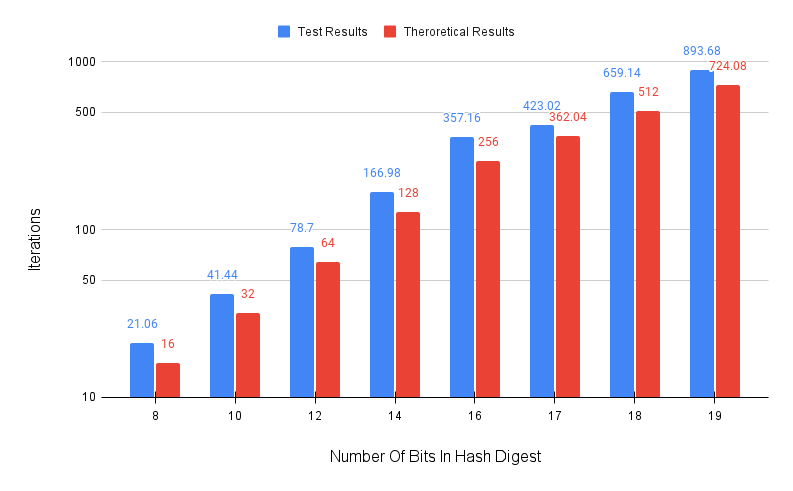
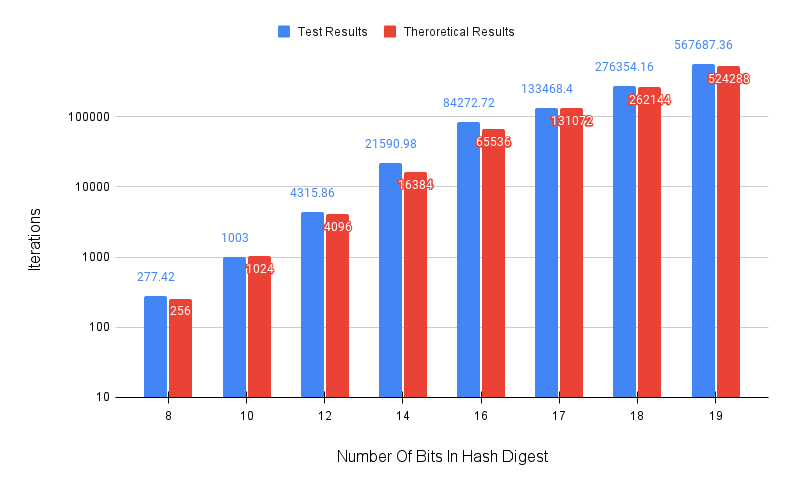
Noah Morris

Hash Attack Writeup

This lab is broken into two parts with the second part also being in halves. The first part was purely the implementation of the SHA-1 hashing algorithm. This part had no results because it was only to implement SHA-1 and did not have any testing associated with it, so we will move on to the second part. The second part was to implement two attacks on the SHA-1 algorithm: a collision attack and a pre-image attack. Both of these were run with 8 iterations of 50 executions of the attack. Each iteration had a different number of bits inputted, these were 8, 10, 12, 14, 16, 17, 18, and 19. To start analyzing the results we will look at the collision attack’s data which is displayed on the graph below. The experimental results are blue and are left of the theoretical results on each iteration, which are in red.

 The results of running the collision attack ended with an average attempt number of each iteration that was slightly larger to the theoretical number of attempts the attack should take for a collision to occur. While there could possibly be a reason that each iteration ended with a relatively small increase from the theoretical value, it is fair to believe that this small difference is within reason and in fact reinforces the time complexity of 2^(n/2). In short, the experimental results are very comparable and align with the theoretical difficulty of running this attack at the 8 bit sizes used.

Continuing the examination of gathered results, the graph below displays the information gained using 8 iterations of the pre-image attack at the same number of bits used for the collision attack. Again, the experimental results are blue and are left of the theoretical results on each iteration, which are in red.

 The results from running the pre-image attack were very close in relative distance to the number given by the theoretical results. In iteration two with ten bits being inputted we even saw an example of the results being slightly lower than the theoretical value which is something that was not present in the data for collision attacks. The experimental results here very much align with the number given by the theoretical difficulty of running this attack and along with that reinforces the theoretical time complexity of 2^n.

Both attacks led to similar results when compared to the theoretical difficulty of performing each attack. It is fair to say that these attacks were successful and demonstrate a real example of these attacks being implemented.

External review givenby: Stephen Cho