# 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

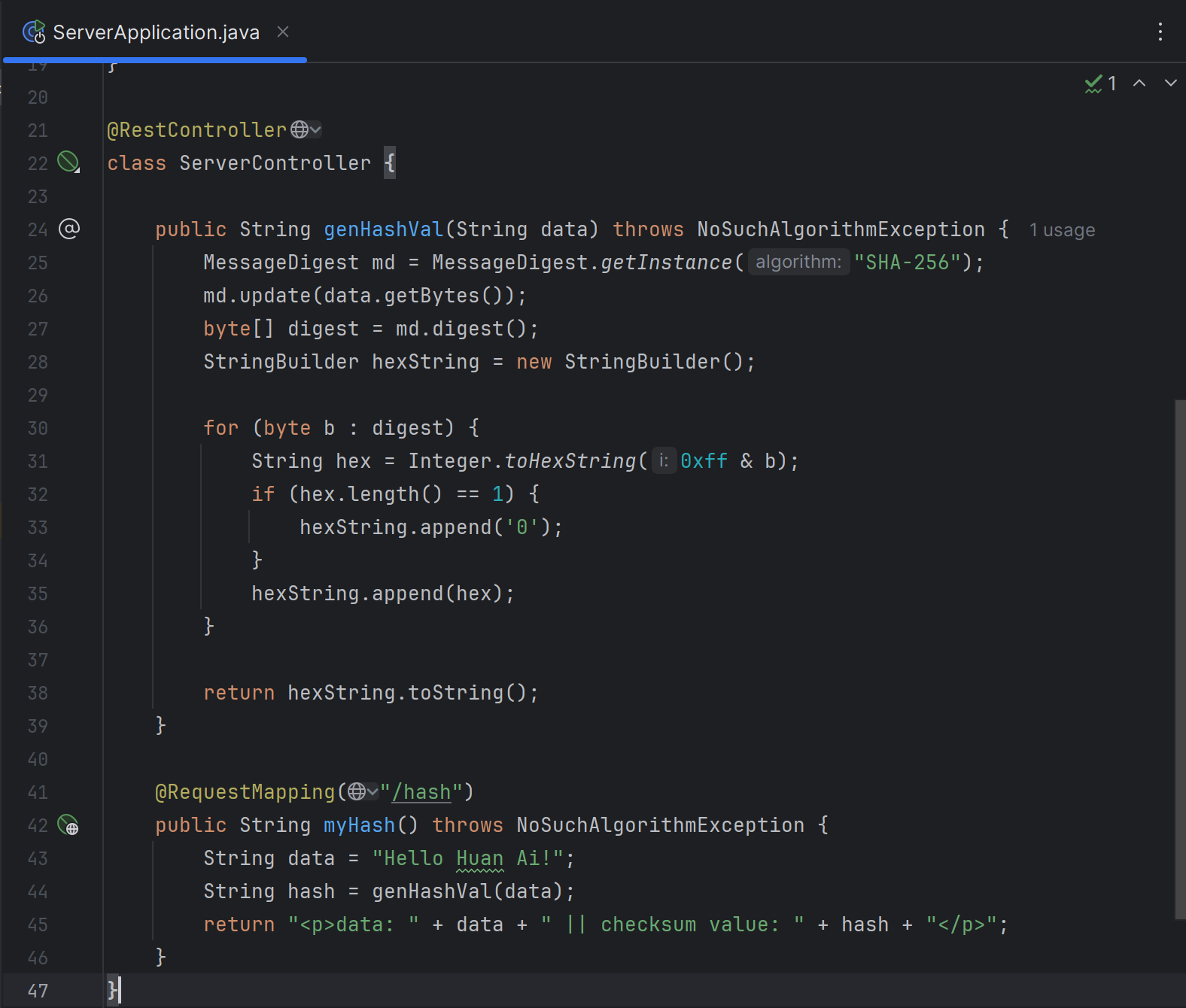
I will recommend the SHA-256 cryptographic hash function.

## Justification

SHA-256 is a type of cryptographic hash function designed by the NSA and standardized by NIST. It produces a 256-bit (32-byte) hash value, typically rendered as a 64-digit hexadecimal number. SHA-256 is widely used in security applications and protocols, including TLS and SSL, PGP, SSH, and Bitcoin. A hash collision occurs when two different inputs produce the same hash output.Collisions could allow attackers to replace legitimate files with malicious ones that have identical hashes, bypassing integrity checks. SHA-256 provides strong collision resistance, meaning it's computationally impossible to find two different inputs that produce the same hash output.

## 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.

