# 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 recommended algorithm cipher that avoids collisions is SHA-256.

## Justification

SHA-256 stands for Secure Hash Algorithm 256 (256 is its digest size in bits) and is a widely used hash algorithm from the SHA 2 family of algorithms (Jena, 2023). As a combined effort from the NSA (National Security Administration) and NIST (National Institute of Standards and Technology), it was published in 2001 because SHA-1 was becoming increasingly weak due to brute force attacks (Jena, 2023). Hashing is performed by scrambling raw information to the point that it cannot be reproduced back to its original form (Jena, 2023). The output it produces of a fixed length is called a hash or message digest (Rhodes, 2023). The output generated from the hashing algorithm will always be the same length, 256 bits, which is 32 bytes or 64 alphanumeric characters (Rhodes, 2023). Significantly, SHA-256 is deterministic meaning it will always produce the same output when it is given the exact same input and there is no way of reverse engineering an input because the knowledge of the output is available (Rhodes, 2023).

When considering an appropriate encryption algorithm, it is important to take into consideration collisions. Collisions occur when you take two completely different inputs, put them through a hashing algorithm, and the same output is produced in each instance (Espinosa, 2021). The higher the amount of bits of the encryption algorithm, the less likely there is a chance of a collision occurring (Espinosa, 2021).

With SHA-256 there are 2^256 (1.157920892e77) possible hash values making it nearly impossible for two different inputs to have the exact same hash value or message digest (Callaghan, 2023).

The most significant reason why SHA-256 is so popular and widely utilized is because it has no known vulnerabilities making it insecure, and the algorithm has not yet been broken (Callaghan, 2023). This makes it a leading algorithm over other popular algorithms like SHA-1, which has been broken. It was reported in February of 2017 that Google and CWI announced that they broke SHA-1 encryption and warning signs of its vulnerability began appearing sometime around 2005 (Forbes Technology Council, 2017).

## Generate Checksum

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

## Verification

Insert a screenshot below of the web browser with your unique information.

A screenshot of a computer

Description automatically generated

**References**

Callaghan, P. (2023). *Why You Should Use SHA-256 In Evidence Authentication*. Pagefreezer Blog.

<https://blog.pagefreezer.com/sha-256-benefits-evidence-authentication>

Espinosa, C. (2021, September 5). *Explanation of Cybersecurity Hashing and Collisions*. Christian

Espinosa. <https://christianespinosa.com/blog/explanation-of-cybersecurity-hashing-and-collisions/>

Forbes Technology Council. (2017, April 13). *SHA-1 Encryption Has Been Broken: Now*

*What?* <https://www.forbes.com/sites/forbestechcouncil/2017/04/13/sha-1-encryption-has-been-broken-now-what/?sh=4377c2077ee7>

Jena, B. K. (2023, August 29). *What is SHA-256 Algorithm: How It Works and Applications: Simplilearn*.

Simplilearn.com. <https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm>

Oracle. (2023, July 10). *API reference for Java Platform, Standard Edition*. Java Security

Standard Algorithm Names. <https://docs.oracle.com/en/java/javase/11/docs/specs/security/standard-names.html#cipher-algorithm-names>

Rhodes, D. (2023, August 31). *SHA-256 Cryptographic Hash Algorithm*. Komodo Academy | En.

<https://komodoplatform.com/en/academy/sha-256-algorithm/>