ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

A Comparative Study on Different Hashing Algorithms

C.G Thomas, Robin Thomas Jose

Assistant Professor, Dept. of I.T., AIMIT, St. Aloysius College (Autonomous), Mangalore, Karnataka, India

III Semester M.Sc. Software Technology, AIMIT, St. Aloysius College (Autonomous), Mangalore, Karnataka, India

ABSTRACT: Passwords play an important role in daily life in various computing applications and play a critical role in online authentication. The main aim for using passwords is to restrict unauthorized users to access the system. Passwords are necessary to provide the security to the users because of many flaws in the conventional password systems. Unfortunately, passwords suffer from two intractable problems: password cracking and password theft. So we use Password hashing to protect password. Password hashing technique allows users to remember simple passwords and have them hashed to create secure passwords. This paper describes widely used hash algorithms and comparative analysis of different hash algorithms which are used in password hashing for making awareness of attacks and selection of hashing method in a particular scenario.

KEYWORDS: MD5, SHA-1, SHA-2, SHA-3, hash

I. INTRODUCTION

In current scenario, where the number of internet users is widely increasing, internet has become the primary medium of communication. So, user's data attains the greatest priority in the field of data communication. To keep the network usage reliable, data integrity, data authentication, non-repudiation, data confidentiality is of utmost importance. Passwords is one of the most common security method to authenticate user's identity in online. They provide a powerful guard against unauthorized access to systems and data. Password occupy the important position in user authentication because other authentication factors something you have and something you are (e.g. Fingerprint) not gained a wide on the Internet, primarily because of their limited flexibility, high cost and restricted portability.

On the other side, passwords are simple, easy to implement and inexpensive. Despite their prevalence Password Hashing security depends passwords on protecting passwords from being stolen. A strong password should be sufficiently long, random, and hard to discover by crackers. However, no matter how strong they are, passwords are also vulnerable to theft like phishing and shoulder surfing.

A technique to obtain secure online passwords is password hashing, where hashed passwords are sent to databases or remote websites. Hashing is an important technique used for secure communication in the presence of eavesdroppers. It provides all the paramount aspects of information security such as integrity, authentication and confidentiality. Password hashing is lightweight and convenient to use and can defend against phishing attacks.

II. STUDY OF HASH ALGORITHMS

MD5 Algorithm

MD5 is one of the widely used hashing algorithms developed by Ronald Rivest in 1991. MD5 is a successor version of MD4. MD-5 is broken in regard to collisions, but not in regard of pre-images or second-pre-images. It produces 128 bits a fixed length hash values. MD5 is very collision resistant. In 1996 attacks on MD-5 were published.

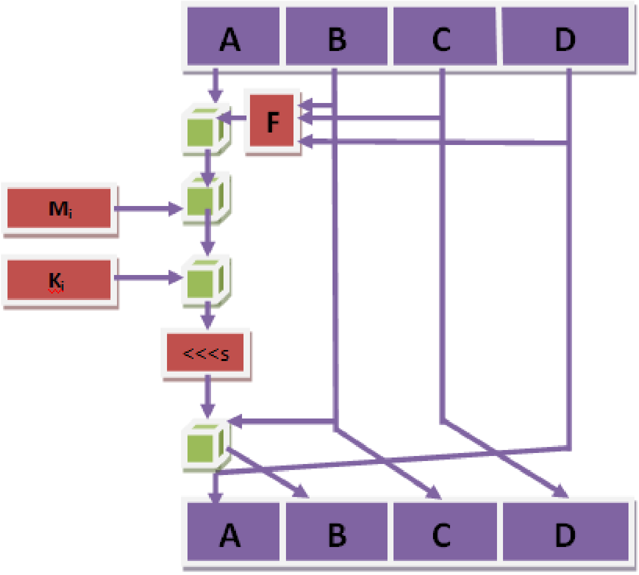

Fig.1 MD5 Algorithm

MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. F is used in each round which is nonlinear function. M_i denotes the message input of 32 bit, and K_i which is different for each operation and is 32-bit constant. s is a left bit rotation by s.The main algorithm MD5 is divided into A, B, C and D which operates on 128 bit where each carry 32 bits.These are constants which are initialized into,

A = 0x67452301
B = 0xEFCDAB89
C = 0x98BADCFE
D = 0x10325376

The processing consists of four same stages and each stage is composed of similar 16 operations. The figure denotes one such kind of operation.
F (B,C,D)=(B AND C) OR (NOT B AND D)
G (B,C,D)= (B AND D) OR (C AND NOT D)
H (B,C,D)= B XOR C XOR D
I (B,C,D)= C XOR (B OR NOT D)

The output is called a hash value, a fingerprint or a message digest.
The advantages and disadvantages of MD5.

- Advantages of MD5
  - Fast computation
  - Collision resistance
  - Is in widespread use
  - Provides a one-way hash
- Disadvantages of MD5
  - Has known security flaws and vulnerabilities
  - Is less secure than the SHA-1 algorithm

MD5 was designed especially to run on 32-bit processors. A 2013 attack by Xie Tao, Fanbao Liu, and DengguoFeng breaks MD5 collision resistance in 218 times.

Secure Hash Algorithm (SHA)
SHA was created by the NIST in 1993. Soon after its creation a flaw was uncovered. It is another cryptographic hash algorithm generates a message digest of fixed 160 bits. It takes 80 rounds.

a) SHA-1
It works similar to MD5 and produces a 160-bit message digest. It is the most widely used algorithm for integrity. The main reason for its popularity among existing algorithms is its time efficiency and its robustness. It was no longer used for most cryptographic uses after 2010 attack by Marc Stevens, which can produce hash collisions with a complexity of 261 operations.

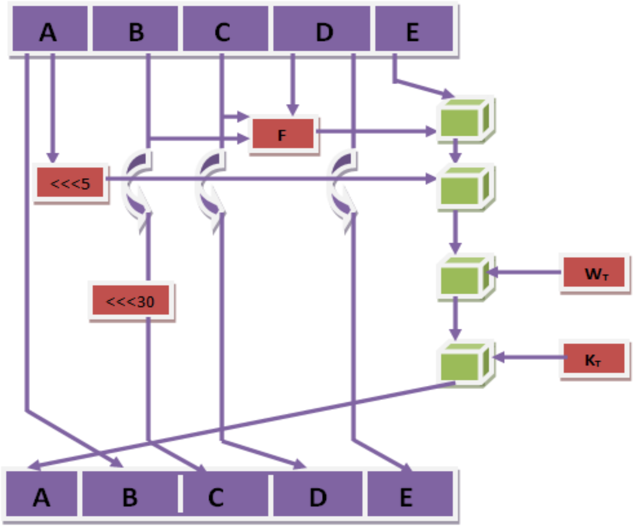

Fig.2 SHA-1 Algorithm

Here A, B, C, D and E denotes the 32-bit words in one iteration of SHA-1 function. F varies and d it is a nonlinear function. N varies for each rotation and denotes a left side rotation. Wt. is the expanded message word of round t. K_t denotes the addition modulo and is a constant. H0, h1, h2, h3, and h4 denotes 32 bit divisions of SHA Algorithm.
h0 =0x67452301
h1= 0Xefcdab89
h2=0x98BADCFE
h3=0x10325476
h4=0XC3D2E1F0
Based on F function message it consist of similar 80 operations. Modular addition and left rotation.

A=h0, B=h1, C=h2, D=h3, E=h4

From iteration 16 to 79

w[i]= (w[i-3] xor w[i-8] xor w[i-14] xor w[i-16]) leftrotate1

The possible F functions:
F(B,C,D)=(B AND C) OR (NOT B AND D)
G(B,C,D)=B XOR C XOR D
H(B,C,D)=(B AND C) OR (B AND D) OR (C AND D) [5]
I(B,C,D)=B XOR C XOR D

SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999 , (0 <= t <= 19)
K(t) = 0x6ED9EBA1, (20 <= t <= 39)

K(t) = 0x8F1BBCDC ,(40 <= t <= 59)
K(t) = 0xCA62C1D6, (60 <= t <= 79)

- Advantages of SHA-1
  - Longer hash value compared with MD5
  - Collision resistant
  - Is in widespread use
  - One way hashing
- Disadvantages of SHA-1
  - Slower computation comparing MD5
  - Known security vulnerabilities

b) SHA-2

It was also formulated by the NSA. It has two hash functions SHA-256 and SHA-512. SHA-256 uses 32-bit words where SHA-512 uses 64-bit words. None of them have proven completely breakable but still these algorithms are not preferred to ensure the integrity because they are not time efficient as SHA-1. It is found that, none of the hash algorithm is secure to ensure the integrity except SHA-2 but it is found that it is not time efficient.

c) SHA-3

It was proposed in 2012 NSA after a public competition among non-NSA designers. It is different in internal structure and supports the same hash lengths as SHA-2. It is not vulnerable to length extension attacks, which affect all M-D hashes like MD5, SHA-1, SHA-2. There are a few reasons one would choose to support SHA-3 or even SHA-2 over SHA-1. First, there are theoretical attacks against SHA-1 that reduce the difficulty of finding collisions. These attacks are still impractical, and SHA-1 can be relied on for strong security for hashes and signatures that expire in a few years' time. SHA-2 is similar to SHA-1, but has not been shown to be susceptible to the same attacks.

III. COMPARATIVE ANALYSIS

In this section, we have compared all the algorithms with each other which are used to ensure integrity over data but most of them are proven breakable.

Table 1: Comparison between MD5 and SHA hash algorithms on general properties basis.

Name Of The Algorithm	Size Of Output	Rounds	Collision Status
MD5	128	60	YES
SHA	160	80	YES
SHA-1	160	80	YES
SHA-2	256/512	60/80	THEORITICAL
SHA-192	192	80	NO
SHA-192	192	64	No
SHA-3	256/512	24	NO

SHA-1 and SHA-2 are less preferable compare to SHA-3 because SHA-2 and SHA-1 is not time efficient as SHA-3.

Table 2: Comparison between MD5 and SHA

Features	MD5	SHA
Security	Less Secure than SHA	More Secure
Length Of Message Digest	128 Bits	160 Bits
No. Of Attacks Needed To Find Original Message	2^{128} bit operations Required	2^{160} bit operations required
Attacks to try and find two messages producing the same MD	2^{64} bit operations Required	2^{80} bit operations required
Speed	Faster, 60 iterations	Slower, 80 iterations
Successful attacks so far	Attacks reported some extend	No such attack reported

Table 3: Timing comparison between different SHA-1, SHA-192[1] and SHA-192[2]

File Size	SHA-1	SHA-192[2]	SHA-192[1]
1KB	0.015	0.14	0.068
5KB	0.182	1.501	0.503
10KB	0.655	2.605	1.288

It is clear that SHA-1 is more time efficient than SHA-192[2] and SHA-192[2]

Table 4: MD5 and SHA Execution

Test String	MD5	SHA-1	SHA-512
“”	1d76382e861d2df96647216b26d38948	dd29ecf524b030a65261e3059c48ab9e1ecb2585	64d24560970ca14d349bea0e7d2526d4754bf3283568ab4dd602bd79eb454dc3657d5bb6f9a30c90ea98d9600ebd0fb45d582f4cae3f8e3c50b0e8fb18059892
abcdefghijklmnopqrstuvwxyz	c3fcd3d76192e4007dfb496cca67e13b	32d10c7b8cf96570ca04ce37f2a19d84240d3a89	4dbff86cc2ca1bae1e16468a05cb9881c97f1753bce3619034898faa1aabe429955a1bf8ec483d7421fe3c1646613a59ed5441fb0f321389f77f48a879c7b1f1
123456789	25f9e794323b453885f5181f1b624d0b	f7c3bc1d808e04732adf679965ccc34ca7ae3441	d9e6762dd1c8eaf6d61b3c6192fc408d4d6d5f1176d0c29169bc24e71c3f274ad27fcd5811b313d681f7e55ec02d73d499c95455b6b5bb503acf574fba8ffe85
aimit	c884202c3c2ccf128cd315ac632593fb	5eb095afbd1a219674778628ece963f349064287	841498bf3a202d8fc473f764072db7a7d3af8899135a2e466e77691593507e61e75d7f1c6e99503615dbcb7f4466b26d97c464426d646e0b99b3e3d726e377ab
AIMIT	0e616b0b6fc9242e8ea9824c470c1aa4	9755dd7a3f3178d2cf851f850ce8359c92223be9	7d1c95b5a226f4b395f8a122a4383d34e1f931f3946fb45e0d5de1dc94ea699d8bb3780fc36a5c709bc3202b3ca3d776e10ced3fd82f1809b63fb420b07b4163
123456789aimit	66bca043599ecaba74e7f9c33a408b5a	d3947692118d0fdf2889b482176b5b5ce4515250	a7ba49ed98da2f2ea87bd6f302a5f6b990f2a109f992db0a7fa784b63c05caa7f26f5266c5823f2d83cd3627b04a5e74f89040e90c01b2cbd05ab7c6d644e347

Table 5: Similarities between MD5 and SHA Algorithms.

Similarities	MD5	SHA
Padding	✓	✓
Message bits	✓	✓
Members of hash family	✓	✓
Resource utilization(same)	✓	✓
Fingerprint	✓	✓

IV. CONCLUSION

This comparative study helped us to understand that the SHA algorithm plays a very important role in comparison to MD5 because SHA algorithms' performance rate is comparatively better than other cryptographic hash algorithm functions. As a future work, we propose to implement double hashing to store passwords so as to get the best of both worlds. More information would be built up which could be used as a motive in the technological testing of the cryptographic hashing algorithms. This would result in an ultimate result of using both hashing and securing password much more efficiently.

REFERENCES

1. Professor Guevara Noubir, Fundamentals of Cryptography: Algorithms, and Security Services.
2. Wikipedia, the free encyclopedia.
3. Jerry li, MD5 Message Digest Algorithm. San Jose University, Computer Science department
4. Andrew S. Tanenbaum, Pearson Publication, Fourth edition, Computer Networks.
5. MD5 is faster than SHA-1.Journal Of Omnifarious-Myth.
6. Ruth Betcher, Secure Hashing Algorithm.
7. http://www.miraclesalad.com/webtools/md5.php
8. http://www.sha1-online.com/