Web-based cryptographic hashing simulator

Student: Lim Dong Li, Tony
Supervisor: Assoc Professor Anwitaman Datta

Motivations
- Learn the hashing process
- Visualize mathematical concepts
- Trace process flow

Languages & Tools
- Hyper Text Markup
- Language 5 (HTML5)
- JavaScript
- jQuery
- Bootstrap
- AngularJS

Each process in the flow can be expanded to view the description and the mathematical steps with the formulas. Every step of processing will be simulated ensuring the processing flow to be easy to follow.

Message Digest 5
The algorithm takes in a variable-length input and produces an output of 128 bits.
The input message is processed in 512-bit blocks.

MD5 Process Flow:
- Padding
- Splitting
- Round Function

There will be 4 defined functions and each function will be used to perform 16 rounds of processing for each 512-bit block.

Secure Hash Algorithm-512
The algorithm can take in an input of up to, but not including, $2^{128}$ bits and produces an output of 512 bits. The input message is processed in 1024-bit blocks.

SHA-512 Process Flow:
- Padding
- Splitting
- Message Schedule
- Round Function

There will be 80 rounds of processing for each 1024-bit block.