CT255 Assignment 2

Breaking Hash Functions

Overview

The objectives of this assignment are as follows:

1. Reinforce your understanding of hash functions.
2. Implement and apply brute-force concepts to find hash collisions.

Please use a screen recorder to complete this assignment.

The Java class *CT255_HashFunction1* (please see Canvas attachment) is a simple hash function that translates a string (consisting of up to 64 characters) into a 32-bit (positive) integer. The hash code is by no means bullet proof, but nonetheless forms the basis of this assignment.

In detail, the class *CT255_HashFunction1* consists of a

- main() method that takes in a command line argument (i.e. the input value)
- hash function *hashF1()* that does all the donkey work.

Problem 1: [2 marks]
Study the code and explain its functionality using the screen recorder, thereby highlighting important source code lines.

Problem 2: [4 marks]
Consider the input "Bamb0" (i.e. "Bamb" followed by a zero). The resulting hash value is 1079524045.
Enhance the code to search for "Bamb0" hash collisions (i.e., different inputs that create the same hash value → weak collision resistance) via a brute-force search.
What collision(s) can you find? Again, explain your solution using the screen recorder.

Problem 3: [4 marks]
Enhance the code in *hashF1()* to make it more robust, i.e., to reduce the risk of hash collisions. Explain your solution using another screen recording.

Assignment Submission

Please submit a zipped folder to Blackboard containing:

- Your screen recordings for problem 1 – 3. Please make sure that you identify yourself (your name and student id).
- Your (well-commented!) source code for problems 2 and 3, all in PDF format.
- For problem 2 screenshots showing your program being compiled and producing results, i.e., a list of (up to 10) hash collisions you could identify.
- For problem 3 screenshots showing your program being compiled.

Marking Scheme

- For problem 1 full marks are awarded for a comprehensive summary of the hash code.
- For problems 2 and 3, half the marks are awarded for a comprehensive, well documented solution, while 50% of marks go towards your video presentation for a comprehensive summary of your solutions.