Ryan Hatch  
SNHU  
CS-305 Software Security  
Module Five 5-1 Coding Assignment  
February 18, 2024

# Checksum Verification

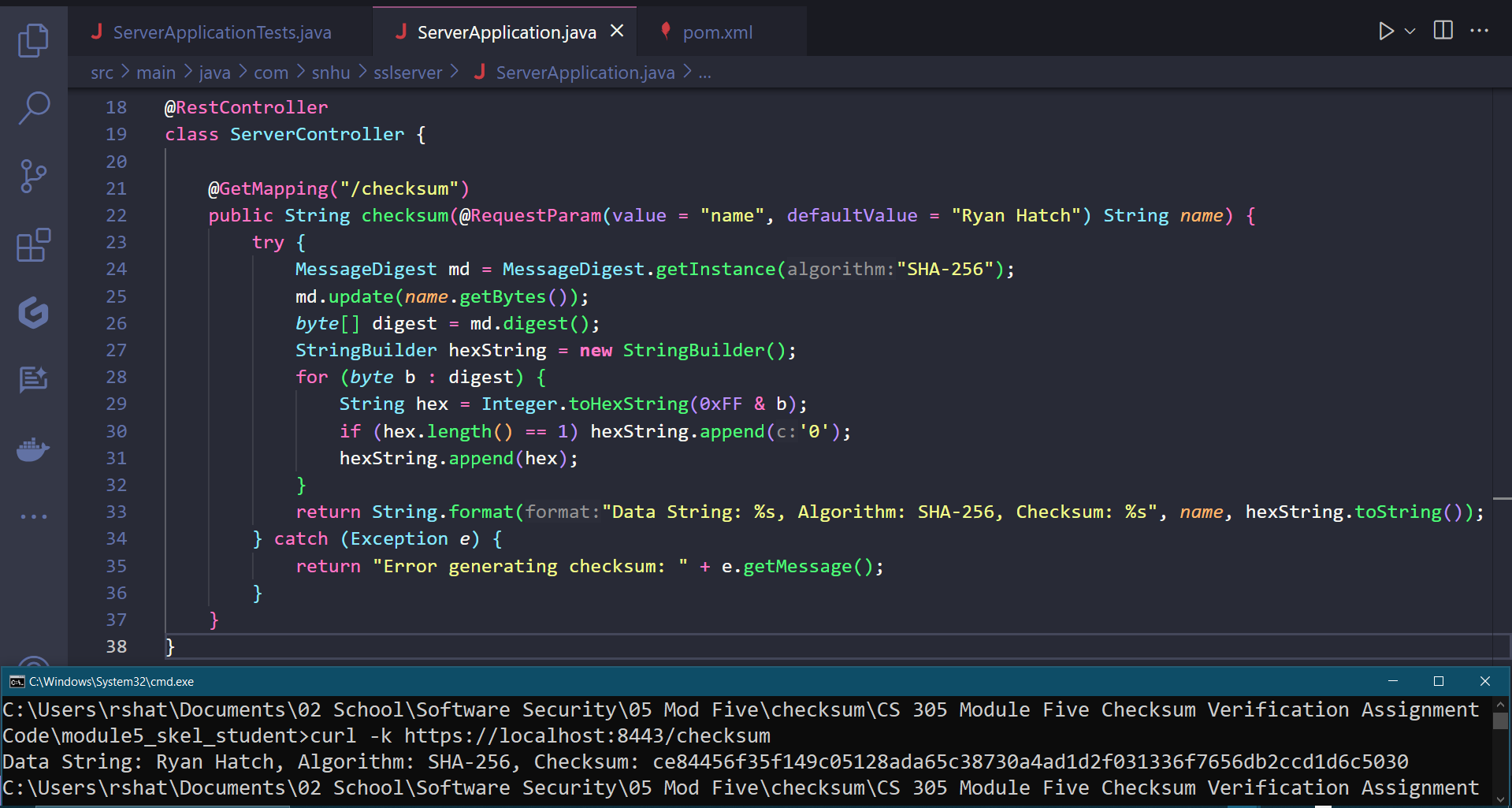
## Algorithm Cipher:

Two of the best algorithmic ciphers have been recommended to be strong in collision resistance and have been selected on the assumption of a collision resistance attack, and they are SHA-256 and SHA-3. SHA-256 forms part of the SHA-2 family of hashes, with it being in use in all security protocols. SHA-3 is the new standard and, although it is not a fix on SHA-2, it provides a different approach to hashing, which in turn offers a better margin of security when the implementation of collision attacks come into play.

## Justification

One important aspect to consider is how the strong collision resistance that SHA-256, and SHA-3, would be used in implementations of the checksum verifications. With collision resistance, no single pair of inputs will yield the same output from the hash function. This ensures that an attacker is unable to replace the file with a new one of the same checksum. Also, the architectural differences between SHA-3 and SHA-2 may give an extra cushion of security, considering that many of the vulnerabilities that could occur from that of SHA-2 may give extra layer of security for many of the vulnerabilities that could fall on the SHA-2 algorithms.

## Generate Checksum



## Verification

