MD5 algorithm in C

Research

G00346996

MD5 Introduction

* The MD5 algorithm was dveloped by Professor Ronald L.Rivest in 1991
* The MD5 “Message digest algorithm” it takes as input a message or arbiutry length and produces as output a 128-bit “fingerprint” or else a “message digest” of the input.
* There are 5 steps to follow in order to compute the message digest of the message
* **Step 1.** Append Padding bits: the input message is “padded” so that its length in bits equals to 448 mod 512. Padding is always performed, even if the length of the message is already 448 mod 512. Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448, modulo 512. In all, at least one bit and at most 512 bits are appended.
* **Step 2.** Append Length: A 64-bit representation of the length of the message is appended to the result of step 1. If the length of the message is greater than 2^64, only the low-order 64 bits will be used. The resulting message (after padding with bits) has a length that is an exact multiple of 512 bits. The input will have a length that is an exact multiple of 16 (32-bit) words.
* **Step 3.** Initialize MD Buffer: A four-word buffer (A, B, C, D) is used to compute the message digest. Each of A, B C, D is a 32-bit register. These register’s are initiliazed to the following values in hexadecimal

**Word A : 01 23 45 67**

**Word B : 89 ab cd ef**

**Word C : fe dc ba 98**

**Word D : 76 54 32 10**

* **Step 4 :**  Process message in 16 word blocks.Four functions will be defined such that each function takes an input of three 32 bit words and produces a 32-bit words and produces a 32-bit word output.

**F(X, Y, Z) == (X ^ Y) v ( ~ X ^ Z) Round 1**

**F(X, Y, Z) == (X ^ Z) v (Y ^ ~ Z) Round 2**

**F(X, Y, Z) == X Ꚛ Y Ꚛ Z Round 3**

**F(X, Y, Z) == Y Ꚛ(X ^ ~ Z ) Round 4**

* **Step 5:** Output. The message digest produced as output is A, B C, D. That is, we begin with lower-order byte of A, and end with the high order byte of D

A picture containing screenshot

Description automatically generated