# 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’m going to recommend the SHA256 algorithm as it has a 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.

SHA-256 was created on 2001 by the National Security Agency in 2001 as a successor to SHA-1. Additionally, SHA-256 is one of the most secure hashing functions on the market as the algorithm has 0.01% probability of having collisions. A collision is when an algorithm produces the same hash value for two distinct pieces of data. As SHA256 outputs characters composed of either lowercase letters or numerals zero through nine. This creates 3664 different possibilities meaning two pieces of data having the same hash value or causing a collision would be very unlikely.

## 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, text

Description automatically generated