# 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.

I recommend using SHA-256, as it is considered a secure hash with extremely low chance of collision.

## Justification

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

The cipher SHA was created in 2001 by the US Government, specifically the NSA or National Security Agency to replace the older cipher SHA-1. SHA-256 has an extremely low probability of collisions, of about 0.01% or 1/(2^256), if not less. SHA-256 works by using characters from both the lowercase alphabet and the numerical set of 0 - 9. By using a large character set, this means any data put into the algorithm will be changed by 36^64th. Using that exponent as an example, it is highly unlikely any two datasets will be identical.

## 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.

