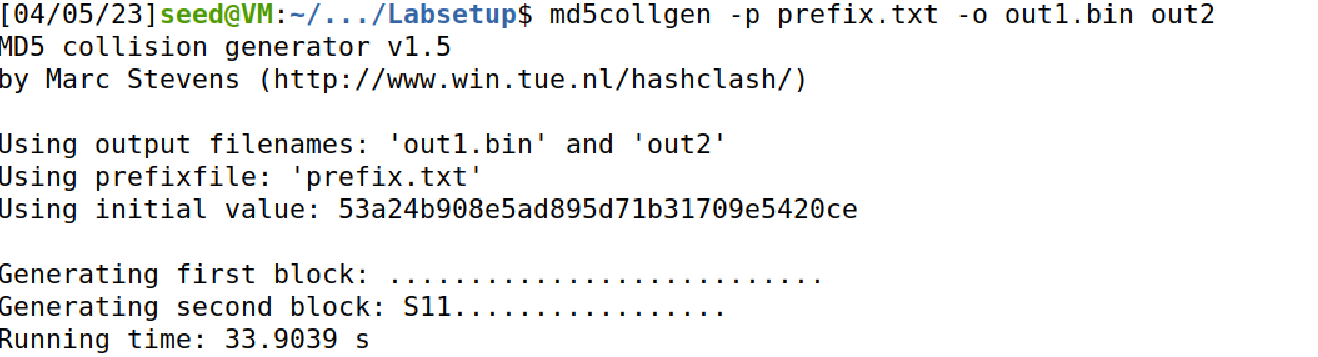
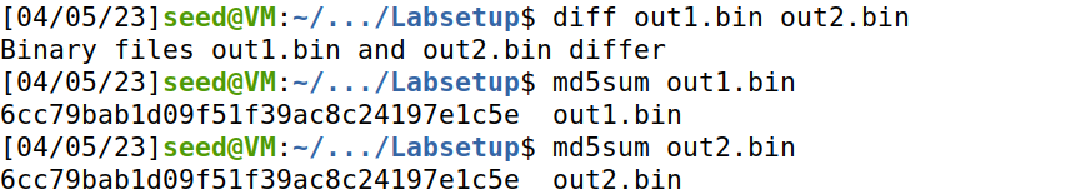
MD5 Collision Attack Lab:

Task 1: Generating Two Different Files with the Same MD5 Hash

Generating two different files with md5collgen:



Checking the weather two files are different or not using diff command and md5sum command to view the files:



Question 1. If the length of your prefix file is not multiple of 64, what is going to happen?

Ans: We will add padding to make the length of prefix to 64.

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

happens.

Ans: Screenshot:

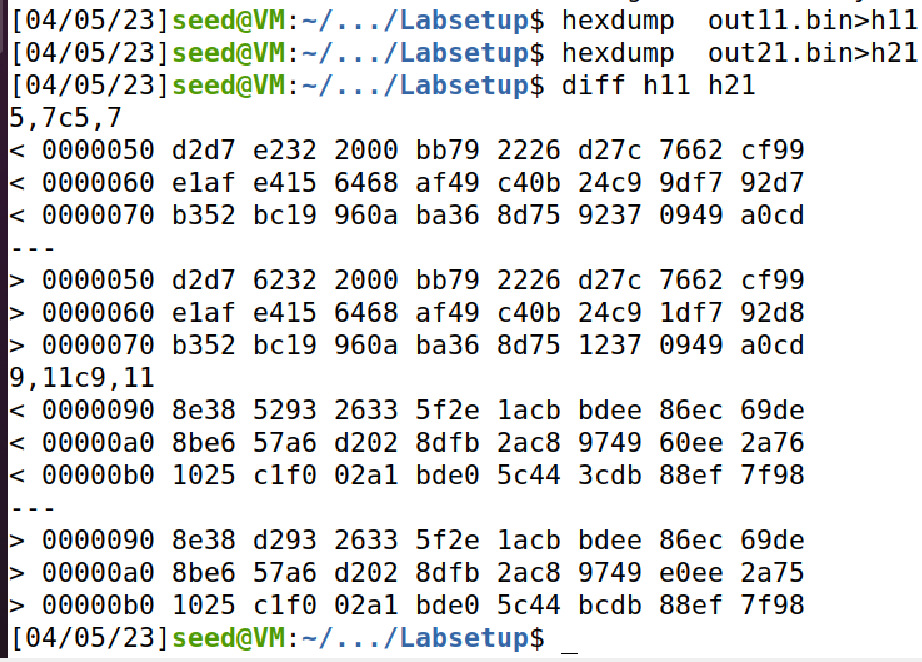
Text

Description automatically generated

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.

Ans: Screenshot



Task 2: Understanding MD5’s Property

Text

Description automatically generated

MD5 property is even though you concatenate two bin files from task and create a new files they will still be different from each other.

Task 3: Generating Two Executable Files with the Same MD5 Hash

Running c program:

Code:

#include <stdio.h>

unsigned char xyz[200] = {

"bbbbbbbbbbb"

};

int main()

{

int i;

for (i=0; i<200; i++){

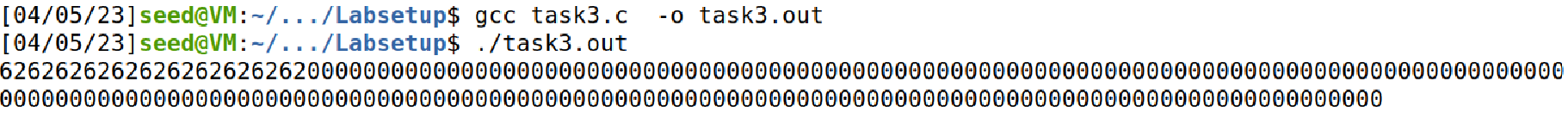
printf("%x", xyz[i]);

}

printf("\n");

}

Output screenshot:



Running head command:



Running tail command:



Running md5collgen command using above prefix file:

Text

Description automatically generated

Running md5sum commands on both output files:

Text

Description automatically generated

And they both are same.

Task 4:

Code:

#include <stdio.h>

#define LENGTH 400

unsigned char X[LENGTH]= {

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

};

unsigned char Y[LENGTH]= {

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

};

int main()

{

int i = 0;

for (i =0; i< LENGTH; i++){

if (X[i] != Y[i]) break;

}

if (i==LENGTH){

printf("%s\n", "Executing benign code... ");

}

else {

printf("%s\n", "Executing malicious code... ");

}

return 0;

}

Output of code:



After running c program checking the output files using bless:

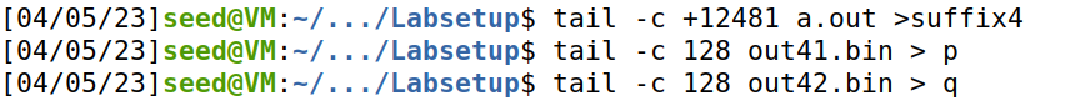
Table

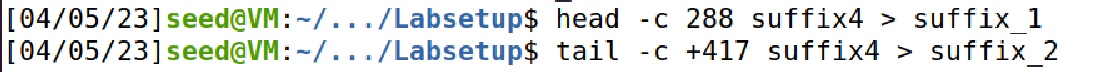
Description automatically generated

Running head, md5collgen and tail commands:

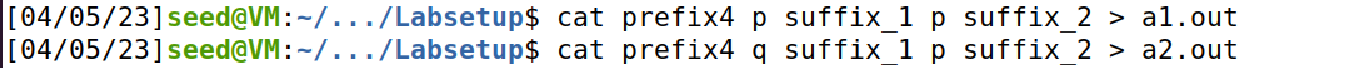
Graphical user interface, text

Description automatically generated

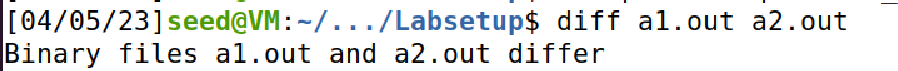




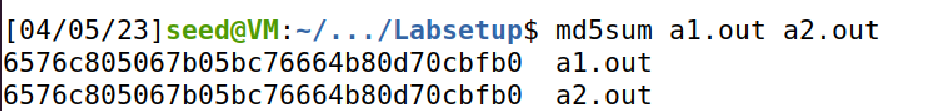
Concatenating prefix and suffix files:



Checking weather the a1 and a2 out files are different or same using differ command:



Running md5sum command on both out files:



Changing the permission for out files as feasible to us read them and running the out files:

Text

Description automatically generated