CS 305 Software Security

Checksum Verification

Sergio Mateos

Southern New Hampshire University

# CS 305 Module Five Coding Assignment Checksum Verification Template

## Instructions

As a software developer, I work with a business that has a public key that would like to distribute to its clients. The public key is available by downloading it from a website. But the business is seeking to verify the key with a checksum.

## Algorithm Cipher

As a developer, I was in charge to select which Algorithm Cipher would appropriately encrypt and avoid a collision. The research was based on Java Security Standard Algorithm Names (1993) which contain a lot of algorithms that will prevent security issues. Based on the research I end up to the conclusion that the best Algorithm Cipher that will prevent any collision and encrypt information properly would be SHA-256.

SHA-256 or Secure Hash Algorithm 256, is an encrypted algorithm that converts any text into a fixed-size string of 256(32 bytes).

## Justification

First, SHA-256 has a chance of collision too low. Second, the alteration of the original input will produce significant changes that increase the difficulty for the malicious user to find out the content of the original text. SHA-256 is approved by the National Institution of Standard and Technology (NIST) and officially approved as a standard algorithm. SHA-256 is the most secure hashing, even slower compared to other algorithm ciphers like MD5 or SHA-1. The Komodo Blog state “SHA-256 is computationally efficient and an ordinary computer can perform the operation dozens or even hundreds of times per second.” (Komodo, 2022). This ensures the efficiency and security of using SHA-256. There has not been a report about the attack broke the SHA-256.

## Graphical user interface, text, application Description automatically generatedGenerate Checksum

Text

Description automatically generated

## Verification

IGraphical user interface, text, application, email

Description automatically generated

[Insert screenshot.]

Reference

*Java Security Standard Algorithm Names*. Java security standard algorithm names. (n.d.). Retrieved January 29, 2023, from <https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names>

Rhodes, D. (2022, April 29). *SHA-256 cryptographic hash algorithm*. Komodo Academy | En. Retrieved January 29, 2023, from https://komodoplatform.com/en/academy/sha-256-algorithm/