ECE 404 Homework #7

Due: Thursday 03/12/2020 at 4:29 PM

SHA-512

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

Your program should have the following call syntax :

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

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

Submission Notes

- Your electronic submission should include the 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 make sure your shebang line works on ECE Grid (or ECN in general) by running the command `chmod +x sha512.py; ./sha512.py` in the terminal.

Electronic Turn-in

`turnin -c ece404 -p hw07 sha512.pl` (if using Perl)
`turnin -c ece404 -p hw07 sha512.py` (if using Python)