Peter M Piper

April 1, 2013

Project #5 Hash Table

**Message Digest 5 (MD5)**

Message Digest 5 is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. MD5 processes a variable-length message into a fixed-length output of 128 bits.

First, the input message is broken up into chunks of 512-bit blocks; the message is padded so that its length is divisible by 512.

Second, a 128-bit state, divided into four 32 bit words, denoted A, B, C, and D, is initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, named rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation. There are four possible functions F; a different one is used in each round:

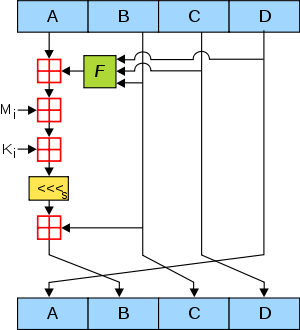
F(X,Y,Z) = (X\wedge{Y}) \vee (\neg{X} \wedge{Z})

G(X,Y,Z) = (X\wedge{Z}) \vee (Y \wedge \neg{Z})

H(X,Y,Z) = X \oplus Y \oplus Z

I(X,Y,Z) = Y \oplus (X \vee \neg{Z})

\oplus, \wedge, \vee, \neg denote the [XOR](http://en.wikipedia.org/wiki/XOR), [AND](http://en.wikipedia.org/wiki/Logical_conjunction), [OR](http://en.wikipedia.org/wiki/Logical_disjunction) and [NOT](http://en.wikipedia.org/wiki/Negation) operations.

[](http://en.wikipedia.org/wiki/File:MD5.svg)

[http://bits.wikimedia.org/static-1.21wmf12/skins/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:MD5.svg)

Figure 1. One MD5 operation. MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. *F* is a nonlinear function; one function is used in each round. *Mi*denotes a 32-bit block of the message input, and *Ki* denotes a 32-bit constant, different for each operation. [left shift](http://en.wikipedia.org/wiki/File:Lll.png)*s* denotes a left bit rotation by *s* places; *s* varies for each operation. [Addition](http://en.wikipedia.org/wiki/File:Boxplus.png)denotes addition modulo 232.