# 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 that I will recommend for this scenario is the Secure Hash Algorithm with a 256-bit key or SHA-256.

## Justification

SHA-256 is a member of the SHA-2 family and was designed by the National Security Agency or NSA. SHA-256 is a longer bit length than its predecessor which makes it more secure. This means that any change in input data results in a completely different hash. The SHA-256 has possible hash values which makes a collision very unlikely, so the updated version is less susceptible to collision attacks. A collision is when two different inputs have the same hash. We need to avoid these to ensure the data is kept secure, ensures trust, and enables secure digital interactions.

## Generate Checksum

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

## Verification

A screenshot of a computer program

Description automatically generated