

SHA 512:

To implement sha512 hashing I first pulled the code from the lecture 15 download. Then I went through that implementation and modified the size of the vectors / permutations because the overall algorithm is the same. I doubled the size of the hex strings and the K constants as specified in section 15.7.2 of the lecture notes. I changed the padding to be mod 1024 and made some other small changes to scale the size correctly. 64 words to 80 words. Changed range of for loop iterating over the words to go 16, 80. Changed the shifts in that loop to what are reflected on page 44 in lecture notes. Changed shifts in the round function loop to what is reflected on page 46. Then I wrote hash_hex_string to the output file rather than returning it.