# 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 I would recommend for generating a checksum would be SHA-256.

## Justification

SHA-256 is part of the SHA-2 family of hashing algorithms that was developed by the NSA. This variant utilizes 64 rounds of hashing in order to generate an output that is truly unique. If this output was not unique, it could generate what’s called a hashing collision, wherein two separate inputs could generate the same output. This would immediately cause a security risk for its use, as multiple inputs generating the same output could mean that attackers could utilize collision data to spoof another value, potentially granting higher access. With its 64 rounds of hashing that it performs, there has yet to be a collision found up to the 64th round, although collisions have been found in lower intervals. Because of this, SHA-256 is a safe and secure algorithm to utilize for generating checksums – you’re guaranteed a unique output for every single unique input that you provide.

## 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.

