Anish Laddha
Professor Avinash Kak
ECE404
February 19 2024

Homework 7

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:
84f353348a552229554fba7ba822005edcb6bca2fac8cf1735d53ae9e2915aa2e625f6d3cfa0106c8707ff0004d3ce95281b47b
851b380ef91c86d2fb0e58b28

Explanation:
First, we initialize the cipher class with the input class, and then load it into a BitVector. Then, we pass the bit vector with a single 1 and a bunch of 0s such that there are 128 bits left from making it divisible by 1024. Note that we will add another 1024 bits if necessary, as having the last 128 bits is very important. Then, in the last 128 bits, we store the length of the original bitvector.

After padding, we iterate through each 1024 sized chunk of the padded bv. For each block, we first generate a message schedule of 80 64-bit words. We do this by dividing the 1024 bit block into 167 chunks to form the first 16 words. Then, the next 64 chucks are created iteratively using shifts and rotations of the previous ones.

With the message schedule, we first initialize an array of 8 64 bit temporary registers, and fill them with the default values. We then iterate through 80 times, for each key/word, and then using various transformations, shifts, and swaps, we alter the temporary registers. Finally, we add those registers to the “default” values, which will be the initial values for the next block.

At the end, these registers will be the 8*64 = 512 bit output.