

Cryptographic hashes are a unique and useful tool in our crypto toolbag. Take a moment and google to find out what exactly a cryptographic hash is. After researching hashes, work to answer the questions below and perform the hash functions as directed. In this set of exercises, you will use any online hash calculator, (for example: <https://www.fileformat.info/tool/hash.htm>). Answer the following questions and then complete the required activities. Submit your answers through Moodle in an appropriately named file.

QUESTIONS

Compute the hashes as requested. Use the assignment sheet (PDF) from Moodle for this assignment as your input. If you do not use the appropriate input file, your submissions will be wrong. When text is required to be input into the application, use all lower case letters.

1. Using the Assignment 6 PDF (this file from Moodle) as the input, compute the following hashes: a. MD5, MD4, SHA1, SHA256, SHA384, SHA512, RIPEMD160, CRC32

2. Create a hash with your full name (first last) as the input data and “cs503” as the key using MD5, SHA1, and SHA512

(link for 2nd question <https://www.freeformatter.com/hmac-generator.html>)

3. Which hash function algorithm is used on the certificate for the following sites: learning.semo.edu