Author: Jason Gillett

Reviewer: Shane Gillett

Lab 2 Project Report: Hash Attack

Overview:

This report will go over the basics of Collision and Pre-image attacks. It will then explain the setup for the experiment and explain the data outputted by the data

Hash function

The hash function takes in any sized string and outputs a fixed-length output that should not be reversible

Collision Attack

This attack creates many different hashes for random string values.
Each time a new hash is create with a new message; it checks previously created hashes to see if that hash had been created before.
If the hash value is not new but the message is, then you have a collision. Where Hash(m1) = Hash(m2)

Pre-Image Attack

This gets a specific message (m1) and hashes it.
It then creates a bunch of new hashes using random string values to find a message that will have the same hash value as the original m1 hash.
Where the collision attack looks for any collision, the pre-image attack only looks for collisions with a specific hash.

Experiment Explanation

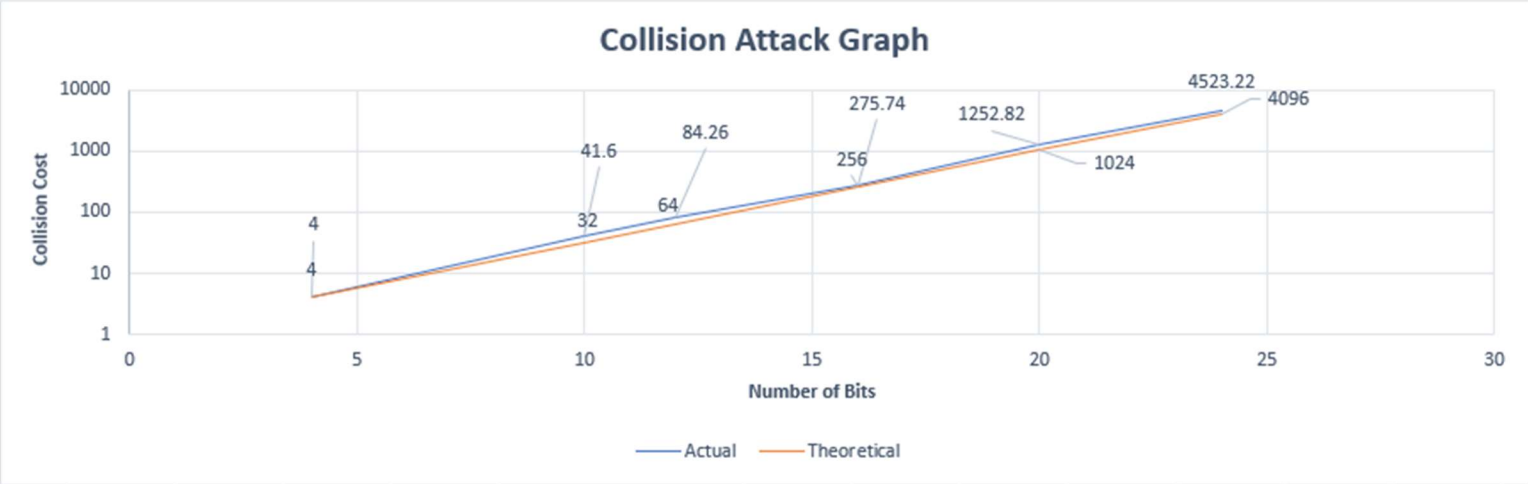
This Hash Attack experiment is mean to show the effect that the hash bit size has on the likelihood of a collision with a pre-mage or collision attack.
The size of the hash is truncated to a specified bit size, n.
So a hash of “Hello World” with size 10 will create a Sha-1 hash of “Hello World” and then truncate the hash to be of bit size n.

Truncating the size of the Hash allows for the effectiveness of collision prevention to be easily seen as the size of the hash increases to its normal size.

The data for this experiment was obtained by running 50 collision and pre-image attacks for each of the following bit sizes: 2,10,12,16,20,24 and then getting the average number of iterations required to find a collision.

Data

Collision Attack



Bit size	Average attempt count	Theory
4	4	4
10	41.6	32
12	84.26	64
16	275.74	256
20	1252.82	1024
24	4523.22	4096

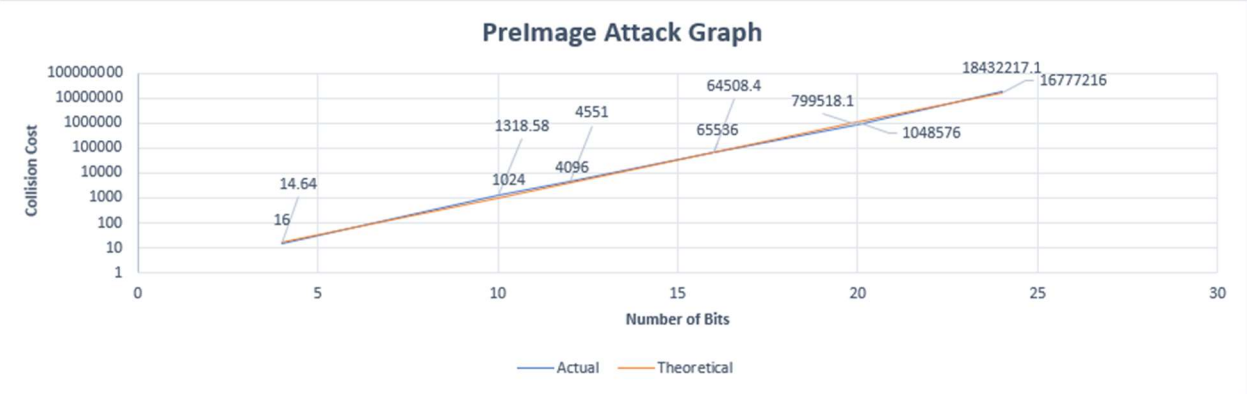
Explanation and Analysis

This graph logarithmically shows the actual experiment data verses the theoretical values for each bit size.

In general, the theoretical and actual values are very similar with a slight tendency for the actual values to be slightly higher than the theoretical values. This is expected with the random nature of the random string generator and hash collisions.

This data clearly shows that with a full sized hash, any collision between hashes would be computationally infeasible

Pre-Image Attack



Bit size	Average attempt count	Theory
4	14.64	16
10	1318.58	1024
12	4551	4096
16	64508.4	65536
20	799518.1	1048576
24	18432217.1	16777216

Explanation and Analysis

This graph logarithmically shows the actual experiment data verses the theoretical values for each bit size.

Here the average cost is also about the same as the theoretical. There are a few inconsistencies where the actual count was either more or less than the theoretical value. This makes sense, a single round where the hash was randomly found very quickly will lower the average in a noticeable amount with only 50 rounds.

This data very clearly shows how hard it is to find a collision for a specific message hash. For a full sized has, it would be computationally infeasible to find a collision for a specific message with a pre-image hash attack