A Comparison of Hashing Algorithms

Matt Anderson

Password Possibilities

Say that you're calculating hashes and storing them into a rainbow table for later use. The possible permutations of any character set can be represented as such:

$$\sum_{i=1}^{Max\ Length} Character\ Set\ Length^{i}$$

Now, assuming that you were making a table with all possible permutations with a character set that included: uppercase characters, lowercase characters, and numbers, for all passwords with a length up to 8 characters, using the above summation would give you this:

$$\sum_{i=1}^{8}(26+26+10)^{i} = 221{,}919{,}451{,}578{,}090 = 2.2191945157809 * 10^{14}$$

First off, that's a lot of fucking permutations for an 8 character password that can contain uppercase characters, lowercase characters and numbers.

Calculating Hash-Time

By using PHP as a medium to measure the time it takes to calculate one hash, I ran 10,000 iterations of hashing of MD5 and Blowfish for a comparison.

MD5 was capable of computing 10,000 hashes in .0052201747894287 seconds which means it takes it on average 0.00000052201747894287 seconds to calculate one hash. Blowfish on the other hand, took 108.68253946304 seconds to calculate 10,000 hashes. This means that on average, it takes it 0.010868253946304 seconds per hash.

Using the rates of hashing, you can calculate how much faster MD5 is than using Blowfish.

$$\frac{0.010868253946304}{0.00000052201747894287} = 20{,}819.71271979846902345$$

That's right, using MD5 is 21 thousand times faster than using Blowfish.

Generating Rainbow Tables

Using the numbers we calculated previously with permutations of any given character set and password length, assuming you were going to make a hash table with these values, let's calculate how long it would take to generate that table.

Assuming that you use the hash time as a conversion rate on the number of permutation, it looks like so:

$$\frac{221{,}919{,}451{,}578{,}090\ Hashes}{} * \frac{0.00000052201747894287\ \ Seconds}{1\ Hash} = \ 1.1584583264118 * \ 10^{8}$$

That's 115845832.64118 seconds or 1930763.877353 minutes or 32179.397955883 hours or 1340.8082481618 days or 3.6734472552378 years.

That's right, at this rate; it would take you a little more than three and a half years to calculate a rainbow table with all of the possible permutations of 8 characters with a character set of 62.

Blowfish can be calculated using the same way replacing the MD5 conversion factor with the Blowfish's.

$$\frac{221{,}919{,}451{,}578{,}090\ Hashes}{} * \frac{0.010868253946304\ Seconds}{1\ Hash} = \ 2.4118769553752 * \ 10^{12}$$

Given that conversion, that's *2411876955375.2* ***seconds*** *or 40197949256.253* ***minutes*** *or 669965820.93755* ***hours*** *or 27915242.539065* ***days*** *or 76480.116545384* ***years*** *or 7648.0116545384* ***decades*** *or 764.80116545384* ***centuries*** *or 76.480116545384* ***millennia****.*

I bid you good luck assuming that you're going to try to brute force Blowfish it won't work, don't try.