**Stephen Cardone**

**Mod5**

**CS 305 Module Five Checksum Verification Assignment**

**Instructions:** Replace the bracketed text with your answers in your own words.

**Algorithm Cipher**

Recommend an appropriate encryption algorithm cipher that avoids collisions.

I reccomend that the business use "SHA3-512"

**Justification**

Justify your reasoning for the recommended algorithm cipher by providing a brief, high-level overview of the encryption algorithm cipher.

I've chosen a SHA3 algorithm as the algorithm for the business for various reasons. Firstly, SHA3 will not have collisions which is something the business was concerned about. SHA1 has collisions, and SHA2 is just SHA1 with larger inputs and larger outputs. SHA3 is a completely different hashing process than its predecessors, and it will be a very long time before any conflicts are identified.

Performance: SHA3 does not have great performance relative to other weaker algorithms. I am going to reccomend SHA3-512 anyway because for the purpose of the business the speed of this event is not significant. Since we will be using this checksum only to check keys, this process will not be completed often. Once the key is recognized, we will not need to check again untill the key expires. Therefore there is no need to sacrifice security for speed in this case.

**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.

[Insert image.]

Please see seperate attached image file.