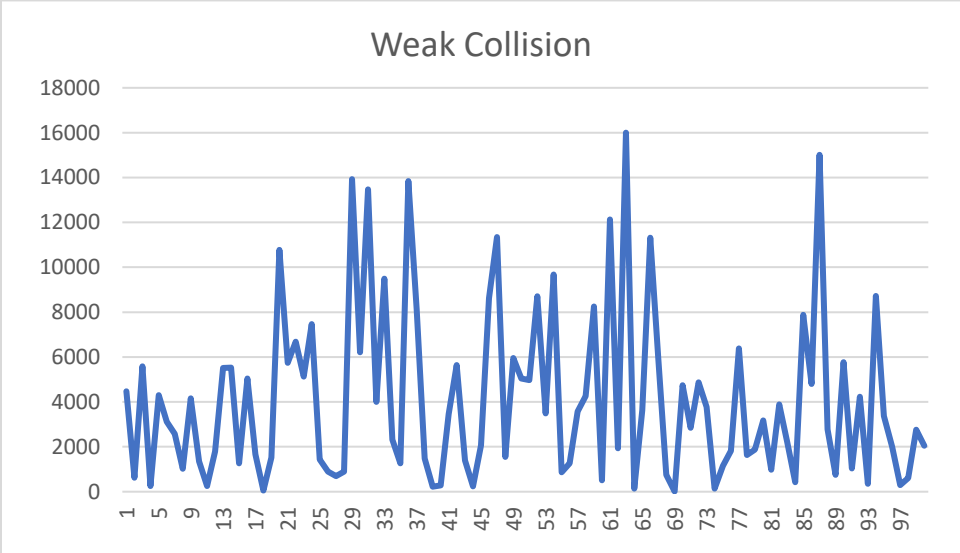
1. How many trials will it take you to break the weak collision resistance property using the brute-force method? You should repeat your experiment for multiple times (100 or more depending on how long each trial takes) and report your average number of trials.

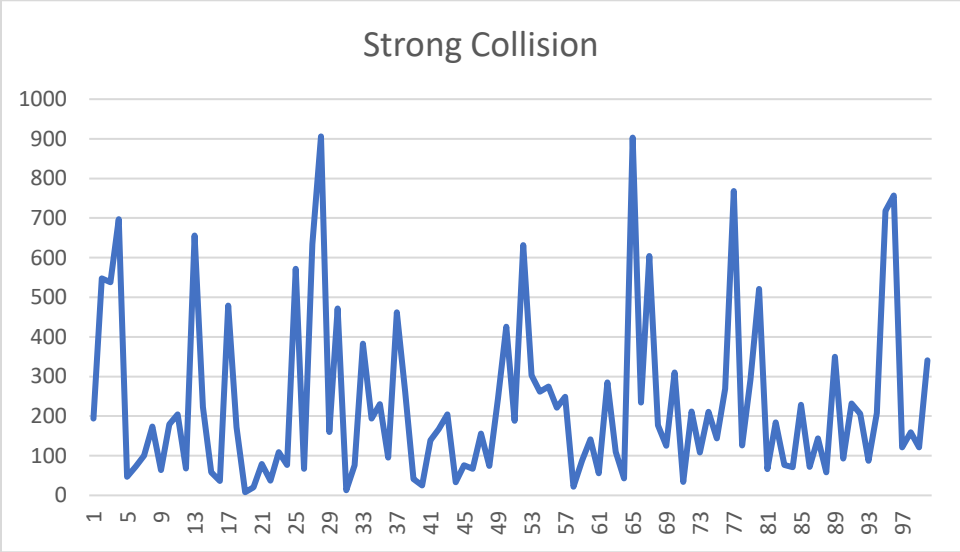
   Using the brute force method the strong collision resistance requires an average of 3259.5 trial to find a collision within a total of 100 multiple runs.



   Note: (Spreadsheet file can be referenced at Book1.xlsx)

2. How many trials will it take for you to break the strong collision-free property using the brute-force method? Similarly, you should report the average.

   Using the brute force method, the strong collision resistance requires an average of 267.5 trial to find a collision within a total of 100 multiple runs.



   Note: (Spreadsheet file can be referenced at Book1.xlsx)

3. Based on your observation, which property is easier to break using the brute-force method?

   Using the brute force method, the strong collision resistance property is easier to break comparing to the weak collision resistance property.

4. Can you explain the difference in your observations?

   The weak collision resistance has a higher average trial to get a collision compared to the strong collision resistance. This means that finding a hash collision is harder with the method of using a given input of x with hash value of h(x) that collides with another input y that produces the same hash value of h(x), as compared to using the birthday attack to find a hash collision. Hopefully, the diagram below can better explain my statement.

   given $x \rightarrow h(x)$
   keep finding $y \rightarrow h(y)$
   that fulfill $h(x) = h(y)$ and $x \; ! = y$

   Using the birthday attack, finding an input that creates hash collision with any other inputs is easier. The birthday attack gives us a 50% or higher probability odds to find a matching hash value. From my implementation perspective, the reason why strong collision resistance has a lower average trial for a collision is because there is a table that stores six of the recent two hash value, which significantly reduce the trial average by allowing us to find a collision with the use of birthday attack paradox. The weak collision resistance has a higher average trial because we have to keep looping to find a match of hash value with the given input, without the use of any table to store the previous hash value, which explain the reason why the weak collision resistance requires a much higher average trial.