ECE 404 Homework #7

Due: Thursday 03/09/2023 at 5:59 PM

SHA-512

To better understand the Secure Hash Algoritm (SHA), use the BitVector module to create an implementation of SHA-512.

Program Requirements

Your program should have the following call syntax :

```
sha512.py <name of input file to hash (input.txt)> <name of output file containing
    hash (output.txt)>
```

An explanation of this syntax is as follows:

- Read the text (in ASCII format) from the input file specified by the first command-line argument. Do not strip or remove any characters (e.g. newlines) when reading the input file.
- The hash is written in *hexstring format* to the file specified by the second argument.

You can include the round constants K_i in the program file.

You can check the correctness of your work by comparing the hash values produced by your code with those produced by Python's hashlib library: https://docs.python.org/3/library/hashlib.html

Submission Instructions

- Make sure that the program requirements and submission instructions are followed. **Failure to follow these instructions may result in loss of points!**.
- You must turn in a single zip file on Brightspace with the following naming convention: HW07_<last name>_<first name>.zip . Your submission must include:
  - A PDF titled `hw07_<last_name>_<first_name>.pdf` containing:
    - a brief explanation of your code. The input and the output of the sha12.py.
  - The file `sha512.py` containing your code for your SHA-512 implementation.
- In your program file, include a header as described on the ECE 404 Homework Page.
- Please comment your code.