Southern New Hampshire University

5-1 Coding Assignment: Checksum Verification

David Vega

Dr. Vivian Lyon

CS-305 – Software Security

02/05/2023

# CS 305 Module Five Coding Assignment Checksum Verification Template

## Algorithm Cipher

The recommended algorithm cipher for the scenario provided is SHA-256 (Secure Hash Algorithm 2) (Oracle, 2017). SHA-256 is a collision resistant algorithm that makes it impossible to reverse engineer the hash value. Collisions typically occur when two pieces of text evaluate to the same hash value. As you can see, this can be dangerous because if an attacker can identify this vulnerability, they can exploit it to gain access to secure systems or encrypted files (N-able, 2019).

## Justification

The justification for using this algorithm is the amount of protection it will provide. This algorithm would deter hackers from using brute-force attacks to try to gain access to secure data. It would be at a significant cost (approximately 2256) for an attacker to use brute-force. This would take an enormous amount of time, and processing power to iterate through all those rounds of block ciphers. According to the Federal Information Processing Standards 180-4 which offers specifications for hashing algorithms and was issued by the National Institute of Standards and Technology (NIST), states:

“*These algorithms enable the determination of a message’s integrity: any change to the message will, with a very high probability, result in a different message digest.”*

This is important because this provides reassurance that the encrypted data hasn’t been altered since the digest was created (NIST, 2015). An example of where this potential exploit can be used by an attacker would be if two different documents were distributed with identical hash values. The issue here would be that the altered document would not have generated an exception allowing for potentially malicious code to make its way into a secure system.

## 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.

Graphical user interface, text, application, website

Description automatically generated

# References

N-able. (2019, September 12). *SHA-256 Algorithm Overview*. Retrieved from n-able.com: https://www.n-able.com/blog/sha-256-encryption#:~:text=SHA%2D256%20is%20a%20patented,as%20long%20as%20when%20unencrypted

NIST. (2015, August 5). *Secure Hash Standards.* Retrieved from Computer Security Resource Center: https://csrc.nist.gov/publications/fips#180-4

Oracle. (2017). *Java Security Standard Algorithm Names.* Retrieved from docs.oracle.com: https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names