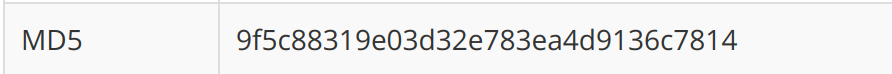
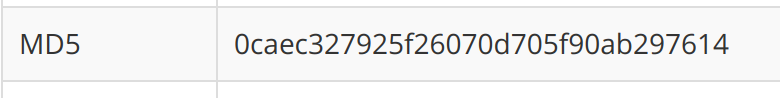
**Assignment on Hashing**

**Tasks to be performed**

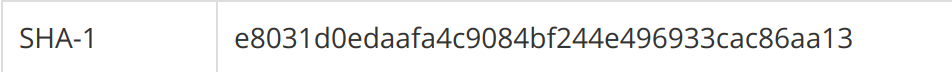
1. Check MD5 box and click calculate.
   1. The output is human readable but meaningless, I may not be able to read the original file. According to techtarget.com, Hashing is defined as a transformation of a string of characters into a usually shorter fixed length value or key that represents the original text. Hashing can also be defined as the practice of using an algorithm to map data of any size to a fixed length.
   2. Output
      1. Output 1



* + 1. Output 2

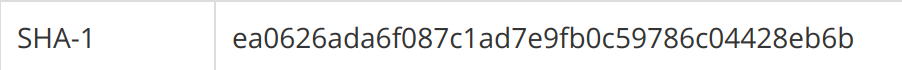


The two files look very different. At the end of the line, I added G. Now the two MD5 codes look very different.

1. Check also the SHA1 box and click calculate (MD5 should remain checked as well).
   1. 

Values generated by SHA-1 are a bit longer compared to the MD5 hashing.

* 1. Based on the hashing methods, the length varies, on MD5 the length can have 128 bits while on SHA1 it can have 160 bits length.

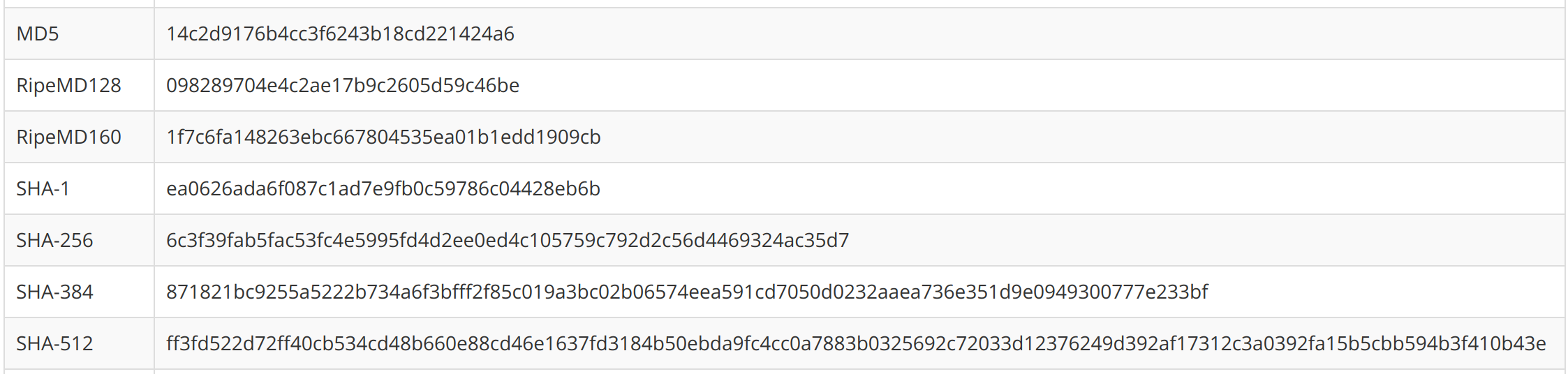
1. Modify the content of the file and keep a single word (the file should now contain only one word), upload the file again; keep MD4, MD5, SHA1 and SHA256 boxes checked.
   1. 

It’s not an error that they are having the same length of bits. That’s the whole concept of hashing, it is decoding characters no matter the length. Even if it was one word, hashing will transform it into mixed characters. In this case SHA1 no matter the length of the original text, it will be 160 bits of length.

* 1. Based on the small research conducted, MD5 is the least powerful hashing method. Because it is very slow and it provides indigent or poor security. In MD5, if the assailant needs to seek out the 2 messages having identical message digest then the assailant would need to perform 2^64 operations which is the least compared to the rest.

SHA256 is considered to be the most secure among the others stated above where a brute-force attack would need to make 2256 attempts to generate the initial data which is super super hard.

1. Considering the family of SHA functions where we have SHA1, SHA256, SHA384, and SHA512.
   1. SHA1: SHA-1 was designed by the United States National Security Agency (NSA). The Secure Hash Algorithm takes a message of less than 264 bits in length and produces a 160-bit message digest which is designed so that it should be computationally expensive to find a text which matches a given hash
   2. SHA2: It is an advanced hashing method where it contains many different-size hashes, including 224-, 256-, 384-, and 512-bit digests and rounds are between 60 and 80.
   3. MD5 is no longer secure because of the following reasons
      1. Hackers now use brute force attacks that are more advanced and unhashing these types of codes became easier
      2. Collisions: MD5 has shown collisions while generating two different words sometimes they provide the same hash.
   4. SHA2 which contains SHA256, SHA384 and SHA512 are the most secure. To be so sure, I’d go with SHA512 where the combination would be 2512 .



1. Hash function application
   1. We need hashing because:
      1. It digests the original characters to a more complex set of characters.
      2. It is used in verifying passwords.
      3. It is used in data structures
      4. It makes certain type of texts secured and unknown
   2. Even if encryption has been done which is ciphering and protecting data in transit, we still need the hashing method which is in charge of checking authenticity and checking if data has not been altered.

Reference

* <https://blog.pagefreezer.com/sha-256-benefits-evidence-authentication>
* <https://www.solarwindsmsp.com/blog/sha-256-encryption#:~:text=SHA%2D256%20is%20used%20in,SHA%2D256%20for%20verifying%20transactions>.
* <https://www.w3.org/PICS/DSig/SHA1_1_0.html>
* <https://www.thesslstore.com/blog/difference-encryption-hashing-salting/>