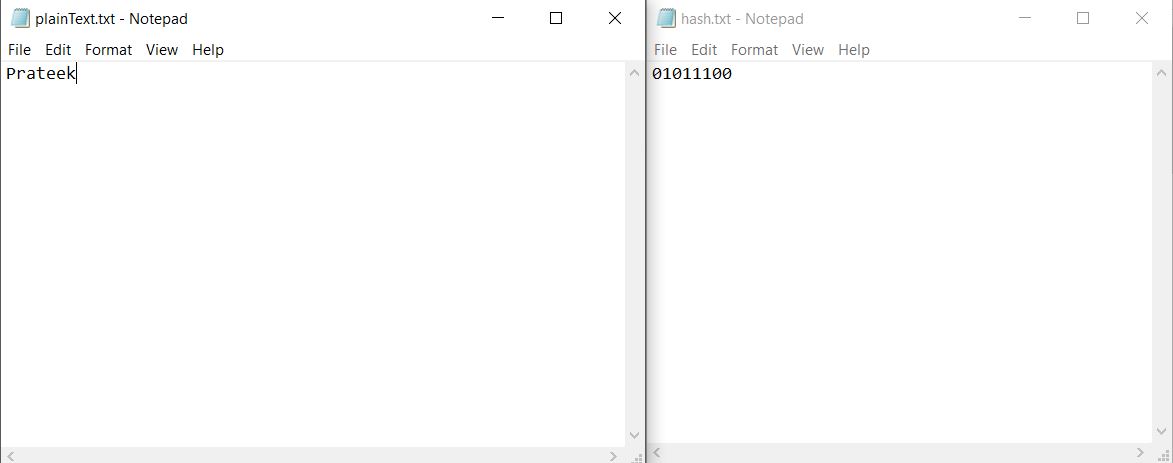
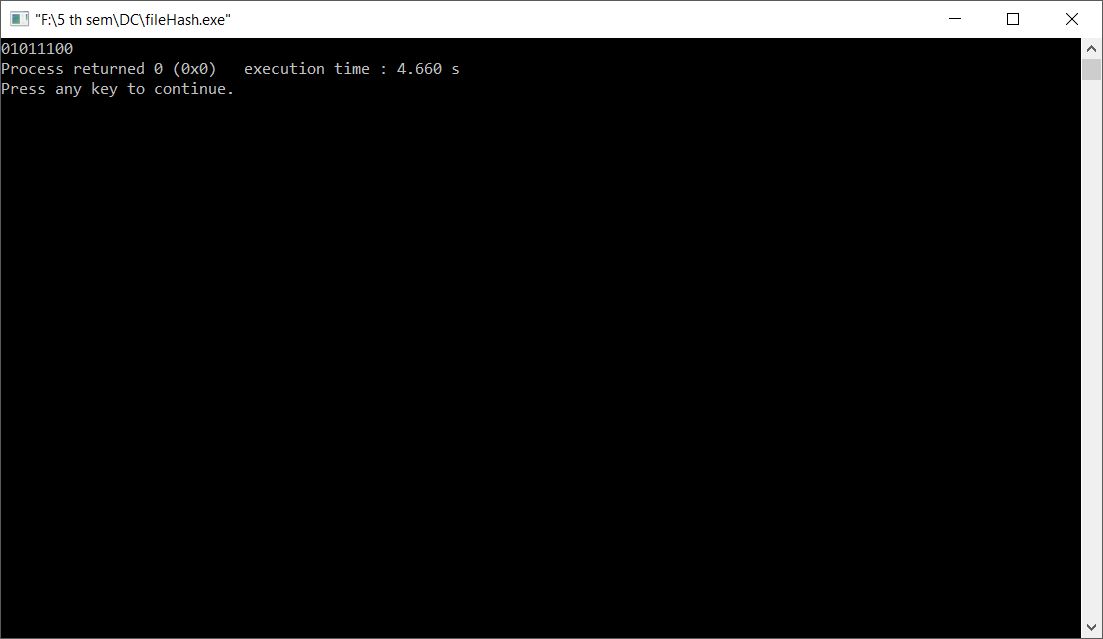
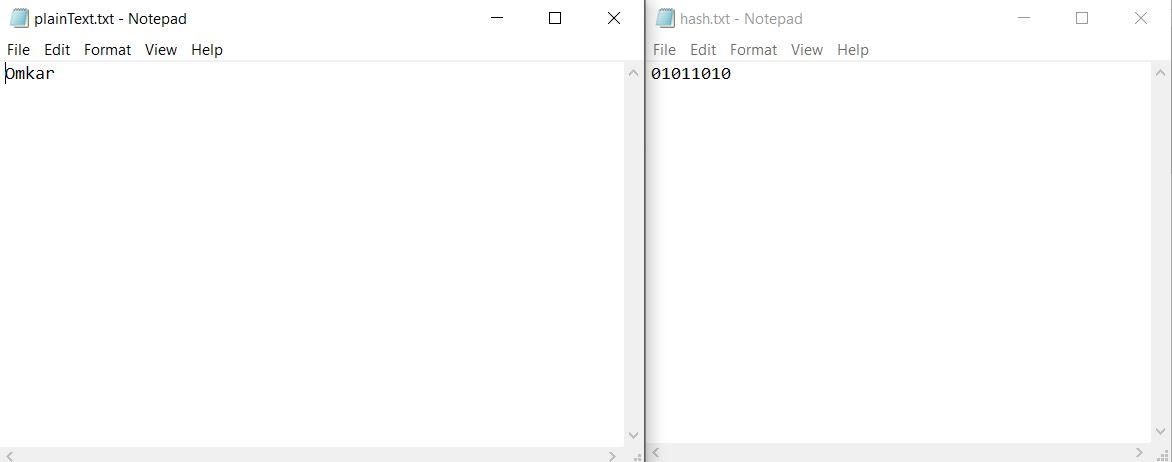
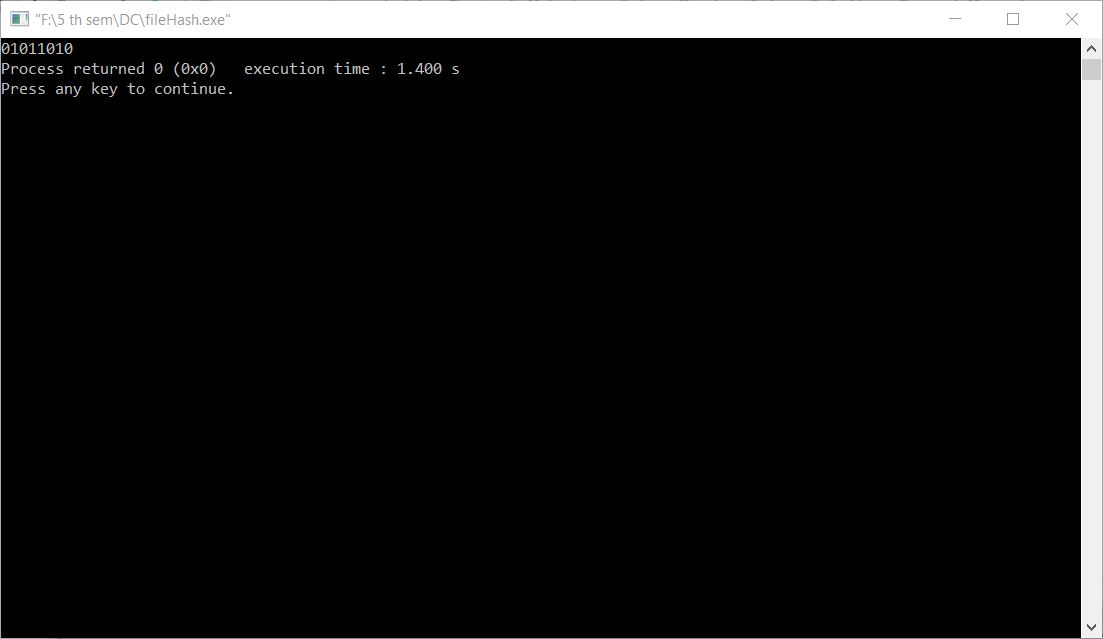
C/C++ Course Project

Title: Simple Hash using C

Objective: To implement simple hash using C

Sample Input Output:



Remarks/Limitations/Improvements

Limitations:

1. Since the hash is 8 bits hence there are only 1 out of 256 hashes possible for any input sequence which can lead to collision(2 distinct messages having the same hash).
2. The hash is simple and rigorous cryptanalysis can show trends that can be used to predict the message.

Improvements:

1. We could shift the rows towards right or left, depending the row number to add confusion.
2. We could increase the size of the hash to increase the range of the hash function making it more collision resistant.
3. We could use multiple rounds to increase the complexity