# CS 305 Module Five Coding Assignment Checksum Verification Template

## Algorithm Cipher

## The encryption algorithm cipher that avoids collisions recommended for the Checksum Verification Project is SHA-256.

## Security hash algorithm 256, referred to as SHA-256, is used to verify message, file, and data integrity. This 256-bit hash function converts data into a new, unrecognizable string using a 256-bit key. A string of random characters and numbers, also known as a hash value, is also 256 bits long (Thakkar, 2022).

## Justification

Hashes with more than one value attached to the same slot in a table or data structure (hash table) are known as collisions. SHA-256 is just as safe as SHA-384 or SHA-512. The security you get with them is identical since they cannot produce collisions with current or future technology. I recommend using SHA-256 because its 256-bit key offers greater security than many other hashing algorithms. As one of the most widely used and trusted industry standards, SHA-256 is trusted and widely used by public-sector agencies and technology leaders. It is improbable that there will be any collisions. According to the article, Why is 2^256 Secure (2022), there is a ^256 chance of a collision in SHA-256, ^256 is slightly less than the number of atoms in the known universe, about 10^8 atoms. Consequently, there is one chance in over 115 quattuorvigintillion of finding a collision. Changes to the original information, even the smallest ones, completely alter the hash value. No collisions have been reported with SHA-256 to date.

## Generate Checksum

(Submitted in Brightspace)

## Verification

***Screenshot of the web browser with your unique information***

Graphical user interface, text, application, email

Description automatically generated

**References**

Thakkar, M. (2022, April 18). *SHA 256 Algorithm Explained by a Cyber Security Consultant*.

InfoSec Insights. <https://sectigostore.com/blog/sha-256-algorithm-explained-by-a-cyber-security-consultant/>

*Why is 2^256 Secure?* (202, July 5). Privacy Canada.

<https://privacycanada.net/cryptanalysis/why-is-2-256-secure/>