s1312014

Tenshi Munasinghe

Code Review

Disclaimer

As *strcpy_s* is not available on gcc, the review is conducted after replacing the said function with *strcpy*.

Functionality

The encryption of the genesis node will not happen properly if the data is too short (if the *input* string is less than 33 characters, *simpleHash* will return the data as it is).
The produced hash is also non-reversible. Which means there is no way to retrieve the hashed information making the encryption useless.
With that said, every process other than the actual hashing algorithm (eg: reading input from user, appropriate memory management of structures, error handling) are done well.

Readability

The code uses structures and decomposition of processes in the form of functions. Appropriate naming of functions and usage of comments make the processes easier to be understood.

Security

Hashing algorithm used is weak, therefore the code has poor security.

Error handling

Proper error handling is done to detect memory leak and invalid input.

Improvements

Usage of better hashing algorithm for better security and functionality

Implementation of nonce for better security.