**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

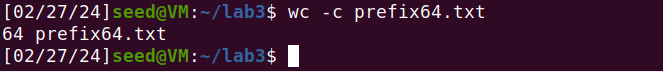
- For the next question, I used python3 to create a new file of “P” that is 64 bytes and feed it into md5collgen to produce two new output files.

**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

1. **Understanding MD5’s Property**

****

**Figure 1. Using a random string to name a suffix file**

**A screenshot of a computer screen

Description automatically generatedFigure 2. Concatenate to the created file and calculate the MD5 value**

**A screenshot of a computer screen

Description automatically generated**

**Figure 3. View the binary of these files**

**A computer screen shot of a black background

Description automatically generatedFigure 4. See the differences between the two files in the task**

1. **Generating Two Executable Files with the Same MD5 Hash (used Ubuntu 16.04)**

**Figure 1. Create a new C program**

**A screen shot of a computer screen

Description automatically generatedFigure 2. The body of our program**

**A screenshot of a computer

Description automatically generatedFigure 3. Modify the permission and run the program successfully**

**A screenshot of a computer screen

Description automatically generatedA screenshot of a computer screen

Description automatically generatedA close up of a computer screen

Description automatically generatedA screenshot of a computer screen

Description automatically generatedA screenshot of a computer screen

Description automatically generatedA screen shot of a computer screen

Description automatically generatedA screen shot of a computer screen

Description automatically generatedA screenshot of a computer screen

Description automatically generated**

**Figure 4. Looking for the binary to search for our “A” array**

**A screenshot of a computer screen

Description automatically generatedFigure 5. The position of the beginning of “A” array**

**A close up of a computer screen

Description automatically generatedFigure 6. Cut the file into 2 parts**

**A computer screen with white text

Description automatically generatedFigure 3.7. Generate the prefix to create the 2 files needed**

**A screenshot of a computer code

Description automatically generated**

**Figure 8. hỏi**

**A screenshot of a computer

Description automatically generatedFigure 9. Check the MD5 values and see the difference in bit**

1. **Making the Two Programs Behave Differently (used Ubuntu 16.04)**

****

**Figure 1. Create a new C program**

**A screenshot of a computer screen

Description automatically generatedFigure 2. The body of our program**

**A screenshot of a computer code

Description automatically generatedFigure 3. Execute the code and see its result**

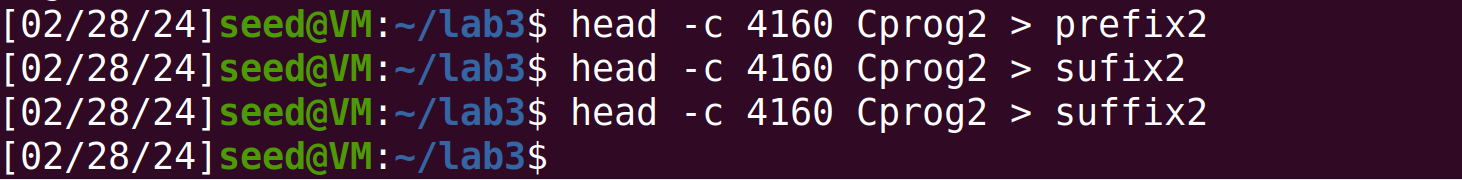
**A screenshot of a computer

Description automatically generatedFigure 4. Search for our “A” array in the binary view**

**A screenshot of a computer screen

Description automatically generated**

**Figure 5. The 2 positions of the beginning of two “A” arrays**

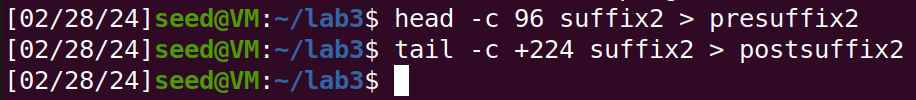
****

**Figure 6. Cut the file into different pieces**

**A screenshot of a computer

Description automatically generated**

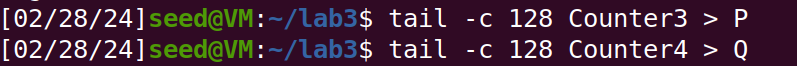
**Figure 7. Trace precisely the position of the second “A” array**

****

**Figure 8. Cut the file one more time into 2 suffix files**

**A screenshot of a computer

Description automatically generatedFigure 9. Generating the 2-prefix file for future “gluing” the pieces**

****

**Figure 10. Extract the 2 parts of a 128-byte long file into P and Q**

**A screenshot of a computer program

Description automatically generatedFigure 11. Connect the pieces and check the result of the 2 state codes**

**A computer screen with white text

Description automatically generated**

**A black background with white text

Description automatically generatedFigure 12. Final checking of MD5 value and comparison between the files**