Southern New Hampshire University

Module Five Assignment:

Checksum Verification

Elizabeth Marticello

Southern New Hampshire University

CS 305-11883-M01 Software Security 2025 C-4

Professor Albanie Bolton

Due Date: August 3rd, 2025

Southern New Hampshire University

Algorithm Cipher

I recommend using SHA-256 as the encryption algorithm to ensure data integrity and security.

Justification

Among common checksum algorithms such as MD5, SHA-1, SHA-256, and CRC. From this list SHA-256 is the most secure and widely used (GeeksForGeeks, 2024). According to Oracle's *Java Security Standard Algorithm Names*, MessageDigest Algorithms include MD2, MD5, SHA-1, and SHA3-256. While SHA3-256 offers enhanced security features, it is still gaining adoption across industries compared to its well-established predecessor (MojoAuth, n.d.). SHA-256 is part of the SHA-2 family and generates a fixed-size 256-bit hash value regardless of input size, making it highly reliable for data integrity verification (MojoAuth, n.d.).

Avoiding Collisions

A collision occurs when two different inputs produce the same hash output, which undermines the hash's trustworthiness. If collisions are easy to find, malicious actors could substitute data without detection (VPN Unlimited, n.d.).

Why Avoiding Collisions is Important

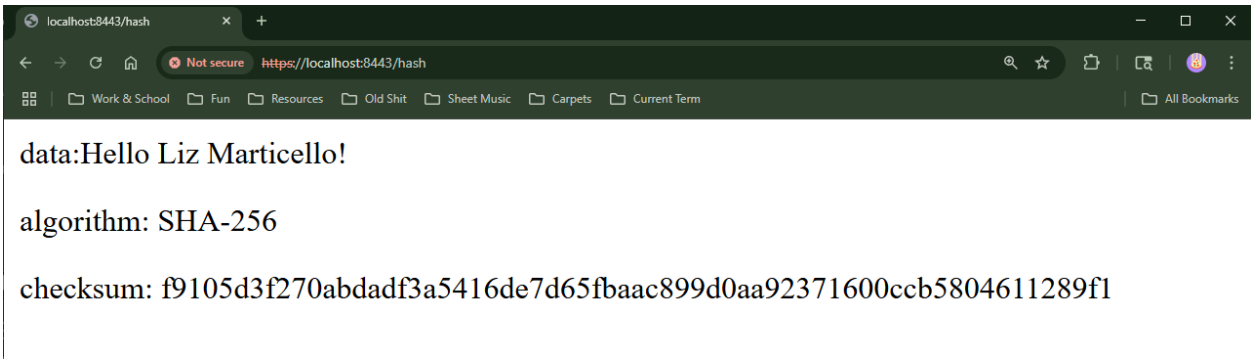
Avoiding collisions is vital to maintaining data integrity and security. If two distinct inputs yield the same hash value, it weakens the checksum's reliability, opening the door to undetected tampering or substitution. By minimizing collisions, systems can confidently verify that the data received or stored matches the original, protecting against unauthorized changes and accidental corruption. This trustworthiness is essential for preserving security and enabling accurate decision-making based on that data (VPN Unlimited, n.d.).

Southern New Hampshire University

Generate Checksum

Please see the attached refactored code for this section.

Verification



Southern New Hampshire University

Resources

(n.d.). *Java Security Standard Algorithm Names*. Oracle. https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names

(2024, May 28). *Understanding Checksum Algorithm for Data Integrity*. GeeksForGeeks. https://www.geeksforgeeks.org/system-design/understanding-checksum-algorithm-for-data-integrity/

(n.d.). *SHA-256 vs SHA3-256*. MojoAuth. https://mojoauth.com/compare-hashing-algorithms/sha-256-vs-sha3-256/

(n.d.). *What is Collision*. VPN Unlimited. https://www.vpnunlimited.com/help/cybersecurity/collision?srsltid=AfmBOopOt0lnNUcfbuY5O9knJmlp1_CkbsdgoifTFTVYQG4B1i_AkprD