**5-1 Coding Assignment: Checksum Verification**

## Algorithm Cipher

After reviewing the scenario and the Java Security Standard Algorithm Names, I recommend using the SHA-256 encryption algorithm cipher to avoid collisions.

## Justification

As technology advances, communication and data transmission have become more reliant on security functions, such as secure hash algorithms (SHA), to protect sensitive information from being stolen. SHA-256 comes from the SHA-2 family and can generate a distinctive 256-bit (32-byte) encryption string using the hash methods.

According to Lake, collision attacks threaten a cybersecurity foundation in software security. Once compromised, unauthorized users can create malicious messages using the same hash value without the system identifying any issues. (Lake, 2023, para 16). It is impossible to avoid collisions. However, using SHA-256 means an attacker would have known the exact output of the 64 digits. This information is important because it means the probability of identifying the code is low, making it one of the most secure algorithms and extremely difficult to crack.

## Generate Checksum

Refactored code is submitted as a separate file.

## Verification

A screenshot of a computer

Description automatically generated

References

Lake, J. (2022, March 30). *What is a Collision Attack?* Comparitech. <https://www.comparitech.com/blog/information-security/what-is-a-collision-attack/>