**Documentation: SHA-2 (Secure Hash Algorithm)**

Mohammed Towseef

Advanced Algorithms

Concordia

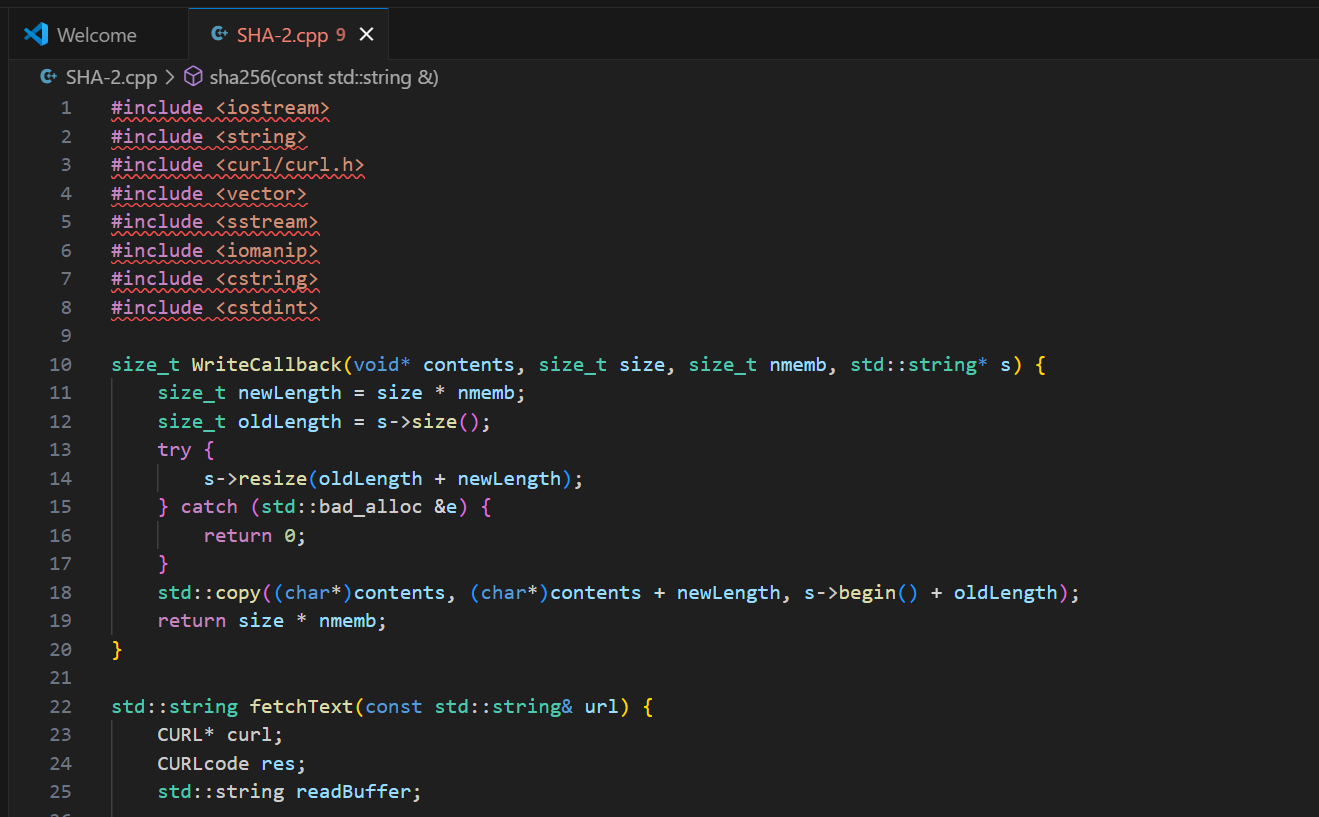
Farah Kamw

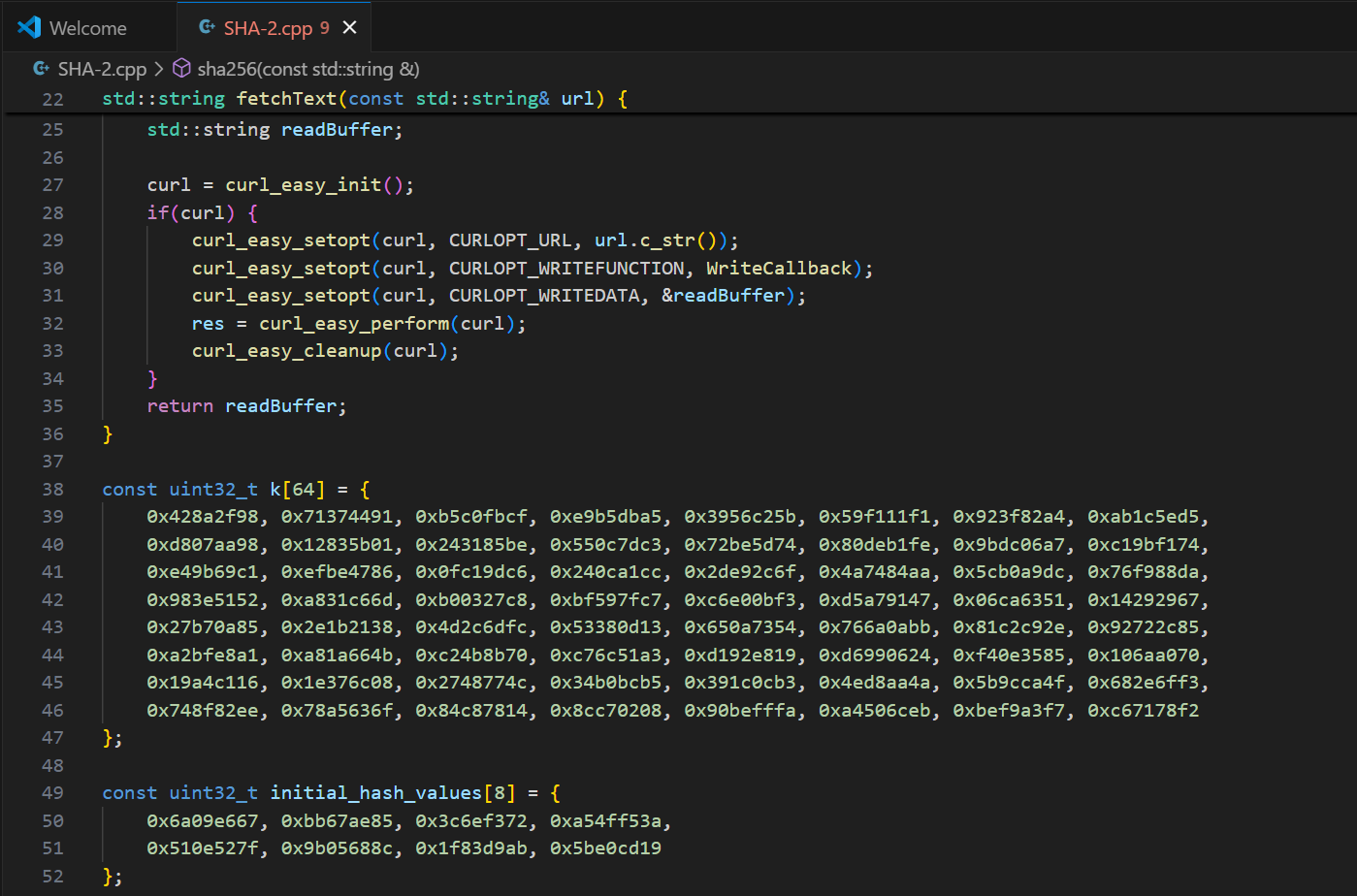
Aug 09, 2024

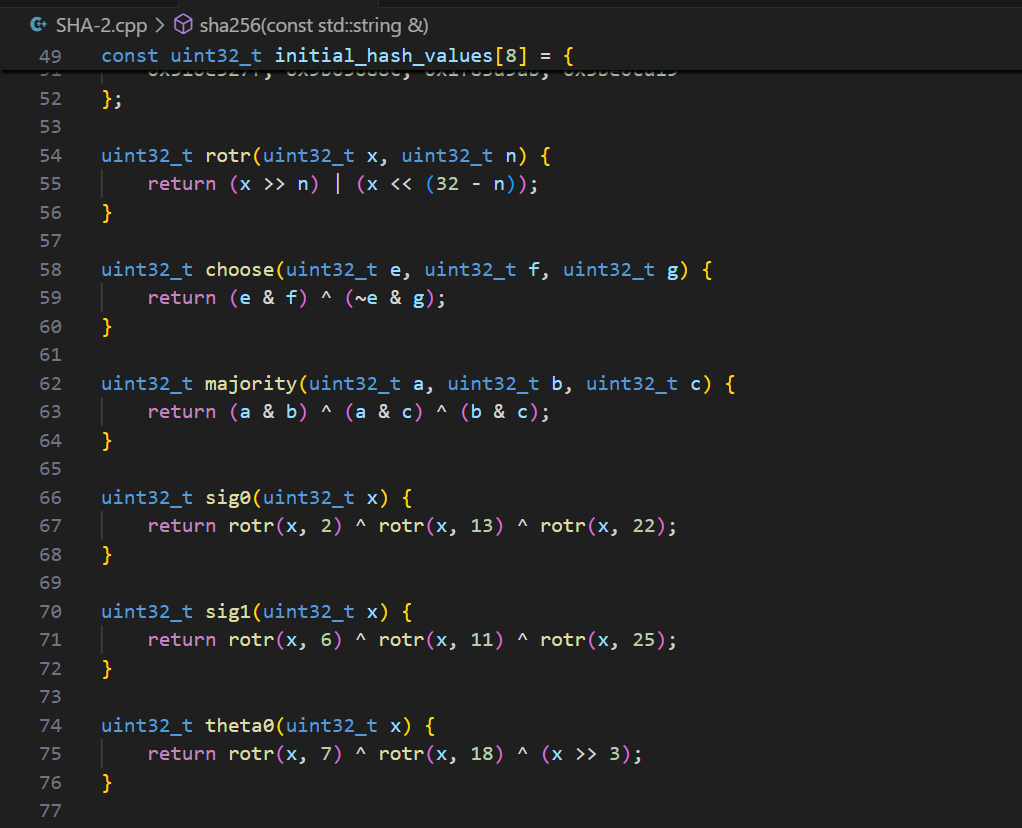
**Problem Analysis:**

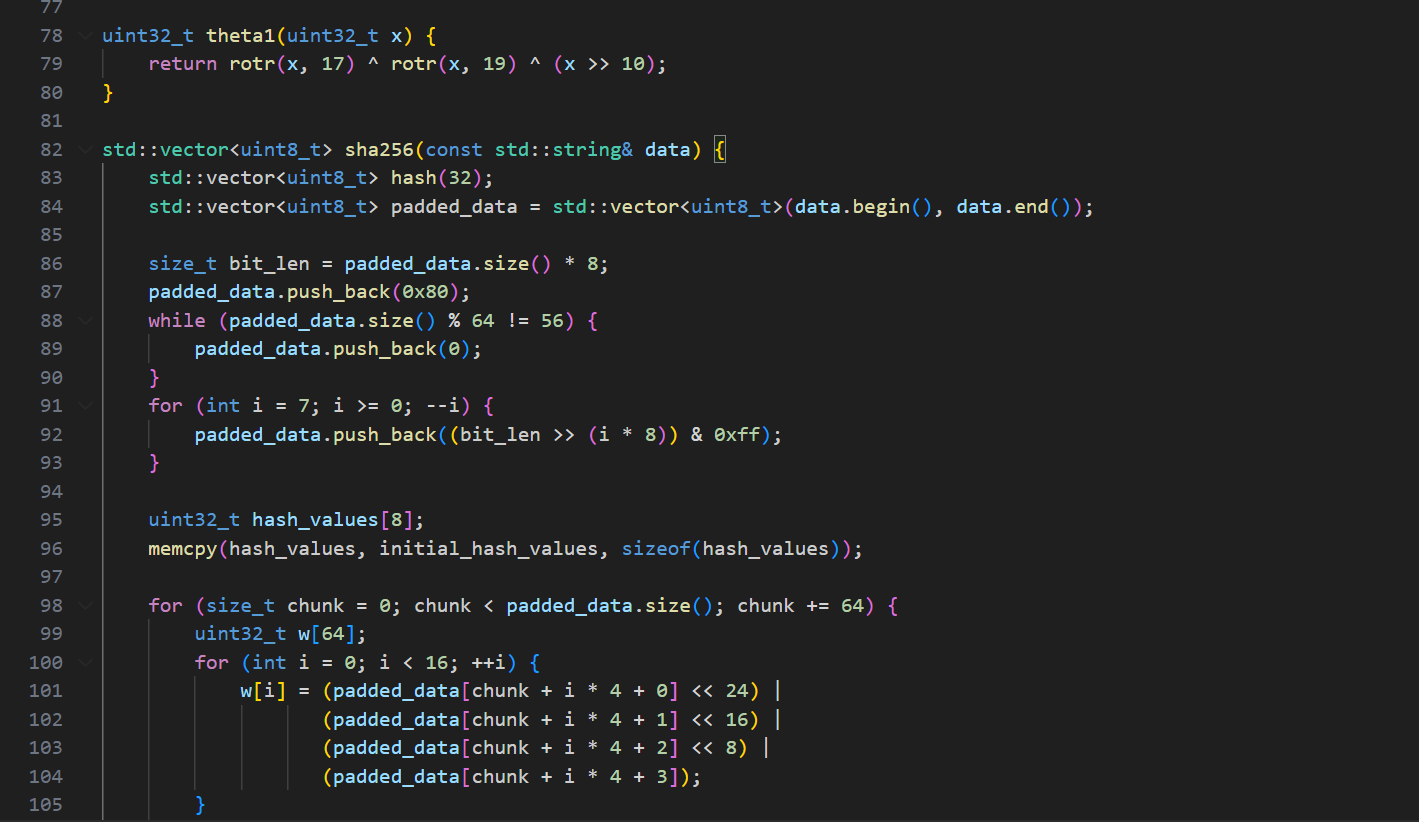
The performance includes using the SHA-256 cryptographic hash function to compute a hash for the entire text of the Book of Mark downloaded from a particular source on the web. SHA-256 is one of the most popular, reliable hash functions that creates a 256-bit (32-byte) hash value usually expressed as a 64-character hexadecimal number. In the project, text data must be obtained from a URL. The message needs to be padded based on SHA-256 algorithm requirements, where the text message is processed in 512-bit blocks, and several bitwise operations are executed to arrive at the final Hash. This process must indeed be adequately performed, each stage, from getting the data to computing the hash then displaying the hash must be done correctly.

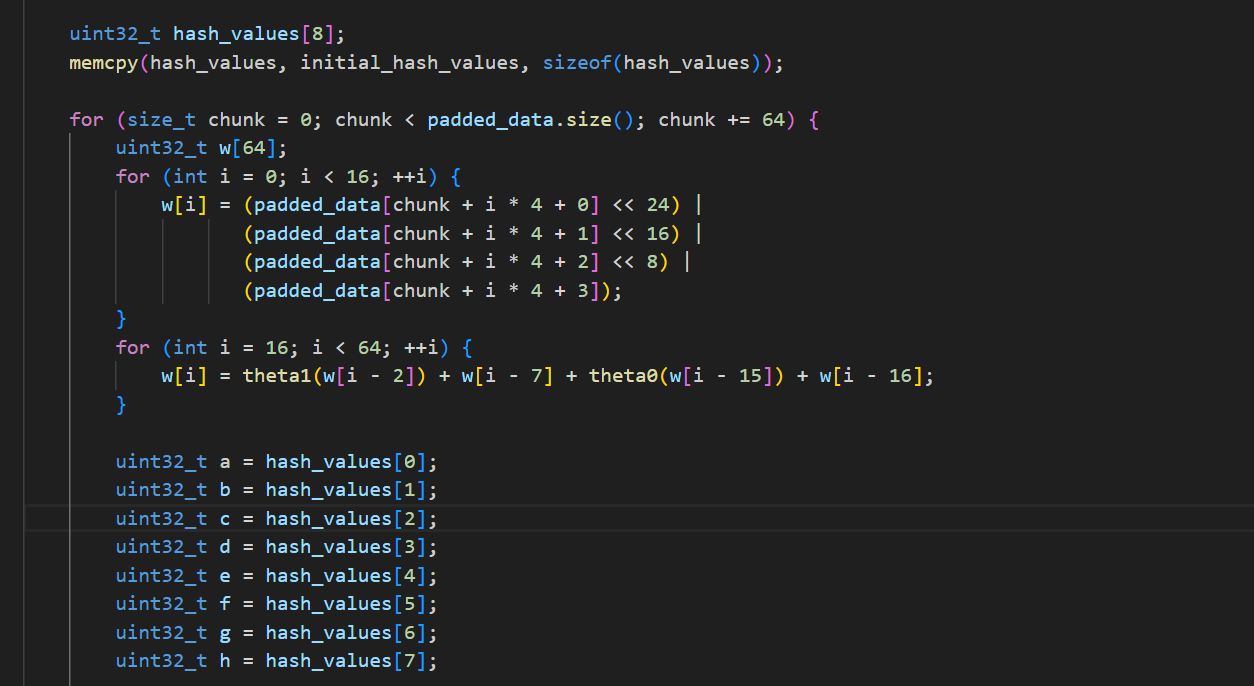
**Code Explanation**

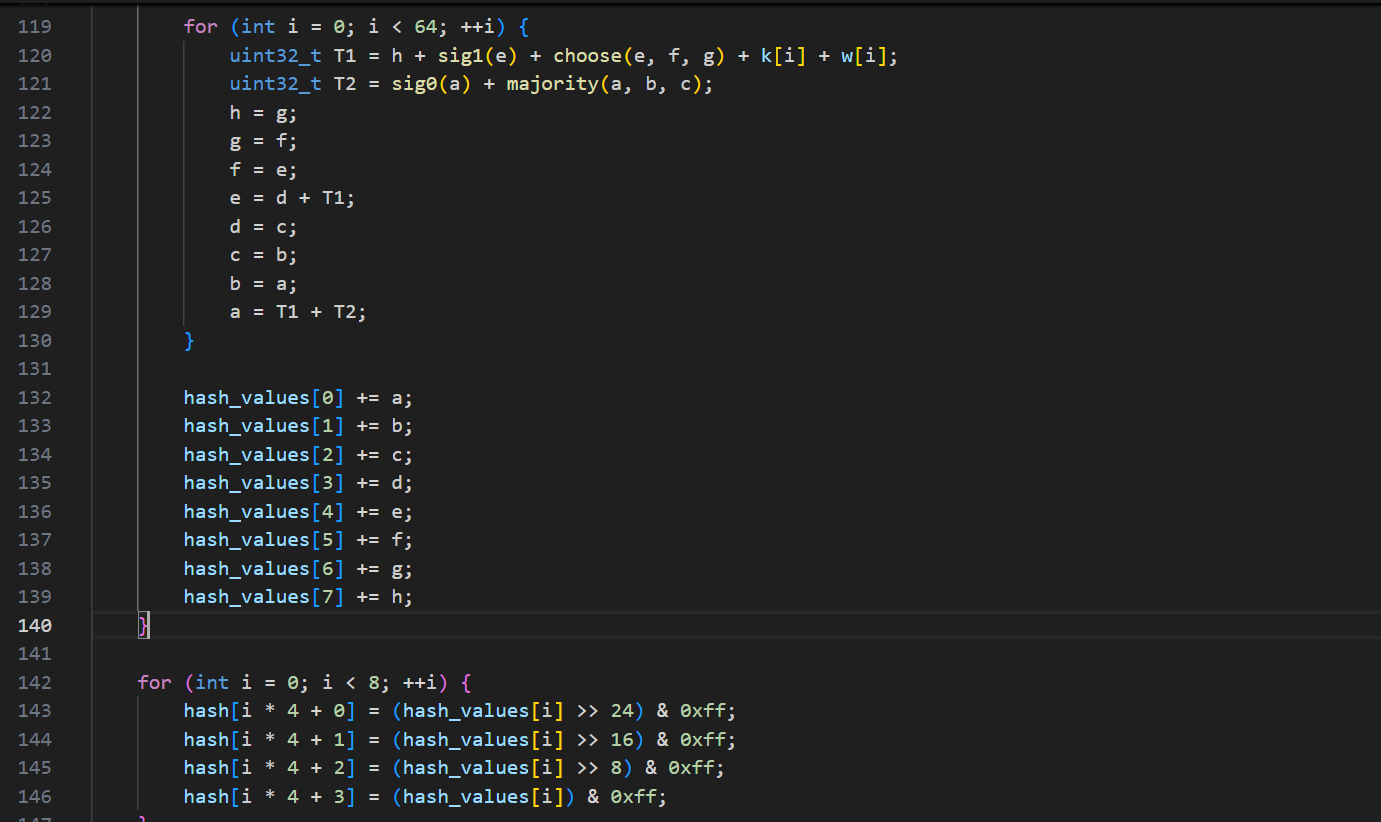
****

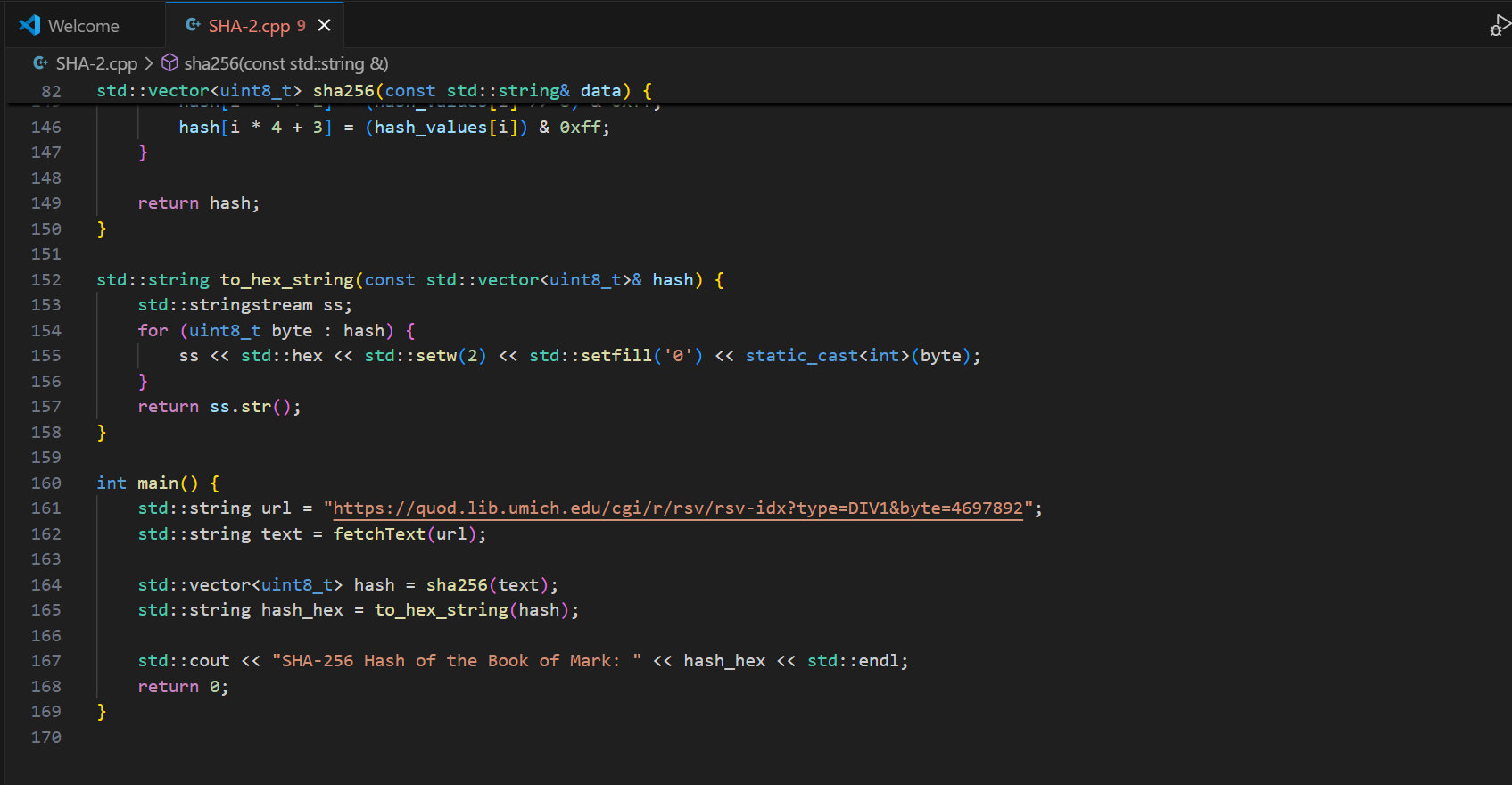
****

****

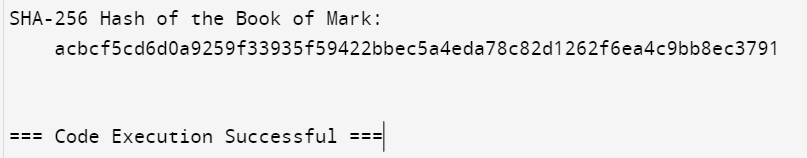




****

****

**Output:**

****

**Conclusion**

In this case, the language code is efficient to execute and apply SHA-256 to solve the problem of producing a cryptographic hash for the entire text of the Book of Mark taken from a specific URL. Next, using libcurl, the code retrieves the text data, which is, in turn, passed through a sequence of logical left shifts and bitwise reorientations as dictated by the SHA-256 structure. The hash computation process goes close to every algorithm step, like padding the message, chunking the data, and finally creating the hash. The output is a hexadecimal string of length 64 because 256 bits can be represented with precisely 64 hexadecimal digits. This implementation satisfactorily fulfills the project objective to provide a SHA 256 hash of the input text as it is pretty correct and free from processing errors in data and computational encryption. The contemplated code is very stable, conforms to the necessary protocols, and is, thus, suitable for submission.