Simplified SHA Digest Generation Algorithm

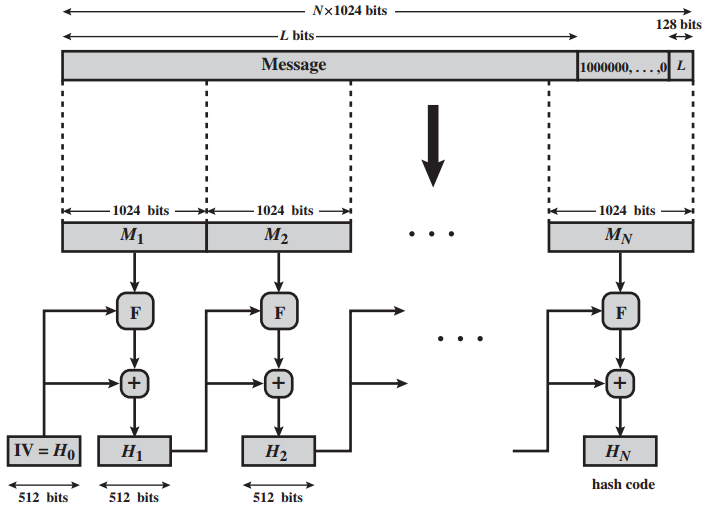
**Experiment Objective:** Deepen understanding of the concept of text digest, learn and implement key programming techniques and methods in the SHA algorithm, and create a simplified SHA digest generation algorithm.

**Experiment Content:**

Based on the simplified SHA algorithm description provided below and the explanations in class, implement the generation of digests for both Chinese and English texts. The simplified version of the SHA algorithm is described as follows:

1. The text information is padded to a length of N\*1024 bits. If the length is not enough for a complete 1024 bits, padding is done with a leading 1 followed by zeros. The last 128 bits are used to record the length of the entire padding area.

2. Using 1024 bits as a unit, iterate through the blocks for digest calculation according to the block chaining pattern shown below. H0 is the value obtained from the binary representation of the fractional part of the square root of the first eight prime numbers (refer to online sources or reference books for obtaining these values).



3.In the above pattern, a simplified round function F is used for digest calculation. The specific steps are as follows:

a) First, divide Mi into two 512-bit parts. Perform a bitwise XOR operation between the first half and Hi-1, and perform a bitwise AND operation between the second half and Hi-1.

b) Then, rotate the results from the previous step to the left and right by (i\*64 mod 512) bits.

c) Finally, perform a bitwise XOR operation between the two rotated results.

4.Based on the calculation of the simplified round function F, divide the output of the round function into 8 groups of 64 bits each. Perform a modulo 2^64 operation on each group of 64 bits and combine them to obtain Hi for the next round of calculations.

5.Repeat steps 2-3 until all blocks of the information have been processed, and obtain the final 512-bit digest. Represent the result in hexadecimal format.

6.Calculate the digest for the texts in the files "english.txt" and "chinese.txt", and make changes to some characters. Compare the digest results before and after the changes to see if the digests have changed.

Experiment Tips:

Provide the storage format for 64-bit data (8\*8 bits), and based on this format, explain the XOR operation, AND operation, and modulo 2^64 operation for two 64-bit data. This method will simplify the algorithm solving process and expression.

Experiment Report:

a) What is a hash function? What is its purpose?

A hash function converts input of variable length into output of fixed length. Its purpose is to verify if the information has been modified.

b) How do you plan to implement the storage of 64-bit data?

I used the bitset class in C++ to store the 64-bit data.

c) How can you achieve message authentication/digital signature based on the simplified SHA algorithm and the experimental results?

After obtaining the digest using the SHA algorithm, you can encrypt the digest with the sender's private key. The receiver can then decrypt the digest using the corresponding public key. If the digest can be decrypted successfully, it indicates that the message was sent by the specified sender, achieving the purpose of digital signature.

d) Provide the function declarations for each function in the rewritten code, and explain their main functionalities.

[Function declarations omitted]

e) How did you implement the XOR operation, AND operation, and modulo 2^64 operation based on the storage of 64-bit data?

Since I used the bitset class in C++ to store the bits, the XOR and AND operations can be directly performed on the bitset objects representing the data. For the modulo 2^64 operation, I performed addition on two groups of 64-bit data, converted the resulting binary bitset into a char array, used a function to calculate the value of 2^64, stored it in an int array, converted the int array into a char array, and then used a function for large number modulo to calculate the remainder by providing the two strings representing the divisor and dividend.

f) Please provide screenshots showing the results of digest calculation for "english.txt" and "chinese.txt" files, and make changes to some content. Compare the modified results with the original results (the modified content should be different from that modified by others).



It can be observed that the results have indeed changed, although the changes may not be very obvious.