508cc99c11744cd24ddefd8e67191249a5d67d7846c5 \_\_\_\_

**Number of characters:** \_51. (48 hexadecimal and 3 spaces.)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Explain why each of the hash values above are different.

\_Each of these different hashing algorithms independantly attack the data. They have different approaches and will therefore yield different approaches. The easiest analogy I can think of would be that everyone performing the act of cooking would be hashing but the specific recipe they cook would be synonmous with different hashing algorithms.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Include a screenshot of your work below.

