CS 305 Module Five Coding Assignment Checksum Verification Template

Instructions

Using the instructions from the Module Five Coding Assignment Checksum Verification Guidelines and Rubric, replace the bracketed text with the relevant information in your own words.

1. Algorithm Cipher

I had a difficult time sorting through the Oracle site, as there is a lot of information in it and my brain was having a difficult time sorting through it. Chris Hoffman mentioned SHA-256 (Hoffman, 2018), which led me to researching the SHA-256 hash algorithm. This is the encryption algorithm cypher that I will recommend for this. SHA-256 is designed to provide a higher level of security compared to its predecessor, SHA-1. It produces a 256-bit hash, making it basically impossible for it to generate two different inputs with the same hash value (collision resistance). In Java, you can use the MessageDigest class with the "SHA-256" algorithm for this hash generation.

2. Justification

Collision resistance is a big reason for selecting SHA-256 as my encryption algorithm cypher. Collision resistance means that it should be mathematically improbable to find two different inputs that will produce the same output (hash value). It provides a large enough range of possible hash values, that it makes it extremely unlikely for collisions (the same hash value) to happen.

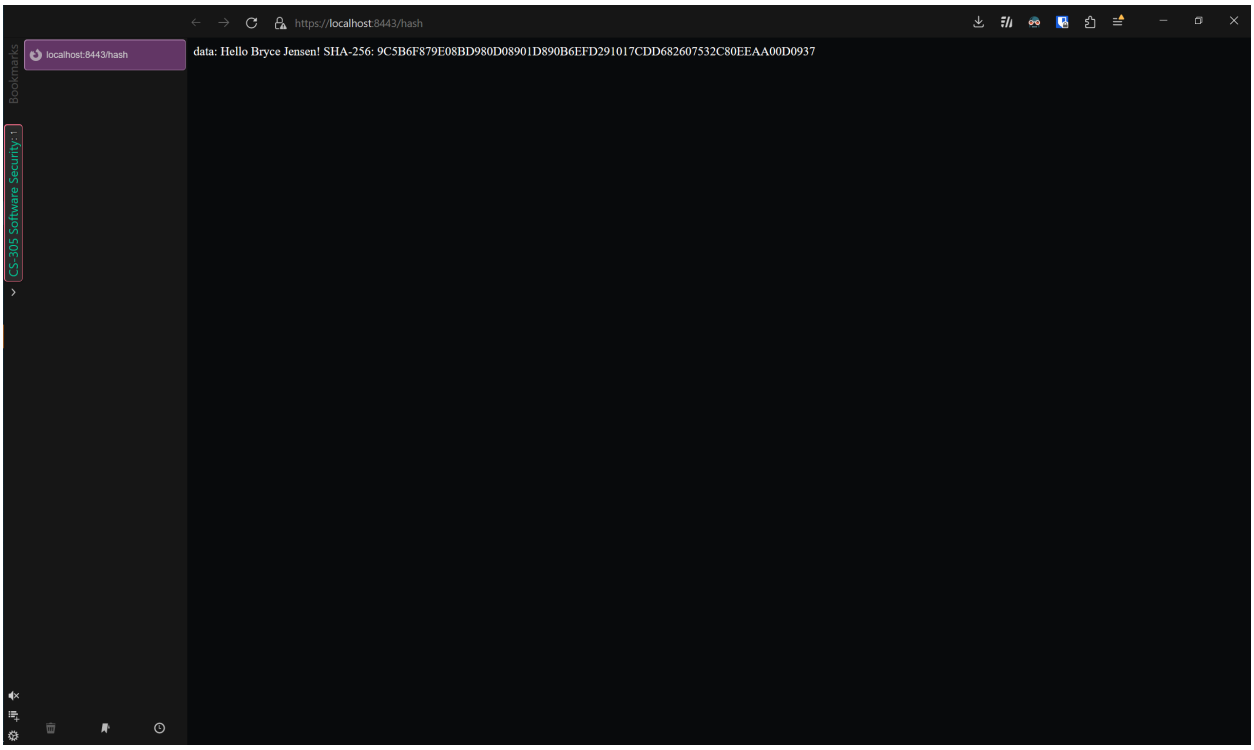
The National Institute of Standards and Technology (NIST) published a standard containing the entire SHA family of cryptographic hash functions. From the document's abstract, "This standard specifies hash algorithms that can be used to generate digests of messages" (Dang, 2015). SHA-256 is part of the SHA-2 family and is considered the most modern of the standards for messages containing less than 2^{64} bits (Dang, 2015). In my opinion, following the guidelines set by governments is generally good practice; if it is good enough for them, it should be good enough for me.

3. Generate Checksum

You'll submit your refactored code to your instructor. Your instructor will review it and this document.

4. Verification

Insert a screenshot below of the web browser with your unique information.


https://localhost:8443/hash
localhost:8443/hash
data: Hello Bryce Jensen! SHA-256: 9C5B6F879E08BD980D08901D890B6EFD291017CDD682607532C80EEAA00D0937
Bookmarks
CS-305 Software Security-1

References

Dang, Q. H. (2015). *Secure Hash Standard (SHS).* National Institute of Standards and Technology (NIST), Federal Information Processing Standards. Gaithersburg, MD: NIST FIPS. doi:https://doi.org/10.6028/NIST.FIPS.180-4

Hoffman, C. (2018, Aug 29). *What Is a Checksum (and Why Should You Care)?* Retrieved from howtogeek.com: https://www.howtogeek.com/363735/what-is-a-checksum-and-why-should-you-care/