# CS 305 Module Five Checksum Verification Assignment

**Brandon Hobbs**

**June 6, 2022**

**Instructions:** Replace the bracketed text with your answers in your own words.

## Algorithm Cipher

Recommend an appropriate encryption algorithm cipher that avoids collisions.

SHA-256 was selected for the hashing algorithm. SHA-256 has a probability of two hashes accidentally colliding of approximately 4.3\*10-60.

## Justification

Justify your reasoning for the recommended algorithm cipher by providing a brief, high-level overview of the encryption algorithm cipher.

SHA-256 is slower than, say, MD5 by about 60% but much stronger than SHA-1. For a typical, non-critical system 256 bits is probably enough. There is no need to suffer the slower performance of SHA-384 or -512.

## Generate Checksum

Refactor the code to encrypt a text string and generate a checksum verification. You will submit your refactored code for your instructor to review in addition to this document.

## Verification

