# CS 305 Module Five Checksum Verification Assignment

Brandon Coulter  
Southern New Hampshire University Attendee

CS-305-T6614 Software Security 22EW6

Dr. Vivian Lyon  
July 31, 2022

## Algorithm Cipher

The algorithm cipher of choice that would best suit the needs of the client would be the SHA-256 algorithm. This algorithm is an exceptionally strong cipher that would work perfectly for public key distribution and verification. SHA-256 is secure from collision attacks that alternative ciphers of a weaker status such as SHA-1 ciphers may be vulnerable to. A hash collision attack occurs when an attacker is able to find two messages that produce the same hash value allowing an attacker to fake an electronic signature and gain access to secure systems. (Safaryan et al., 2021)

## Justification

Due to the security and collision resistant nature of the SHA-256 algorithm, the use of this cipher would work excellent for distribution of the company’s public key to their clients. Creation of a checksum value with the SHA-256 cipher will ensure that the key that is received is the key that is given and not fake or malicious. The SHA-256 cipher algorithm is chosen because of the nearly impossible means of finding a collision that could be used to exploit the security system. This is expressed by the National Institute of Standards and Technology (NIST) in its publication FIPS PUB 180-4 *Secure Hash Standard (SHS)*, when they say, “All of the algorithms are iterative, one-way hash functions that can process a message to produce a condensed representation called a message digest. 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 property is useful in the generation and verification of digital signatures and message authentication codes, and in the generation of random numbers or bits.” (National Institute of Standards and Technology, 2015) As mentioned above, the importance of avoiding collisions with a hash algorithm is evident in the inherent vulnerability that comes along with a weak hash function. A weak hash algorithm is more susceptible to collisions allowing attackers to gain access or sign false certificates. The protection of the digital signature and verification that the product given is the product received is crucial for the trust of the clients. The digital signature of a product can be verified with a checksum verification, which ensures the confidence of the receiving party, thus demonstrating the confidence in security of the product to be downloaded. (Manico, 2015) The SHA-256 cipher ensures this requirement is met, ensuring that the clients can trust the key to not be forged or altered.

## Generate Checksum

Refactor the code to encrypt a text string and generate a checksum verification. You will submit your refactored code for your instructor to review in addition to this document.

## Verification

Demonstrate that a hash value has been created for the unique text string (your first and last name) by executing the Java code. Then use your web browser to connect to the RESTful API server. This should show your first and last name as the unique data string in the browser, the name of the algorithm cipher you used, and the checksum hash value. Capture a screenshot of the web browser with your unique information and insert it below.

Graphical user interface, text, application, email

Description automatically generated

Reference

Manico, J., Detlefsen, A., & Kenan, K. (2015). *Iron-clad Java*. O'Reilly Online Learning. Retrieved July 28, 2022, from <https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/ch01.html#ch01lev2sec3>

National Institute of Standards and Technology. (2015, August 4). *Secure hash standard (SHS)*. CSRC. Retrieved July 28, 2022, from <https://csrc.nist.gov/publications/detail/fips/180/4/final>

Safaryan, O., Cherckesova, L., Lyashenko, N., Razumov, P., Chumakov, V., Akishin, B., & Lobodenko, A. (2021). *Modern Hash Collision CyberAttacks and Methods of Their Detection and Neutralization*. Journal of Physics: Conference Series. Retrieved July 28, 2022, from <https://iopscience.iop.org/article/10.1088/1742-6596/2131/2/022099/pdf>