ECE 404 Homework #8

Due: Tuesday 03/22/2022 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> <name of file containing hash (output)>
```

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 to follow program requirements specified above. **Failure to follow these instructions may result in loss of points!**.
- For this homework you will be submitting 1 file electronically. Your submission must include:
  - The file `sha512.py/pl` containing your code for your SHA-512 implementation.
- In your program file, include a header as described on the ECE 404 Homework Page.
- If using Python, please denote the Python version in your code with a shebang line (e.g. `#!/usr/bin/env python3`)
- Please include comments in your code.

Electronic Turn-in

`turnin -c ece404 -p hw08 sha512.pl` (if using Perl)
`turnin -c ece404 -p hw08 sha512.py` (if using Python)