# 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 selected for generating the checksum is SHA-256 (Secure Hash Algorithm with 256-bit output). SHA-256 belongs to the SHA-2 family developed by the National Security Agency (NSA) to provide cryptographic hashing that ensures data integrity.]

## Justification

[SHA-256 was chosen because of its strong security properties and widespread acceptance as a dependable hashing algorithm. It creates a 256-bit (32-byte) fixed-length hash from any input, making it computationally infeasible to reverse-engineer the original data from the hash. This resistance to inversion helps maintain data confidentiality and integrity. Additionally, SHA-256 is highly resistant to collision attacks, where two distinct inputs generate the same hash value, which is essential for trustworthy checksum verification.

Its extensive use in security protocols, such as SSL certificates and blockchain, highlights its reliability. SHA-256’s capability to produce a consistent and unique hash regardless of input size makes it ideal for confirming that data remains unchanged during transmission or storage.

Using SHA-256 enhances the checksum verification by adding a robust layer of security, suitable for applications demanding strong protection against tampering and cyber threats.]

## 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.

[Insert screenshot.]

A screenshot of a computer

AI-generated content may be incorrect.