

hw07\_Panchagnula\_Raghava

# Homework Number: HW07

# Name: Raghava Vivekananda Panchagnula

# ECN Login: rpanchag

# Due Date: 3/05/2024

Code uses functions given in lecture notes, abiding instructions given in HW document.

```
diff hashed.txt test.txt
(.venv) vivek@vivek-desktop:~/Files/coursework/ECE-40400/Homework/HW07$ make
python3 sha512.py input.txt hashed.txt
diff hashed.txt test.txt
(.venv) vivek@vivek-desktop:~/Files/coursework/ECE-40400/Homework/HW07$
```

Commands to run all required code. Test.txt and hashed.txt is as follows:

```
84f353348a552229554fba7ba822005edcb6bca2fac8cf1735d53ae9e2915aa2e625f6d3cfa0106c8707ff00
04d3ce95281b47b851b380ef91c86d2fb0e58b28
```

Input.txt is:

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.

This just tells me that the code should run as expected

```
diff hashed.txt test.txt
(.venv) vivek@vivek-desktop:~/Files/coursework/ECE-40400/Homework/HW07$ make submit
zip -r hw07_Panchagnula_Raghava.zip hw07_Panchagnula_Raghava.pdf sha512.py
updating: sha512.py (deflated 60%)
adding: hw07_Panchagnula_Raghava.pdf (deflated 9%)
(.venv) vivek@vivek-desktop:~/Files/coursework/ECE-40400/Homework/HW07$
```

Commands to create the output (ignore zip warning as PDF wasn't created for this example.)

sha512.py

- Preamble:
  - Define  $h_n$  values and  $K$  and  $K_{bv}$

- Summary of sha512 function:
  - Message Padding:
    - Reads the message from the input file and creates message\_bv.
    - Determines the number of zeros to append for padding, considering the addition of a '1' bit.
    - Creates a padded message by appending '1' followed by the calculated number of zeros and the original message length.
  - Message Block Processing:
    - Iterates over the message blocks of 1024 bits.
    - Breaks each block into 80 64-bit words (words).
    - Applies specific operations to generate the next 64 words based on the previous words.
  - SHA-512 Word Calculation:
    - Computes new words based on the equations from Avi Kak's lecture notes.
  - Hash Value Update:
    - Updates the hash values (h0 to h7) using the calculated words.
    - Iterates over multiple blocks, updating the hash values iteratively.
  - Concatenation and Output:
    - Concatenates the final hash values.
    - Writes the resulting SHA-512 hash to the output file.
    - Closes both the input and output files.
- main
  - I called sha512 with input file and output file as the params