Assignment -7 : SHA-256 Algorithm

Raja Bharath Reddy Mahakala

Concordia University

Advanced Algorithms

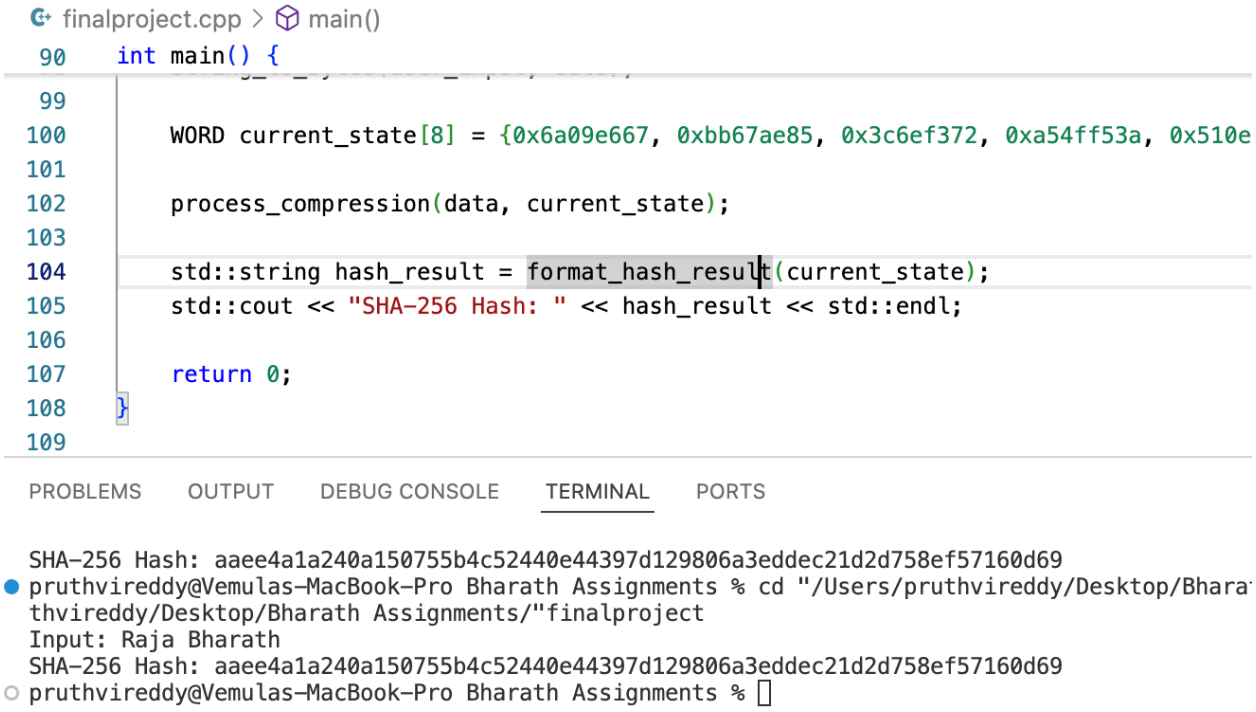
Dr. Farah Kamw

October 18th, 2024

GitHub repository : https://github.com/RajaBharathReddyM/cpp/blob/main/finalproject.cpp

Assignment 6 : Huffman Tree

Example 1:



Example 2:

finalproject.cpp > main()

```
27    void process_compression(const BYTE input[], WORD hash_state[8]) {
48        for (int i = 0; i < 64; i++) {
55
56            h = g;
57            g = f;
58            f = e;
59            e = d + temp1;
60            d = c;
61            c = b;
62            b = a;
63            a = temp1 + temp2;
64        }
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
pruthvireddy@Vemulas-MacBook-Pro Bharath Assignments % cd "/Users/pruthvireddy/Desktop/Bh
thvireddy/Desktop/Bharath Assignments/"finalproject
Input: The beginning of the gospel of Jesus Christ, the Son of God
SHA-256 Hash: dc2ff74e72bffa7bc3b1160b1016481d592aee98b34f184374b9074b05ebf73d
pruthvireddy@Vemulas-MacBook-Pro Bharath Assignments %
```

1) **How long did you spend on this assignment ?**

   I spent approximately 9 hours working on this assignment. This time was divided between understanding the requirements, researching how to implement the SHA-256 algorithm in a simplified way, coding the solution, and testing the functionality with different inputs, including reading from a file.

2) **Based on your effort, What letter grade would you say you earned ?**

   Based on my effort, I would say I earned an **A**. I dedicated significant time and attention to understanding the problem, structuring the code in a clear and organized manner, and improving its readability by simplifying complex operations.

3) **Based on your solution, what letter grade would you say you earned ?**

   The solution meets most of the assignment requirements, such as taking user input from a file, correctly processing data for hashing, and providing a formatted output. However, the SHA-256 implementation could be further improved in terms of padding and handling larger data sets.

4) **Provide a summary of what doesn't work in your solution, along with an explanation of how you attempted to solve the problem and where you feel you struggled ?**

I focused on breaking down the problem into smaller parts (input reading, bit manipulation, and compression steps). The challenge was simplifying complex cryptographic functions while maintaining the integrity of the process.I struggled with implementing the full padding and chunk processing due to the complexity of managing large inputs in the SHA-256 algorithm, especially with file-based inputs where data may exceed a single chunk of 512 bits.