

MD5

MD5 has four “rounds” and produces a 128-bit key.

First pad the message M with a 1 and as many 0’s as needed to make the total length $\equiv 448 = 512 - 64 \pmod{512}$. The last 64 bits hold the length of the message (in bits) before padding (modulo 2^{64}). This makes the message length a multiple of 512 bits. Call the 512-bit blocks Y_0, \dots, Y_{L-1} .

MD5 uses a buffer of four 32-bit registers: a, b, c, d. These are initialized to the hexadecimal values a = 01 23 45 67, b = 89 AB CD EF, c = FE DC BA 98, d = 76 54 32 10.

The message is hashed by computing $abcd = f(Y_i, abcd)$, with the last value of abcd being the hash value.

Each round of MD5 has 16 steps.

SHA

The Secure Hash Algorithm, created by NIST and NSA, uses four rounds to produce a 160-bit message digest.

The message is first padded to a multiple of 512 bits just as in MD5.

SHA uses a buffer of five 32-bit registers: a, b, c, d, e. These are initialized to the hexadecimal values a = 67 45 23 01, b = EF CD AB 89, c = 98 BA DC FE, d = 10 32 54 76. e = C3 D2 E1 F0. (The first four constants are the same as for MD5, but stored in big-endian format rather than the little-endian format used in MD5.)

Each round of SHA has 20 steps.

Comparison of MD5 and SHA

Both add a fourth round to MD4, which had only three rounds.

The four non-linear functions of MD5 are all different. SHA has the same non-linear functions in Rounds 2 and 4.

MD5 uses 64 different constants t_i . SHA uses four different constants K_t , one per round, like MD4.

MD5 has only one symmetric non-linear function. SHA has two symmetric non-linear functions.

Both MD5 and SHA add aa to a , etc., in each step to promote rapid mixing.

MD5 has variable shifts in each round. SHA has constant shifts in each round.

SHA has an expansion of each 512-bit block. MD5 does not do this.

MD5 produces a message digest of 128 bits. SHA produces a message digest of 160 bits. Thus SHA is more resistant to a birthday attack.

The design criteria of MD5 are public. The design criteria of SHA are secret.