**Lab3**

1. **Lab Requirements**

****

**Figure 1: Create new directory and access to it**

1. **Task1:**

**A computer screen with white text

Description automatically generated**

**Figure 2. Creating the string file and feed to the program**

**A blue and white text on a black background

Description automatically generated**

**Figure 3. Find the size of the created file using wc -c**

**A screenshot of a computer

Description automatically generated**

**Figure 4. MD5 value for the 2 files generated**

**A screenshot of a computer screen

Description automatically generated**

**Figure 5. Viewing the binary of the out1.bin**

**A screenshot of a computer screen

Description automatically generated**

**Figure 6. Viewing the binary of the out2.bin**

**Question 1. If the length of your prefix file is not multiple of 64, what is going to happen? (use hexdump to see)**

The md5collgen generates padding using 0x00 bytes to concatenate with the prefix until it gets 64

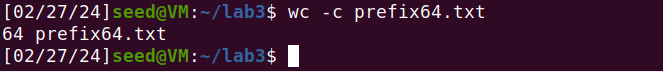
- For the next question, I used python3 to create a new file of “P” that is 64 bytes and feed it into md5collgen to produce two new output files.

**A computer screen shot of white text

Description automatically generated** **A pixelated image of a grid

Description automatically generated**

**Figure 7. Redo all the steps to analyze the working mechanism**

****

**Figure 8. Word count of filing the exact size**

**Question 2. Create a prefix file with exactly 64 bytes, and run the collision tool again, and see what happens.**

This time, md5collgen did not add any padding of 0x00 bytes into the binary files.

- Now use the cmp command to see the differences between the two files in each case.

**A computer screen shot of a computer code

Description automatically generated**

**Figure 9. The differences between the first two files**

**A screenshot of a computer

Description automatically generated Figure 10. The differences between the second two files**

**Question 3. Are the data (128 bytes) generated by md5collgen completely different for the two output files? Please identify all the bytes that are different. (You can use cmp)**

For comparison, the differences between two files:

For: out1.bin and out2.bin

84th 110th 124th 148th 174th 175th 188th

For: out64\_1.bin and out64\_1.bin

84th 110th 111rd 124th 148th 174th 188th