# CS 305 Module Five Coding Assignment Checksum Verification Emily Wood 3-30-2023

## 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

I chose to use the Secure Hash Algorithm (SHA-256) as it was listed under the MessageDigest section of the Java Security Standard Algorithm Names provided by Oracle.

## Justification

The organization requests a cryptographic hash function that is not susceptible to collisions. SHA-256 is an industry standard and widely used. There are 2256 possible hash values which makes it almost impossible to have a collision of the exact same hash value (Callaghan, 2020).

## Generate Checksum

Text

Description automatically generated

## Verification

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

Graphical user interface, text, application, email

Description automatically generated

**References:**

Callaghan, P. (2020, August 19). *Why you should use SHA-256 in evidence authentication*. Pagefreezer Blog. Retrieved March 30, 2023, from https://blog.pagefreezer.com/sha-256-benefits-evidence-authentication#:~:text=Predictably%2C%20these%20are%20also%20the,SHA%2D1%20have%20known%20vulnerabilities.