International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Message Digestion

Surya Prakash Dwivedi†*

†Faculty of Engineering, MGCGV Chitrakoot, MGCGV Chitrakoot MP Satna India

Accepted 05 March 2017, Available online 09 March 2017, **Vol.7, No.2 (April 2017)**

Abstract

Message Digestion is a popular technique for representing a full length message in to short form i.e. Shorter form of message in coded form but have full information about the message after decoding that text. This is popular and novel approach of public key cryptography .Using a specific cryptographic hashed formula we convert the full length message into a strings of digits and protect the integrity of a text or media and check the alternatives of all part of information. In this proposed paper I introduce various comparative message digestion technique. They typically consist of two main components: a compression function that operates in fixed-length part of input message text, and a unique mode of operation that predomination, how apply the flatten function again and again on the pieces in order to permit for random-length text inputs. Crypto-graphic hash operations are next to needs to sustain some important and draconian security features along with (but not limited to) first-premise resistance, second-preimiage resistance, collision resistance, pseudo randomness, and unpredictability.

Keywords: *Hash function, SHA-1,2,3,4, Message Digest, compressed function, collision resistance, cryptography security, Collision, Bruit force, Salt.*

Introduction

Message Digest (MD) describes a mathematical function that can take place on a variable length string. A full length of text is compressed into smaller one, that can deliver or transfer in a channel is easier and faster. Message digests are also called straight hash functions because they generates values that are tough to reverse, difficult to attack, effectively separable, and widely distributed.

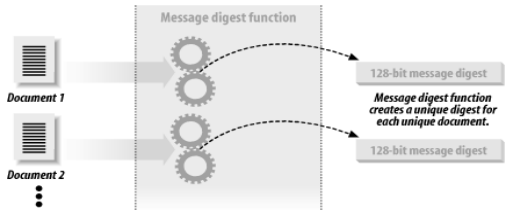


Figure 1 Digestion Function

Using cryptographic hashed function we encrypt and digest the message and transfer via secure channel, receiver decrypt the message and elaborate the text and get the original form of message. Message digest hash numbers specify some specific data consisting the private works. One message digestion is assigned to unique data content. MD can produce a change made accidentally, but it carried out the real to identify the correction as well as the others making the modification. Message digests are calculated step generation (algorithmic) digits.

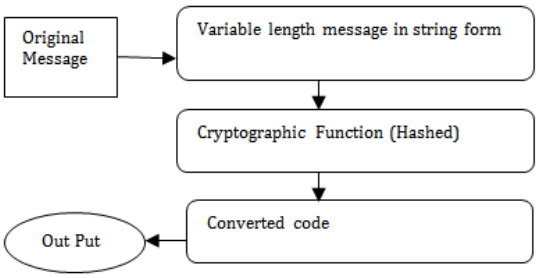


Figure 2 Message Digest Idea

This term is also known as a hash value and sometimes as a checksum. Message digest functions filter the information consisting in a file (small or large) into a single number, typically in length between 128 and 256 bits. No Hash is 100% Secure ,it means guessing the password and bit stream by applying various algorithms and bruit force technique but The best message digest planning combines such mathematical features:

- All bits of the digest text are related to its input produced by the digest function.
- If the any bit of input message is change during the digestion function the probability of change in output is occurs may be approximately 50%.

*Corresponding author: **Surya Prakash Dwivedi**

- Input and output are receives after and before passing through digest function.

There are numbers of message digestion techniques are developed but some of them are as bellow and they are widely used in various cryptographic coding fields :

MD2

MD-2, introduced by Ronald Rivest. This message digest is may be the much secure as per before developed techniques, but it takes the large comutation. That's why, MD-2 is normally less in use. MD2 generates a 128-bit digestion.

MD4

MD-4, was also introduced by Ronald Rivest. This message digestion algo. was developed as amendment of MD2. generally, MD4 has some possible weakness like infeasibility to find a 128-bit key-space).

MD5

It is also introduced by Ronald-Rivest (1996). MD5 is a modification of MD4 that covers techniques work out to make it more compatible and secure. Collision of message bits text is the weakness of algorithm. As a result it falls after some time. MD5 and SHA-1 are both used in SSL & Authentication code innovation. It is an technique i.e. used to authenticate data uniqueness through the generation of a 128-bit message. Message digest from data input which may be random in length that is prevail to be unique and secure for that message data like as a fingerprint. MD-5 is initially developed for the complex type of signature and complex large data text using a key cryptograph under a public key cryptosystem. MD5 is currently known as a standard IETF, RFC . According to these standard, it is - functionally and computationally quite to impossible that no any two messages bits that have been inputted to the MD-5 algorithm could have both output and message digest same. All Rivest's algos. have specific feature and functionalities like MD2 was optimized for 8-bit machines and MD-4 are optimized for 32-bit machines. The MD5 algorithm is an expansion of MD4, which is much faster, but assumption not always safe.

MD6

The **MD-6** Message-Digest Algorithm is a cryptographic hash function. It uses a Markel tree-like structure to allow for large parallel computation of hashes for very long inputs. The MD6 hash algorithm is a cryptographic hash algorithm developed at MIT by Ronald L. Rivest .
MD6 Mode of Operation However, MD6 makes versatility of a really different tree-based structures mode of functions that covers for huge parallelism. Whereas the Merkle-Damg˚ard development, when viewed in graph, really it is primarily a long chain, MD-6 may be rubberneck as a tree-like 16 steps development, with a 4-to-1 compress function minimizing the huge length of the text message at each level. 0 1 2 3 level. The computation begins from the bottom to top; the root node shows the final compress functional operation which gives us output as the message digest. What makes this particular mode of operation different from other tree-based structures hashing and Message Authentication Code .Each node in the tree is labeled with some prelim information that also feeds into the digest function. In particular, each node is given a unique key identifier and the root node is flagged with a bit z that recognize that it is the final digest operation used. This auxiliary key information convert (coded form) into the input of the each compression function secure the type of hash function bleach whereby an reciprocal may develop a wisely-constructed text message problem that related to some another sub-structure of another section (problem) (for example, prohibit large length-augmentation attacks).

SHA

Secure Hash function, related to MD4 and Digital Signature have some Standards (NIST's DSS). It is not much capable for small changes in coded form. SHA produces a 160-bit text digest the standards for cryptographic hashed function is followed by National Institute of Standards and Technology (NIST) for U.S. Federal Information Processing Standard (FIPS). Some of versions for SHA's are s follows as per advancement:

SHA-0

A method used in the genuine version of 160-bit hash algo. Broadcast in year 1993 covered by the name SHA, but having some better and new result using this technique the slightly next form of sha is SHA-1. In SHA-0, the 16 message bits are augmented into 80 unoriginal words with a sort of word-wise linear response shift register., and, indeed, SHA-0 collisions have been found (with effort 239239, which is highly achievable) while SHA-1 collisions still remain theoretical.

Algorithm and variant- SHA-0
Output size(bits)- 160
Internal state size(bits)- 160(5 × 32)
Block size(bits)- 512
Max message size(bits)- $2^{64} - 1$
Rounds- 80
Operations- And, X-or, Rot, Add (mod 2^{32}), Or
Security(bits)- <80(collision achieve)

SHA-1

160 bit used for Cryptographic digestion for text but it was not having new amendment in reducing attack, due to such weaknesses SHA-1is not further used after

2010. SHA-1 adds a bit round rotation to these word derivation. The extra bit rotation is makes SHA-1 unique from SHA-0; it also makes SHA-1 much stronger against collision attacks. Collision streaming is still in theoretical model.

Algorithm and variant- SHA-1
Output size(bits)- 160
Internal state size(bits)- 160(5 × 64)
Block size(bits)- 512
Max message size(bits)- $2^{64} - 1$
Rounds- 80
Operations- And, X-or, Rot, Add (mod 2^{32}), Or
Security(bits)- <80(Theoretically found)

SHA-2

Algorithm and variant- *SHA-224,SHA-256, SHA-384,SHA-512,SHA-512/224,SHA-512/256*
Output size(bits)-- 224,256, 384,512,224,256
Internal state size(bits)- 256,(8 × 32), 512, (8 × 64)
Block size(bits)-512,1024
Max message size(bits)-$2^{64} - 1$, $2^{128} - 1$
Rounds -64,80,And, X-or, Rot, Add (mod 2^{32}), Or, Shr, And, X-or, Rot, Add (mod 2^{64}), Or, Shr
Operation Security- 112,128,192,256,112,128

SHA-3

A hash function formerly called *Keccak*, chosen in 2012 after a public competition among non-NSA designers. It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family.

Algorithm and variant- *SHA3-224,SHA3-256,SHA3-384,SHA3-512,SHAKE128,SHAKE256*
Output Size(bits)- 224,256,384,512, *d* (arbitrary), *d* (arbitrary)
Internal state size(bits)- 1600,(5 × 5 × 64)
Block size(bits)- 1152,1088,832,576, 1344,1088
Max message size(bits)- Unlimited
Rounds- 24
Operations- And, X-or, Rot, Not
Security(bits)-112,128,192,256,min(d/2,128), min(d/2,256)

SHA-256, SHA-384, SHA-512

These are, respectively, 256, 384, and 512 bit hash functions designed to be used with 128, 192, and 256 bit hashing technique. These functions were promoted by NIST in 2001 for use with the AES(Advanced Encryption Standard).

Whirlpool

Whirlpool is a hashing technique developed by Paulo S. L. M. Barreto and Rijmen. It has been promoted by the NESSIE project (covers with SHA-256/384/512) and contributed as ISO/IEC 10118-3:2004.Whirlpool uses Merkle-Damgärd bloster and is a Miyaguchi-Preneel design based on a gradually changing Advanced Encryption Standard (AES). It is a sraight-way, collision-resistant 512-bit hashing technique operating on messages > 2256 bits in length.

Given a Text > 2256 bits in length, it returns a 512-bit message digestion. It sustain of the repeated application of a squeezing function, based on an given 512-bit block code that uses a 512-bit key. The round function and the key schedule are designed according to the Wide Trail brainchild.

Whirlpool applyment on 8-bit and 64-bit boaner gives benefit from the functional structure, which is not pointing toward any special platform. Even a small modification in the text message will (with an complex high probability) result in a isolated hash function, VOCAL over-true a large range variety of cryptographic complex solutions in both hardware systems and software systems.

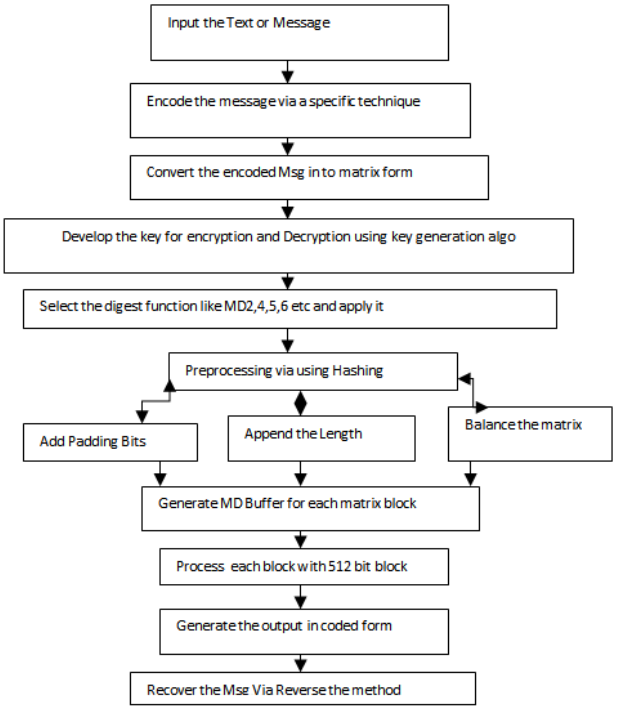
MD5 vs MD4

A fourth round has been added. Each step has a unique and add constant. The function g in round 2 is changed from (XY v XZ v YZ) to (XZ v Y not(Z)). Each step adds in the result of the previous step. The order in which input text words are fetched in rounds 2 and 3 are changed. The shift amounts in each round have been optimized. The shifts in different rounds are distinct.

SHA vs MD5

In one platform, SHA1 and MD5 look very similar. Their diagrams include bundles of bits, bit rotation, xor and special functional operation. Their implementations are generally the same length, but many of knows widely known that MD5 is fall down, but currently SHA1 is working. Some of main designable differences like -SHA-1 has a huge state: 160 bits msg vs 128 bits msg.SHA-1 has more step rounds: 80 vs 64. SHA-1 rounds have an extra bit rotation and the clubbing of state words is very less different. Bitwise clubbing functions and round constants are not same. Bit rotation counts in SHA-1 are the simillar for all rounds, while in MD5 each round has its own rotation count. The message bit words are pre-scheduled in SHA-0 and SHA-1, In MD5 each round uses one of the 16 message words as it is.

Proposed Process Flow



Some of other points we have to notice in this understandings like one-way encryption, collision, salt, Bruitforce.

One-wayEncryption

It is hard to crack this functional properties because this the straight forward procedural uni -directional scheme . MD5, SHA or Whirlpool encryption standard works is by taking a string message and then changing (coded) it into a hashed function . Then, if we check the validity and versatility of a password, the system takes the user-input password and put it into a hash. If the two hashes code is match, then it can be correct—except of this the system ever having to back - trace engineer the encoded (hashed) string. In this way, even a systems administrator would not know its own users derived secure password.

BruteForce

Encrypted hashes are wide open for brute force attacks. It always be possible when a un -authenticated person takes a well known hashed string message and then systematically (procedurally and logically) tries to guess the password till it achieve a string data that matches the hashed message. Hashed password strings can be put up from cookies or by bleaches into databases. Also, for sites un-protections against mostly used automated login , brute force can be done it by directly on the web without taking the login name and password a hashed string.

Collisions

This is the area where MD5 becomes reasonable. A collision occurs when two or more strings messages generate the same hash code. This widely increases the turns that a attacker can successfully get a password that will give to them un authorized access in to a system. MD5 has short of bits, so the possibility of a collision are greater. In fact, bleachers have compiled numbers of tables to help them crack MD5 database by giving reference to other known matches. The real thing of the matter is that it is just a matter of guessing of a password using brute force attack. With auto generated programs, algorithms and high capable hard-ware, a brute force program can go through millions of random strings matching in minutes. A big hash message code means that it takes a attacker vast to guess your password—granted, it may take months or years to do so, but it still hard to break be done.

Salt

All of the above hashing methods are best used when combined with a salt. A salt can be added to an MD5, SHA or Whirlpool string. A salt is a common technique where a system joins a string data to a password before to encryption. With this versatility, it is quite hard for a hacker to bleach a password without understanding and knowing the salt. To develop a salt more secure, you can create a unique salt for each and every user, when we are develop and apply a system-level salt.

Conclusion

More bits ,a hash contains i.e. the more secure. MD5 is a 128-bit data string, SHA-1 is a 160-bit data string and Whirlpool is a 512-bit data string. On behalf of these features, it is decided that Whirlpool is stand superior to both SHA-1 and MD5 digestion technique using hashed function. Using a Whirlpool encryption might be difficult - especially for those who are managing a 512-bit large string , it is a quite ungainly. Instead of, you should use a salt method for encryption, In respect of what are you using for encoddation. Unless untill someone trace your source code, they would face much difficulties if hacker tries in it in short I can say that unable to break (hack) your user passwords using brute force and any other methods.

References

W. Diffie and M. E. Hellman, (1976) New Directions in Cryptography , *IEEE Transactions on Information Theory*, Vol. 22, No. 6.International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.1

M. E. Hellman, (1978), An Overview of Public-Key Cryptography, *IEEE Transactions on Communications*, Vol. 16#6, pp. 24-32.

T. ELGamal,(1985), A Public Key Cryptosystem and a Signature Scheme Based on Discrete

Russell Impagliazzo, Leonid A. Levin, and Michael Luby,(1989),Pseudo-random Generation from one-way functions (Extended Abstracts), STOC, ACM, pp. 12–24.

R.L. Rivest.(1991), The MD4 message digest algorithm, Advances in Cryptology, Crypto‟90, Springer-Verlag, pp. 303-311

R.Rivest,(1992),The MD5 message-digest algorithm, IETF RFC 1321

B. den Boer and A. Bosselaers, (1992),An attack on the last two rounds of MD4, Advances in cryptology, *Proc. Crypto'91, LNCS 576, J. Feigenbaum, Ed., Springer-Verlag,*192, pp.194-203.

E. Biham, and A. Shamir,(1993),Differential Cryptanalysis of Full 16-Round DES, *Advances in*

Cryptology- CRYPTO '92 Proceedings, Springer-Verlag.

H. Dobbertin , A. Bosselaerand B. Preneel(1996) RIPEMD-160: Astrengthened Version of RIPEMD, Fast Software Encryption, LNCS 1039,pp. 71-92, Springer-Verlag.

NIST,(1993),Secure Hash Standard, FIPS PUB 180, May Zhao Yong-Xia, Zhen Ge. 2010. MD5 Research,IEEE, pp. 271-273

C.Kaufman,September,(1993),DASS-Distributed Authentication Security Service, *RFC 1507*.

B. den Boer, and A. Bosselaers,(1994), Collisions for the compression function of MD5,*Advances in Cryptology, Proc. Eurocrypt'93, LNCS 765, T. Hellseth, Ed., Springer Verlag,*194,pp.293- 304.

H.Dobbertin,(1996),Cryptanalysis of MD5 compress. *Announcement on Internet*.

W.STALLINGS,(1997), Cryptography and Network Security, 2nd ed..New York: Prentice-Hall.

Hans Dobbertin,(1998),Cryptanalysis of MD4 *Journal of Cryptology* Volume-11, Issue 04, pp 253-271.

Deepakumara, H.M. Heys, and R. Venkatesan, 2001,FPGA implementation of MD5 hash algorithm, IEEE , vol.2, pp. 919 – 924.

DR. H. Handschub, Dr. H. Gilbert, (January2002), Evaluation Report Security Level of Cryptography – SHA-256, Technical Report, Issy-les-Moulineaux.

NIST,(2002),Secure Hash Standard (SHS), FIPS PUB 180-2.

Chiu-Wah Ng, Tung-Sang Ng and Kun-Wah Yip.(2004), A UNIFIED ARCHITECTURE OF MD5 AND RIPEMD-160 HASH ALGORITHMS. IEEE, pp.889-892.

H. S. Kwok Wallace and K. S. Tang,(2004), A Chaos-Based Cryptographic Hash Function for Message Authentication, International Journal of Bifurcation and Chaos (IJBC), Vol. 15, pp. 4043-4050.

X. Wang, H. Yu,(2005),How to Break MD5 and Other Hash Functions, Advances in Cryptology, proceedings of EUROCRYPT 2005, Lecture Notes in Computer Science 3494, pp. 19–35.

J. Lee, D. Chang, E. Lee, H. Kim, D. Hong, J. Sung, S. Hong, and S. Lee,(2005,)A new 256-bit hash function DHA-256 – Enhancing the security of SHA-256, Presented at NIST Cryptographic Hash ,Workshop.

W. Stalling ,(2005),Cryptography and Network Security Principles and Practices, Prentice Hall, Fourth Edition, P 353.

T.S. Ganesha, M.T. Fredericka, T.S.B. Sudarshanb, and A.K. Somania, (2007) Hashchip: A shared-resource multi-hash function processor architecture on FPGA, The VLSI journal, vol. 40.

pp. 11-19.

Praveen_Garavaram,(2007),Cryptographic Hash Functions: Cryptanalysis Design and Application, Ph.D thesis, Information Security Institute, Faculty of Information Technology, Queensland University of Technology.

H. Mirvaziri, K.Jumari and M.Ismail (December 2007),A new Hash Function Based on Combination of Existing Digest Algorithms, The 5th Student Conference on Research and Development, SCOReD 2007.

Hancheng LIAO.(2008), Image Retrieval Based on MD5. IEEE, pp. 987-991

Y. Sasaki, L. Wang, and K. Aoki.,(2009),Preimage Attacks on 41-Step SHA-256 and 46-Step SHA-512, IACR Cryptology ePrint Archive, Vol. 2009.

M. Lamberger and F. Mendel,(2011) ,Higher-order differential attack on reduced SHA-256, Cryptology ePrint Archive, Report 2011/037.

Wikipedia,MD5,[EB/OL].http://en.wikipedia.org/wik i/MD5.

A. kasgar, J. Agrawal and S. Sahu, (March 2012)

New Modified 256-bit MD5 Algorithm with SHA Compression Function, International Journal of Computer Applications (0975 – 8887) ,Vol.42,No.12, L. Chen and Gaithersburg,(2012), Communication System Security, CRC Press.

M.Juliato and C.Gebotys,(July2013)A Quantitative Analysis of a Novel SEU-Resistant SHA-2 and HMAC Architecture for Space Missions Security, IEEE Transactions on Aerospace and Electronic Systems, Vol. 49, pp. 1536-54.

G. Gupta, S. Sharma,(2013),Enhanced SHA-192 Algorithm with Larger Bit Difference, International Conference on Communication Systems and Network Technologies (CSNT)