# CS 305 Module Five Checksum Verification Assignment

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

## Algorithm Cipher

Recommend an appropriate encryption algorithm cipher that avoids collisions.

My recommendation is SHA256 (Secure Hash Algorithm 256) due for the very low chance of collisions

## Justification

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

SHA-256 was developed by the NSA, National Security Agency. It is one of the best hashing functions to use with an incredibly low probability of having collisions. It being a hash function, it has three main effects of scrambling the data, accepting an input of any length and have a fixed length output, and most importantly: to manipulate the data where the input cannot be retrieved from the output. SHA-256 uses an output made of just lowercase letters and numbers 0-9, which would allow for 3864 combinations. This means that two different inputs have a very rare chance of having the same hash value causing a collision.

## 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

Demonstrate that a hash value has been created for the unique text string (your first and last name) by executing the Java code. Then use your web browser to connect to the RESTful API server. This should show your first and last name as the unique data string in the browser, the name of the algorithm cipher you used, and the checksum hash value. Capture a screenshot of the web browser with your unique information and insert it below.

Graphical user interface, application

Description automatically generated