International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2584
Volume 3, Issue 05, May-2017

Review Paper on Secure Hash Algorithm With Its Variants

Aradhana[1], Dr. S. M. Ghosh[2]

[1]Research Scholar in Dr. C.V. Raman University Bilaspur, [2] Professor in Dr. C.V. Raman University Bilaspur

Abstract: The Cryptographic hash function is produce irreversible and unique hash value. It provides greater resistance against attack .The variants of SHA algorithm are designed differently named are SHA-0, SHA-1, SHA-2, and SHA-3. This is a review paper which includes the comparisons between different secure hashing algorithms.

Keywords:-Hash, SHA, Data integrity, Massage Authentication, Digital Certificate.

1. Introduction

A cryptographic hash function is a hash function. It takes an arbitrary block of input string and returns a fixed-size bit of output string. The cryptographic hash values differ such that any accidental or intentional change to the data. The data to be encoded are often called the message and the hash value is called the message digest. The SHA Algorithm is used in digital certificate as well as in data integrity and massage authentication.SHA is a fingerprint that specifics the data and was developed by N.I.S.T. as a U.S. Federal Information Processing Standard (FIPS), is intended for use with digital signature applications [1].

As a wide use of internet day by day it is needed that a proper file has been download from peer to peer (P2P) servers and network. Due to present of same name file it is quite difficult to find the original so message digest plays an important role in such type of downloads. These type of file may be bound with message authentication code which proves that the source is verified otherwise it shows the warning that verified source not found or vice versa

Applications of Hash Functions Applications of hash functions:

- Message authentication: used to check if a message has been modified.
- Digital signatures: encrypt digest with private key.
- Password storage: digest of password is compared with that in the storage; hackers cannot get password from storage
-
- Key generation: key can be generated from digest of pass-phrase; can be made computationally expensive to prevent brute-force attacks.
- Pseudorandom number generation: iterated hashing of a seed value.
- Intrusion detection and virus detection: keep and check hash of files on system

1.1 SHA-0

SHA -0 is160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1.

1.2 SHA-1

SHA-1 produces a message digest based on principles MD4 and MD5. SHA-1 differs from SHA -0 only by a single bitwise rotation in the message schedule of its compression function.SHA – 1 produces a 160 bit hash value known as message digest. This hash value is rendered as hexadecimal number .It is 40 digits long.

Step 1:- Bits Padding:-Add Padding to the end of the genuine message length is 64 bits and multiple of 512.
Step2:- Appending length: - In this step the excluding length is calculated.

Step3:- Divide the Input Text into 512-bit blocks :- We divide the input in the 512 bit blocks
Step4:-Initialize chaining variables. In this step we initializing chaining variables here we initialize 5 chaining variables of 32 bit each=160 bit of total.
Step5:-Process Blocks
1) Copy the chaining variables
2) Divide the 512 into 16 sub blocks
3) Process 4 rounds of 20 steps each

SHA-1: The Function H Compression function operates as follows:

- Each round has 20 steps which replaces the 5 buffer words (A,B,C,D,E) with: (E + f(t,B,C,D) + (A << 5) +Wt +Kt),A,(B << 30),C,D)
- t is the step number
- f(t,B,C,D) is nonlinear function for round
- Wt is derived from the message block
- Kt is a constant value derived from sin

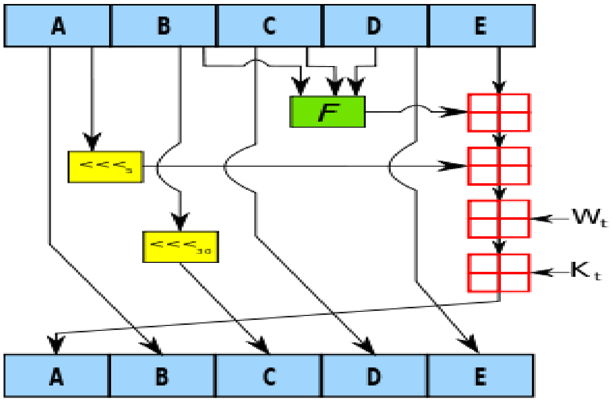


Fig 1:-One SHA -1 iteration

SHA-1 forms part of several widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME, and IPsec. SHA-1 hashing is also used in distributed revision control systems

1.3 SHA -2

SHA-2 includes significant changes from its predecessor SHA-1. The SHA-2 family consists of six hash functions .they are SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224,SHA-512/256.SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds[7].

SHA-224 and SHA-384 are simply truncated versions of the first two, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512.

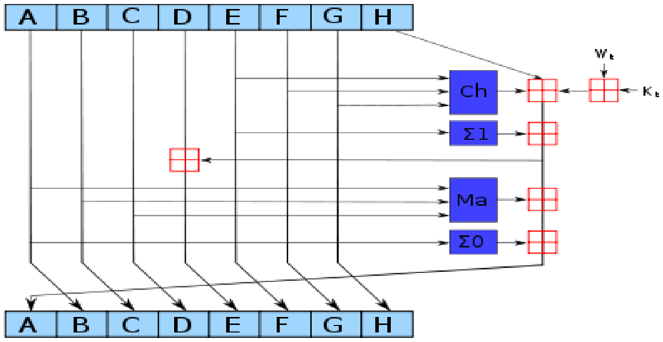


Fig 2:-One SHA -2 iteration

SHA-256 partakes in the process of authenticating Debian software packages and in the DKIM message signing standard. SHA-512 is part of a system to authenticate archival video from the International Criminal Tribunal of the Rwandan genocide. SHA-256 and SHA-512 are proposed for
use in DNSSEC. Unix and Linux vendors are moving to using 256-bit and 512-bit SHA-2 for secure password hashing.

1.4 SHA -3

SHA-3 uses the sponge construction in which data is "absorbed" into the sponge and then the result is "squeezed" out. In the absorbing phase, message blocks are XORed into a subset of the state, which is then transformed as a whole. In the "squeeze" phase, output blocks are read from the same subset of the state, alternated with state transformations.

In SHA-3, the state consists of a 5 × 5 array of 64-bit words, 1600 bits total. Keccak is also defined for smaller power-of-2 word sizes w down to 1 bit (25 bits total state). Small state sizes can be used to test cryptanalytic attacks, and intermediate state sizes (from w = 8, 200 bits, to w = 32, 800 bits) can be used in practical, lightweight applications.

The block transformation is a permutation that uses xor, and and not operations, and designed for easy implementation in both software and hardware
Block permutation:

- Defined for $w = 2\ l$ bit (w=64, l= 6 for SHA-3)
- State = 5×5×w bits array: notation: a[i, j, k] is the bit with index (i×5+ j)× w+k
- Block permutation function = 12+2×l iterations of 5 subrounds ($f = \iota \circ \chi \circ \pi \circ \rho \circ \theta$):
    - θ: xor each of the 5×w columns of 5 bits parity of its two neighbours.
    - ρ: bitwise rotate each of the 25 words by a different number, except a[0][0] .
    - π: Permute the 25 words in a fixed pattern.
    - χ: Bitwise combine along rows.
    - ι: xor a round constant into one word of the state.

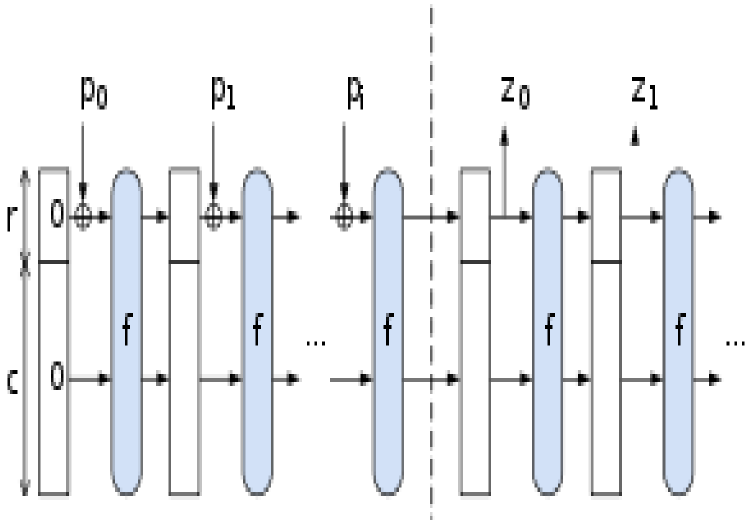


Fig 3:-One SHA -3iteration

The SHA-3 family consists of four cryptographic hash functions SHA3-224, SHA3-256, SHA3-384 and SHA3-512 and SHA 3- 512 has two extendable output functions SHAKE128 and SHAKE256.It is different in internal structure extension attacks, which affect all MD hashes like MD5, SHA-1, and SHA-2.

2. LITERATURE REVIEW

A several analysis by numerous researches is work on SHA and its variants. The outline of the analysis is reviewed as follows:

Author	**Year**	**Title**	**Outcomes**
Piyush Garg, and Namita Tiwari	2012	Performance Analysis of SHA Algorithms (SHA-1 and SHA-192): A Review	It has been observed that SHA-160 and SHA-192 are better in respective field. SHA-192 algorithm is more secure in terms of the number of brute force attacks needed to break it and SHA-160 is fast when compared to the other secure hash algorithms.
Priyanka Vadhera and Bhumika Lall	2014	Review Paper on Secure Hashing Algorithm and Its Variants	SHA is more secure than MD5 but on the other hand MD5 is more fast than SHA on 32 bit machines.
Piyush Gupta, and Sandeep Kumar	2014	A Comparative Analysis of SHA and MD5 Algorithm	SHA is more secure than MD5 but on the other hand MD5 is more fast than SHA on 32 bit machines.
Snigdha Soni and Pratap Singh	2015	Secure and Efficient Integrity Algorithm based on Existing SHA Algorithms	This paper discussed one of the problems faced in integrity algorithms that all existing algorithms are either proven breakable or not time efficient
C.G Thomas and Robin Thomas Jose	2015	A Comparative Study on Different Hashing Algorithms	SHA algorithms' performance rate is comparatively better than cryptographic hash algorithm functions

3. PARAMETERS USED FOR COMPARSION OF DIFFERENT SHA ALGORITHMS

Variants of SHA algorithms are differ in both construction and how the resulting hash is created from the original data and in the bit-length of the signature primarily. We focus on the bit-length as the important.

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Word size (bits)	Rounds	Bitwise operations	Collisions found	Example Performance (MiB/s)
SHA-0		160	160	512	$2^{64} - 1$	32	80	and, or, xor, rot	Yes	-
HA-1		160	160	512	$2^{64} - 1$	32	80	and, or, xor, rot	Theoretical attack	192
SHA-2	SHA-224 SHA-256	224 256	256	512	$2^{64} - 1$	32	64	and, or, xor, shr, rot	None	139
	SHA-384 SHA-512 SHA-512/224 SHA-512/256	384 512 224 256	512	1024	$2^{128} - 1$	64	80	and, or, xor, shr, rot	None	154
SHA-3	SHA3-224 SHA3-256 SHA3-384 SHA3-518	224 256 384 512	1600 (5x5x64)	1152 1088 832 576	unlimited	64	24	and, not, xor, rot	None	-
	SHAE 128 SHAE 256	d (arbitrary)		1344 1088					None	-

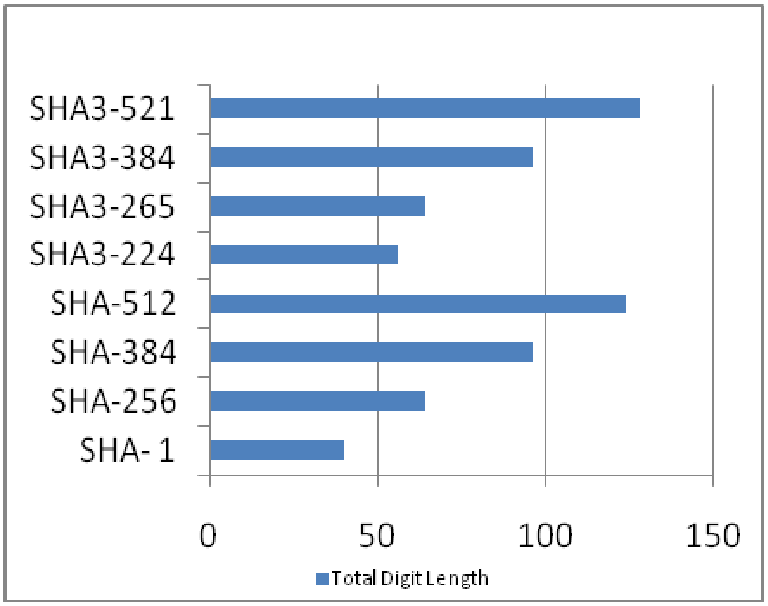
4. EXAMPLE EXECUTION

These three strings hash value, password, cryptography were taken as sample string for generating massage digest for SHA -1,SHA-2 and SHA-3. The following results have come out using JAVA tool. This proves that new version (SHA-2 and SHA-3) is more secure than SHA-1 but on the other hand SHA-1 is relatively faster than its versions .

TEST STRING	SHA - 1	SHA 256	SHA 3-512
hash value	d79c69966efe62977628f804bdaa8d0b823e09e7	d13baa5b91ea95462b1d26b3a3b1874b6be955af5a9630d1d1d0ea9bb981bf0e	c144557cbbff73c70b50c5b28bdf75bcb0ec3f3b00b0da012773f58322bab04d72ede150fc0451470db846f1a79bb1296c9bef09a01157ca1a1514cbff0474f2
password	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8	e9a75486736a550af4fea861e2378305c4a555a05094dee1dca2f68afea49cc3a50e8de6ea131ea521311f4d6fb054a146e8282f8e35ff2e6368c1a62e909716
cryptography	48c910b6614c4a0aa5851aa78571dd1e3c3a66ba	e06554818e902b4ba339f066967c0000da3fcda4fd7eb4ef89c124fa78bda419	d95d0ba1e24a97716ba736a33a545bb93515a1b95ebf0d120807ee628bfdeb548926eb23a3d74b9e62e8c1770d1441e79136bea681c5e4306cfeec4fd43d436b

5. RESULT

The following chart shows the length of the output digit of SHA and its variants.



5. CONCLUSION

This research paper consists of comparisons between different secure hashing algorithms and its variants. Each algorithm takes the time for the computation of hash value. By computing the time required from each of these algorithm and finding the algorithm which will require the less amount of time for computation of the hash value As a future work, we propose to implement double hashing .We can combine the best secure hashing algorithm for network security so as to increase the security of the data being sent in clouds.

6. REFERENCES

[1] Kasgar A. K., Agrawal Jitendra, Sahu Santosh, 2012, “New Modified 256-bit MD5 Algorithm with SHA Compression Funct ion”, IJCA (0975–8887) Volume 42 (12) , pp47-51.

[2] Rivest R., 1992, “The MD5 Message-Digest Algorithm,”RFC 1321,MIT LCS and RSA Data Securit y, Inc.

[3] Kahate, Atul, 2003, "Cryptography and Network Securit y", TataMcGraw-Hill ,India.

[4] William Stallings, Cryptography and NetworkSecurity: Priciples and Practice,5th Edit ionPrent ice Hall; 5 edit ion (January 24, 2010).

[5] Vandana P., V.K Mishra, Architecture based on MD5 and MD5-512Bit Applications , IJCA(0975 – 8887)Vol. 74– No.9, July 2013.

[6]Piyush Gupta et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4492-4495

[7]www. http://www.sha1-online.com/