# CS 305 Module Five Coding Assignment Checksum Verification

# Alexis Prazak

## Algorithm Cipher

After reviewing the current MessageDigest algorithms, SHA-256 seems like the best algorithm for the business to use.

## Justification

SHA-256 is used widely today. This is because it presents little chance of collisions. Simply put it’s less likely that two keys will have the same hash value. Two pieces of data that collide can put users at a higher security risk. It can also degrade data and system performance. Checksum’s purpose is to verify data integrity. Other cipher algorithms, such as MD-5, are at a higher risk of collisions.

## Generate Checksum

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

## Verification

See screenshot below:

A screenshot of a computer

AI-generated content may be incorrect.