# CS 305 Module Five Coding Assignment Checksum Verification

Richard Howell

CS-305

SNHU

1/30/2023

## 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.

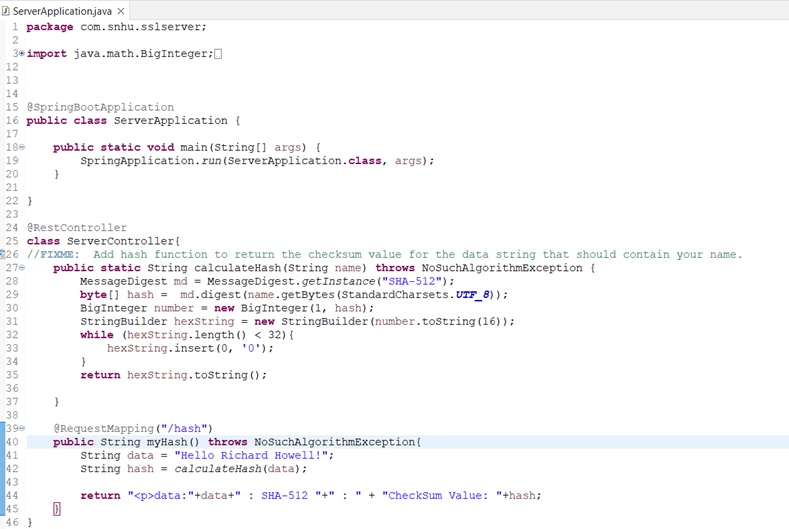
## Algorithm Cipher

I chose to implement the SHA-512-bit hash algorithm. This is also the algorithm I would recommend for avoiding collisions while maintaining processing speed.

## Justification

I think the SHA-512-bit algorithm is the best because it can take any length input message and create a fixed output digest of 512 bits. This is the largest currently available and will help mitigate the risks of potential collisions to almost zero. While collisions are still theoretically possible the probability is almost zero when using SHA-512. SHA-512 is also one of the strongest hash functions available at the current time. The SHA-512 hash algorithm is also a one-way process which makes it almost impossible to compromise. If an attacker was to use a brute force method it would take almost years. This means that even with the fastest known computers on the planet it would take millions of years to crack the SHA-512 hash algorithm.

## Generate Checksum



## Verification

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

Graphical user interface, application

Description automatically generated