# CS 305 Module Five Coding Assignment Checksum Verification Template

## Algorithm Cipher

I would recommend using the second generation of Secure Hash Algorithm (SHA-2), specifically SHA-256, as it is currently one of the most secure algorithms for keeping data secure. The SHA algorithms were created by NSA and the SHA-256 always produces a 256-bit hash value. It has a reasonable balance between security and speed of the function.

## Justification

The hash function works by converting a string input into a 256-bit hash value by putting it through it’s SHA-2 algorithm. One of the characteristics of the SHA-256 algorithm is that the hash functions are irreversible meaning that passing the digest value into the algorithm will not yield the original value. This is done to help prevent brute force attacks. Additionally, since the number of possible hash values is 2^256 it is highly improbable for a collision to occur even if someone was actively trying to brute force a collision, with our current level of technology.

## Generate Checksum

A computer screen shot of a program

AI-generated content may be incorrect.

## Verification

A screenshot of a computer

AI-generated content may be incorrect.