CIS 3362 Homework #5: Coding Intensive Group
Note: THIS IS AN INDIVIDUAL ASSIGNMENT!!!
Crack the Hash Function - Birthday Attack and More

Part A - Find any two unique messages that hash to the same value.

You will be given a hash function in the file hash.c that returns a 48 bit value in a long long. Your goal for this portion of the assignment will be to find two unique strings, s and t, such that f(s) and f(t) are equal.

Part B - Spoof a message!

You have found a message that is being sent to an opponent that uses the hash function from part A for validating the contents of the message. You'd like to pass along a *different* message that will pass the validation check by the recipient. Namely, determine a different string, s, than the message, msg, conveyed in the file hash.c such that f(s) = f(msg). Now, you can replace msg with s and the recipient will still validate the message, thinking it was the original message!!!

Part C - Spoof a message, intelligibly!

Repeat part B, but try to create a message s with f(s) = f(msg) such that s actually makes some intelligible sense!

Deliverables

Write code to automate your search and describe your strategy in a text/pdf document. In addition, attach your code. In the write up, if successful, provide an input string that yields the same hash value (for the given function) that your name does. Include a discussion section in your document that talks about the difficulties in your search and how you overcame them. If you don't find a matching string, carefully explain all the means you used to attempt to find out.

Note

Parts B and C are very challenging. Don't feel bad if you don't complete these parts.