**Lab 8**

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

Table

Description automatically generated

Text

Description automatically generated

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

Ans. Padding shall be done with zeroes.

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

Ans. There is no zero-padding found. I ran ***md5collgen -p prefix.txt -o out1.bin out2.bin***and ***bless out1.bin*** & ***bless out2.bin***. Below, is the output for the same.

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. No, not all bits are different.

A picture containing text

Description automatically generated A picture containing text

Description automatically generated

**out1.bin out2.bin**

According to many trials, these differences are not continuous. Above is the difference between the bytes evidently.

**Task 2: Understanding MD5’s Property**

Ans. Hash created below,

**Text

Description automatically generated with medium confidence**

* Concatenation and append a random string to the end of both files and check their MD5 hashes once more. The MD5 hashes remain similar seen below.

**Text

Description automatically generated**

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

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

* ***md5collgen -p prefix -o a1 a2*** and running ***head -c 12300 a.out > prefix****.* We now have two files with identical MD5 hashes but distinct suffixes. In bless, look at both a1 and a2 (***bless a1 a2*** ). Now we'll use***tail -c 12600 a.out > commonend*** to get the common end to be appended. By running, you can put them together. Run both files after giving them executable permission hence, noting that the results aren't identical.

**A screenshot of a computer

Description automatically generated with low confidence**

**Task 4: Making the Two Programs Behave Differently**

**Text

Description automatically generated**