# CS 305 Module Five Coding Assignment Checksum Verification Template

## Instructions

Using the instructions from theModule Five Coding Assignment Checksum Verification Guidelines and Rubric, replace the bracketed text with the relevant information in your own words.

## Algorithm Cipher

The algorithm cipher I selected for this business application is SHA-256 (Secure Hash Algorithm 256-bit).

## Justification

SHA-256 works by padding the original data with a one and zeros until the sum of the length and 64 bits is a multiple of 512. Next, a modulus value is determined, consuming those remaining 64 bits (Jena, 2023). In SHA-264, eight hash values are used initially, each is a 32-bit set of characters derived from square roots of prime numbers (Jagannath, 2023). The data will be separated into 512-bit blocks and hashed 64 times, so 64 keys will be needed as well. It is a chain reaction; each time a block is hashed, the subsequence block will use the prior output as input. The final output of the final block is a 256-bit digest (the final hash value) (Jena, 2023).

I selected SHA-256 for several reasons. First, it is an approved hash algorithm specified as a Federal Information Processing Standard (FIPS 180-4). It is included in this standard because of the low probability of producing two different messages from the same hash (collision resistance), and its resistance to reverse-engineering to find the original message from the hash alone (Information Technology Laboratory, 2015). Collisions occur when two different pieces of data produce the same hash. This can be dangerous because it can be impossible to know which of the two data sets was the original set.

## Generate Checksum

You’ll submit your refactored code to your instructor. Your instructor will review it and this document.

## Verification

Insert a screenshot below of the web browser with your unique information.

A screenshot of a computer

Description automatically generated

# References

Information Technology Laboratory. (2015). *FIPS PUB 180-4.* Gaithersburg, MD: National Institute of Standards and Technology.

Jagannath, S. (2023, 8 7). *What is SHA-256 Hash? An In-depth Guide with Examples*. Retrieved from DebugPointer: https://debugpointer.com/security/sha256-overview

Jena, B. K. (2023, 8 29). *A Definitive Guide to Learn the SHA-256 (Secure Hash Algorithms)*. Retrieved from SimpliLearn: https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm