Homework Number: 7

Name: Dylan Huynh

ECN login: huynh38

Due Date: 3/9/2023

This code closely follows the lecture code for SHA256 located in SHA256.py. Firstly, it takes the input and output file and reads them into streams, and creates a bitvector from the string. The h and K values are the squares and cube roots of the first 8 and 80 primes, respectively, as 64 bits. Both of those are precomputed and placed into bitvectors. The message string is then checked for how much padding it needs, taking into consideration the extra 128 bits allocated to the length of the string. The bitvector is first padded with a 1, then 0's until the last 128 can be filled by the length bits. Then, it loops continually through the blocks of 1024 bits, by first generating a message schedule. In the message schedule the first 16 are made of the 1024 bit block split into 16, and the words after that are made by taking the words in the indexes, -16, -15, -7, and -2 in comparison to the current index. The -15 and -2 word is put through a sigma function where it has 3 values XORed together that are right shifted, where -15 is circular shifted 1 and another at 8, and a padded shift by 7; -2 is circularly shifted 61 and 19, and padded shifted by 6. Now that the message schedule has been created, it is used in the 80 round process. For the round functions, 8 registers, a-h, are held where all of the letters are shifted up but d and h are specially processed for the e and h registers. I don't think I need to get into the details of how each variable was calculated, but I will mention that I changed the shifts according to what is necessary for SHA-512 as opposed to SHA-256. Then the registers from the output of this round become the output of the next round, until the blocks have all been iterated through. Finally it puts all the registers together and writes it to a file.

Input: The phony war is over and it will soon be time to discover who's hot and who's not on the 2023 Formula 1 grid. Red Bull ended last season in dominant shape, winning all bar one of the grand prix in the second half of the 22-round championship. Because of that - and their 2021 budget cap breach - they have less time to spend on developing their RB19. Will that allow Ferrari and Mercedes to reduce their advantage?

Output:
5b11ec306b005aa885c0fb9c7c286caf9e261538495944b9550d8698aeea61f552ad85c564210088bd3f25669c89da2fdd79ee8024f1eb8d1c0bffe948637191