Michael Rivnak

COMP3590-01

Prof. Raymond Hansen

29 June 2019

**Evaluating Hash Algorithms**

Each of the provided hash algorithms was tested automatically using a script which also recorded the runtime of the hashes. Regarding the runtime, there does not appear to be a correlation with the size of the output hash and the time required to calculate it. For example, with SHA hashes, the larger sizes tended to run faster for this input file than the smaller hashes, whereas with SHA3 this opposite was true. Further, I also include a graph of run time per bit for each or the hashes to demonstrate how a hash like ripemd-160 is particularly time consuming to calculate while only providing 160 bits of complexity. In comparison the SHA hashes as well as BLAKE2b512 seem to be particularly adept at producing large hashes quite quickly. Each hash was calculated 8000 times to avoid any outliers, and each 1000 trials were run separately in case there was anything else running on my computer that may bottleneck it. In addition to run time checking, this script also verifys that the output hashes are all identical and displays that to the terminal. Through 8 trials of 1000 passes of 14 hashes I did not observe any errors in the hash calculations