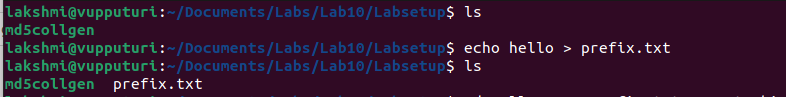
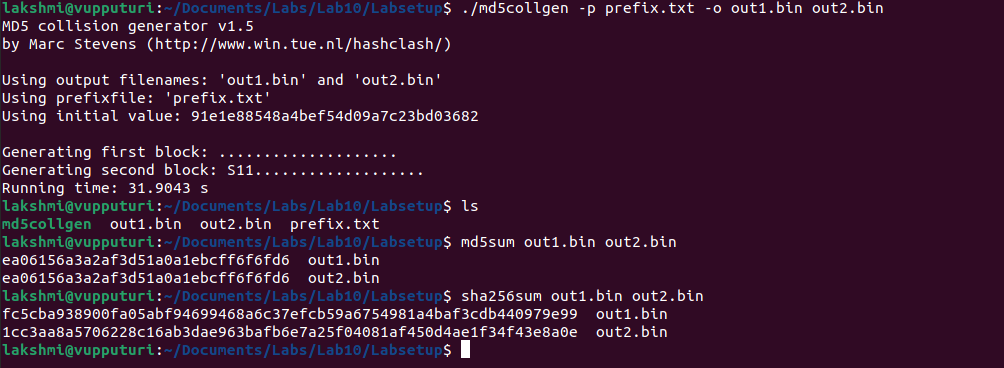
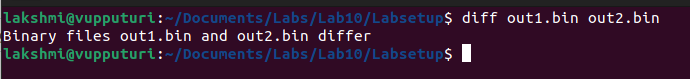
Lab 10



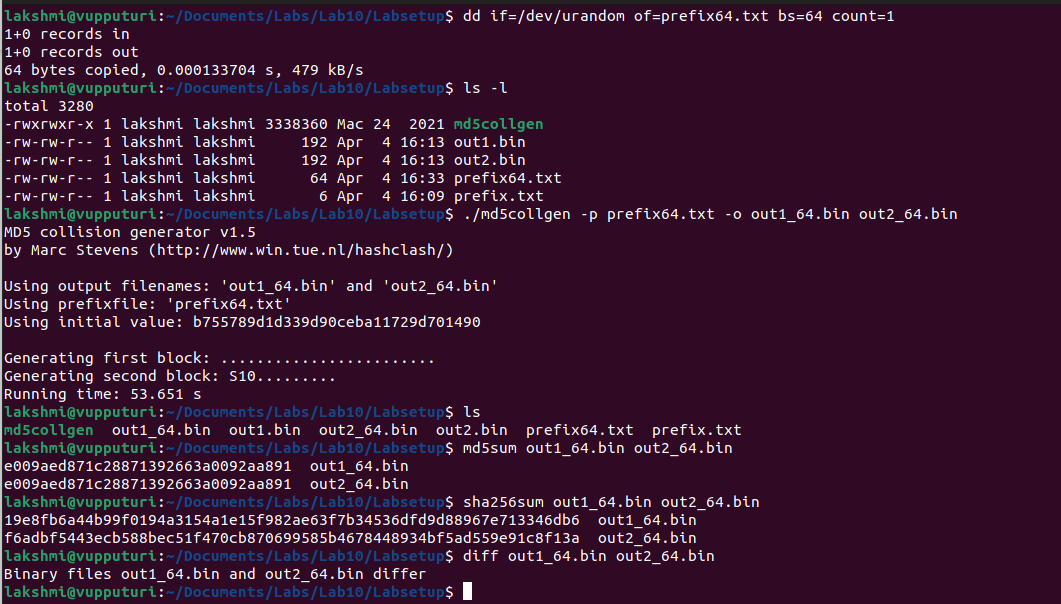


The hash generated by md5 algorithm is the same for both files out1.bin and out2.bin but different when using sha256 algorithm to generate the hash.



When opened in a text editor, the binary files differ in lines 6,7, 8, 11 and 12.

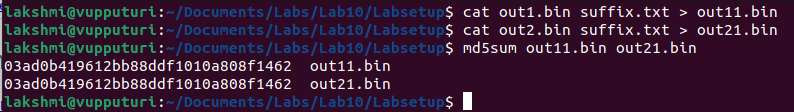
If the length of the prefix file is not a multiple of 64, zeros will be added to so as to make it a multiple of 64.



There is no padding for the output files when the file is exactly 64 bytes when using md5collegen. The hash generate md5 algorithm is the same for both files but different for the sha256 algorithm.



There are 6 different bytes between the files, bytes 84, 110, 124, 148, 174 and 188.



The md5 hash generated for both of the new files after appending the same data are the same.

When comparing the two algorithms, the md5 algorithm is faster than sha256 for hashing. This is because it generates hashes that are shorter. However, the sha256 algorithm is more secure even though it is slower than the md5 algorithm. This is because md5 generates a 128 bit hash while sha256 generates a 256 bit hash. The longer hash means that the sha256 algorithm has a lower probability of collisions compared with the md5 algorithm. The difference in speed and performance versus when compared with the security offered means that sha256 should be used for hashing whenever possible.