# CS 305 Module Five Coding Assignment Checksum Verification Template

## 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 advise using the Secure Hash Algorithm 256-bit (SHA-256)

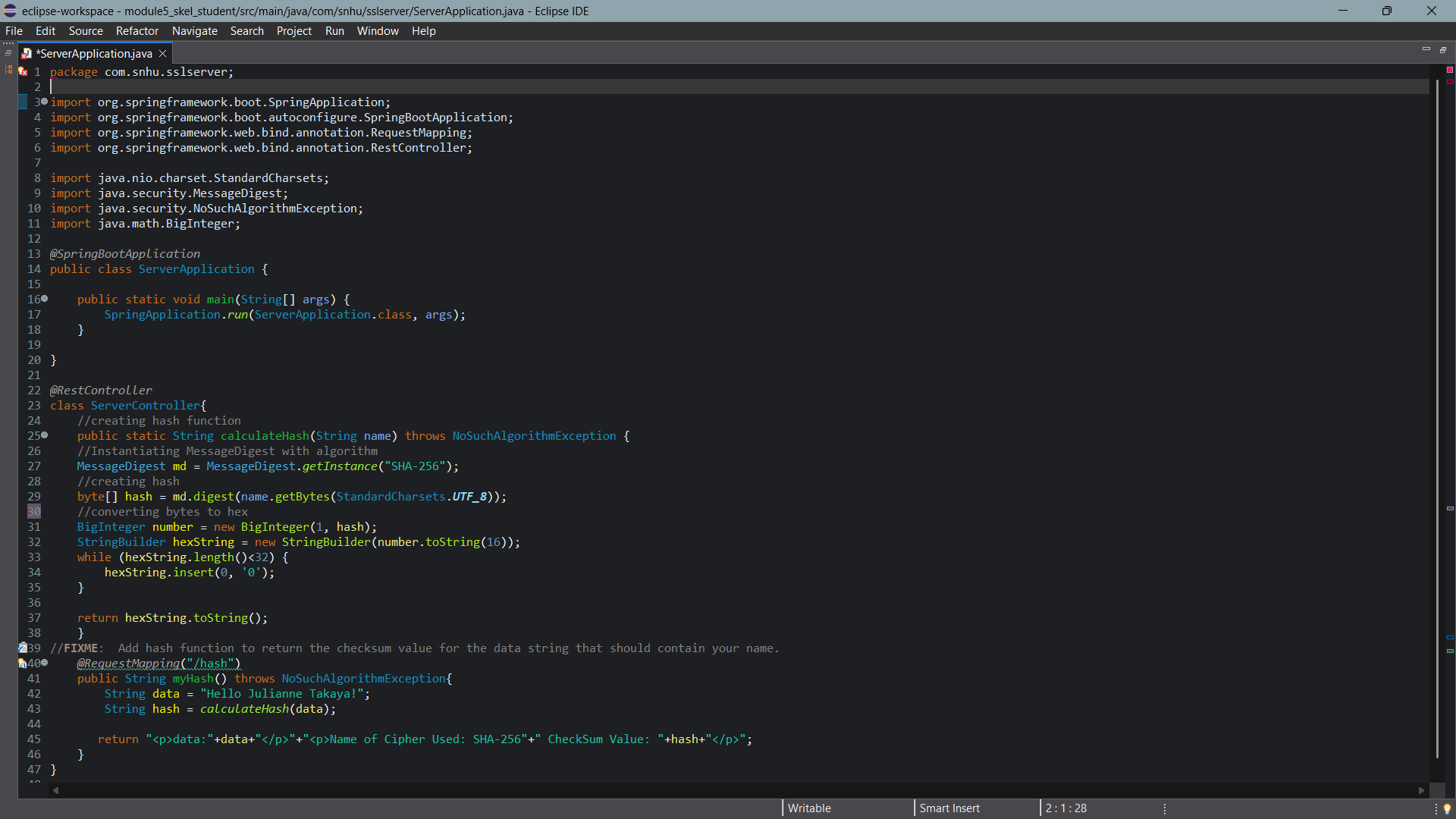
## Justification

SHA-256 is resistant to cryptographic attacks and collisions as the algorithm generates a unique fixed-size 256-bit hash value for every unique data input. This ensures that even with small changes in data, a new and unique hash value will be generated. SHA-256 is standard, ensuring acceptance across platforms and systems. Additionally, SHA-256 is non-reversable, meaning that deriving the original data from the hash result is computationally impossible.

SHA-256 works by processing an input message of any length into blocks of 512 bits, padding the data if necessary. These data blocks are then processed through several computation cycles, then compressed into an intermediate hash value for each block. The block hash values are then added together to generate the final 256-bit hash value. The fixed size block hashing guarantees a unique hash value for each input. SHA-256 uses a strong hashing algorithm to prevent collisions, which occur when two different inputs result in the same hash value. This is important, as collisions make it possible for attackers to produce unique inputs that match the hash of other inputs, which could jeopardize the integrity of the hash function and expose security holes.

## Generate Checksum

You’ll submit your refactored code to your instructor. Your instructor will review it and this document.



## Verification

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

I am unable to verify this hash function works, as I cannot move past this error, which prevents me from running the program.

