Ethan James
33378430
Epjames

HW07

****Code Adapted from AVI KAK sha256

Let me walk you through step by step on my code. The first thing I do is create a class for SHA 512. I then read my input file so that I can create my preliminary steps. I also set the initialization vectors to variables given the values to us from lecture. They are the initial hash values. I also then get my round constants from the government website and convert them to a BitVector to be used for hashing later on in the algorithm. I also pad the input message by a appending a1 bit. I also calculate the number of 0 bits needed for padding to make sure the message length is a multiple of 1024 bits. I also then add the 0 bits to the padded message finish the padding. Then I convert the length of the message into a 128-bit integer. It will add added security.

Next we initialize the array of words for storing the message schedule with 80 words. We get the first 16 words and store them. Then we compute the remaining 64 words based on the formula outlined in the lecture notes.

I then create variables to store the initial hash values since we will have to update these variables at a later time. In this step we carry out the round based processing which consists of 80 rounds. The round function for the i-th round consists of permuting the previously calculated contents of the hash buffer registers as stored in the temporary variables a,b,c,d,e,f,g and replacing the values of two of these variables with values that depend of the i-th word in the message schedule, words[i], and i-th round constant, K[i].

Finally, In the last round, the temporary variables after 80 rounds of processing are now mixed with the contents of the hash buffer calculated in step 3. Then finally I concatenate the contents of the hash buffer to obtain the Bitvector object. I then output it to the file as a hex string.

INPUT: Boku no Kokoro no Yabai Yatsu is the greatest romance, slice of life manga I've ever read. It is a series of constant progress that respects the reader's time and trusts them to read between the lines - Characters make mistakes and learn from them. Misunderstandings are never used to pad out the story, and never feel cheap. Progress is never undone. It is one of the most fully realized depictions of the liminal space between two young people as they begin to fall in love - The roller coaster between bubbly feelings and crippling cringe that is first love is so difficult to portray. I've never encountered another manga that has managed to capture this specific feeling so accurately and with so much detail.

Output:
84f353348a552229554fba7ba822005edcb6bca2fac8cf1735d53ae9e2915aa2e625f6d3cfa0106c87
07ff0004d3ce95281b47b851b380ef91c86d2fb0e58b28