# 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.

AES\_128 is “Advanced Encryption Standard”, capable of handling 128-bit block ciphers that avoids collisions.

## Justification

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

## According to Oracle documentation, AES cipher can be used with one valid key size using AES\_<n> format, where n is 128, 192, 256-bit sized keys. Higher bit keys require more processing power and higher latency, though it takes longer to guess. This makes AES\_128 a great choice for storing archives of large sizes over long periods.

## Creating strong keys requires pseudo-random generation techniques, as generation of the key for a symmetric algorithm requires a random string of 128 bits.

## AES is a symmetric key algorithm, in which the key is used for both encrypting and decrypting data.

## AES was developed as a mathematically efficient symmetric block cipher, and the standard replaced the slower DES in 2000.

## Extra:

## AES Operates in CBC Mode, which requires IV to make each message unique.

## 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.

