ECE 40400: Introduction to Computer Security

Spring 2024

Prateek Yashwant Jannu

Purdue University, West Lafayette

Professor: Dr. Avinash C Kak

Problem 1

Input Text

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 Text

84f353348a552229554fba7ba822005edcb6bca2fac8cf1735d53ae9e2915aa2e625f6d3cfa0106c8707ff00
04d3ce95281b47b851b380ef91c86d2fb0e58b28

Code Explanation:

1. The sha512 function takes two parameters: input (the file to be hashed) and output (the file where the hashed result will be stored).

3. It reads the input file and stores its contents in a variable text, then closes the file.

4. The input text is converted to a BitVector for processing.

5. Padding is applied to the input text to ensure its length is a multiple of 1024 bits, as required by the SHA-512 algorithm.

6. The SHA-512 constants (K_given) and initial hash values (prime_1 to prime_8) are initialized.

7. The input text is processed in chunks of 1024 bits.

8. Within each chunk, the 1024 bits are further divided into 64-bit blocks.

9. The main SHA-512 algorithm loop is executed for each block:

a. The block is expanded into an 80-word array.

b. A series of logical and arithmetic operations are performed on the hash values (prime_1 to prime_8) and the words in the array.

c. The hash values are updated based on the results of the operations.

10. After processing all blocks, the final hash value is obtained by concatenating prime_1 to prime_8.

11. The final hash value is written to the output file in hexadecimal format.

12. The script can be run from the command line, taking two arguments: the input file and the output file.