HW07: SHA
Homework Number: 07
Name: Jack Gardner
ECN Login: gardne97
Due Date: 3/9/23

Sha Explanation: The implementation of SHA512 is very similar to the SHA256 implementation provided in the lecture notes. The first step of SHA is to pad the message so that is is a multiple of 1024 bits. Additionally, the last 128 bits must be the length of the number. Next, the message schedule is generated. The message schedule has 80 words, 16 of which are built from the message block. Next, round based processing is applied to each message block. We store the hash values for the previous block in temporary variables. We then permute these values and mix in the word schedule and the k constant. Next, we update the hash values calculated for the previous block by adding it to the temporary variables.

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?

Recovered output:
5b11ec306b005aa885c0fb9c7c286caf9e261538495944b9550d8698aeea61f552ad85c564210088bd3f25669c89da2fdd79ee8024f1eb8d1c0bffe948637191