# 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

By collision I assume you mean a situation s where two different plain texts encrypt to the same ciphertext (a property known as collision resistance). Once again the AES has his property so I will not change my recommendation from the last one. If you where referring to a hash function SHA-256 is designed to avoid collisions because the hash will look very different even with a small difference.

## Justification

SHA-256, how it works:

1. The input message can be of any length, from a few bytes to several gigabytes. SHA-256 processes the input message in fixed-size blocks (512 bits or 64 bytes). Padding is added to the message to ensure that its length is a multiple of the block size.
2. SHA-256 operates on each block of the message using a series of logical and arithmetic operations, including bitwise operations, modular arithmetic, and bitwise rotations. These operations are applied to the bits of the message block, and the result is used to update an internal state.
3. SHA-256 maintains an internal state, which is a set of variables that change as each message block is processed. The internal state is initialized to a fixed value at the beginning of the hash computation.
4. SHA-256 uses a compression function that takes the current internal state and the current message block as inputs. This function transforms the internal state and produces a new state.
5. After processing all message blocks, the final internal state represents the hash value. This hash value is a 256-bit (32-byte) representation of the input message.

Avoiding collision, how?:

Given the same input message, SHA-256 will always produce the same hash value. This property ensures consistency and predictability. It is computationally infeasible to find the original input message from its hash value. This property is known as preimage resistance. Given a specific input message, it is computationally infeasible to find a different input message that produces the same hash value. This property is crucial for avoiding collisions. SHA-256 is designed to make it extremely unlikely for two different input messages to produce the same hash value (collision). The 256-bit output space is large, with 2^256 possible hash values, making it statistically improbable to find two inputs that collide.

## Generate Checksum

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

## Verification

