Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review and Analysis of Hashing Techniques

Sangeeta Raheja[#1], Shradha Verma[2] Nisha Raheja(Dept of ECE)
[#]*Computer Science and Engg. Department, First-Third University*
Manav Rachna International University, Faridabad
India

Abstract-:- :- In these days sharing the information over the internet becoming a critical issue. So number of techniques is available to protect the data. The present work will focus on the comparison of hashing techniques. The hash value is of fixed length string. When the user sends the information with hash value and the third party changes the information then the hash value will be changed.

Keywords—Cryptography , SHA-1 ,SH256 ,SHA512

1. Introduction

Today the use of internet for communication has increased. So the security of information is important issue for safety. Cryptography is a technique of securing the information. The Cryptography is used for encrypting and decrypting the data. Encryption means convert the plain text into cipher text. The decryption means convert the cipher text into plain text. The encryption is done at the sender side and decryption is done at the receiver side. Cryptography is classified into symmetric cryptography and asymmetric cryptography. The symmetric key means same key is used for encryption and decryption. The asymmetric key means different key is used for encryption and decryption. Hashing is a function of cryptography that produces the hash value. The hash value is an arbitrary-length string that provide the integrity as well as authentication. The hash value is a one way function. One way function means from the original document we can produce the hash value but from the hash value we can not generate the Original document. The hash algorithms are like SHA-1, SHA-2 and SHA-3.

2. Analysis Of Different Hashing Techniques

A. Secure Hash Function-1(SHA-1):-

In cryptography, SHA-1 is cryptographic function that is designed by National Security Agency. The full form of SHA is secure hash function. SHA-1 produces a 160 bit message digest. The three algorithms comes under SHA are SHA-0, SHA-1, SHA-2. The SHA-1 is very similar to SHA-0 and was first published in 1995. SHA -1 is very widely used algorithm for producing the hash value. SHA-1 is currently used in wide variety of applications, including TLS , SSL and SSH. The construction of SHA-1 is similar to MD4 and MD5 functions. It has a 512 bit block size and has 80 number of rounds. The steps of SHA-1 algorithm are:-

1. Padding
○ Pad the message with a single one followed by zeroes until the final block has
448 bits.
○ Append the size of the original message as an unsigned 64 bit integer.
2 Initialize the 5 hash blocks (h0, h1, h2,h3,h4) to the specific constants defined in the SHA1standard.
3 Hashes (for each 512bitBlock)
○ Allocate an 80 word array for the message schedule
■ set the first 16 words to be the 512bitblock split into 16 words.
■ the rest of the words are generated using the following algorithm
 Word [i3]
XOR word [i8]
XOR word [i14]
XOR word [i16]
Then
Rotated 1 bit to the left.
○ Loop 80 times doing the following. (Shown in Image1)
■ Calculate SHA function () and the constant K (these are based on the
Current round number.
■ e=d
■ d=c
■ c=b (rotated left 30)
■ b=a
■ a = a (rotated left 5) + SHAfunction() + e + k + word[i]

○ Add a,b,c,d and e to the hash output.
 Output the concatenation (h0,h1,h2,h3,h4) which is the message digest.

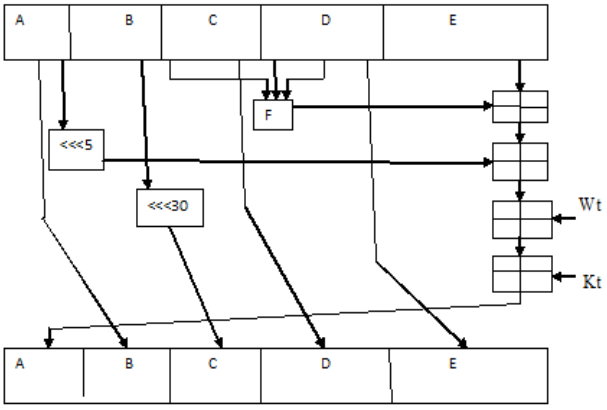

Figure 1: sha-1 diagram

B. **Example of SHA-1 algorithm**

Input(Text file	Output(SHA1 Hash)
hi	8afg3dh4sfg5adnm3gh2jkm3cbg5jk4nhjkl4bn5
hello	Gh2h4jjkl5lnbh5jkl7mmk8lkhdghj2kklrn4nb5b
This is very good	Ghkl3jbv4bnmj5klg5bm,l5lhgj7bhkl6lop3b5

C. SHA-256(Secure Hash Algorithm)

There are number of limitations and security issues of SHA-1. The limitations of SHA-1 are removed by SHA-2 algorithm. SHA-2 has number of hashing algorithms like SHA-224, SHA256, SHA-384 and SHA-512. The only difference between these algorithms is they have different message digest. On SHA-1 the collision attacks are there. But on SHA-2 there is no any collision attack yet been produced. The SHA-256 has message digest length of 256. The SHA-256 is more secure and faster than SHA-1 Algorithm. It takes less time to produce hash value as compared to SHA-1. The SHA-256 has 64 number of rounds. On SHA-2 no attack yet has been produced. The algorithm of SHA-2 has same as SHA-1 algorithm.

D. **SHA-512(Secure Hash Algorithm)**

In SHA-2 the SHA-512 is strongest among other SHA-2 algorithms. The SHA-512 produces message digest three times larger than SHA-1. That's why SHA-512 is more secure. The algorithm of SHA-512 uses more complex operations to SHA-1, making the algorithm by itself stronger. In SHA-2 the SHA-512 is more secure and faster than other SHA-2 algorithms. The SHA-2 has 80 number of rounds. The SHA-512 has block size of 1024 bits . On SHA-512 no attack yet has been proposed. It is secure because of its message digest length.

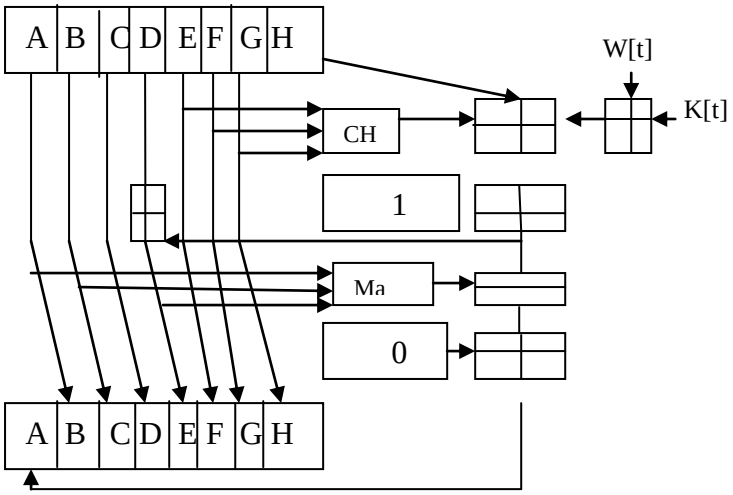

Figure 2: sha-2 diagram

E. Comparison of hashing algorithms

Table 1: comparison of hashing algorithms

Algorithm	Output size	Block size	Word size	Rounds	collision
Sha-0	160	512	32	80	yes
Sha-1	160	512	32	80	2^63
Sha-256/224	256/224	512	32	64	None yet
Sha-512/384	512/384	1024	64	80	None yet

3. Conclusion:-

In Data communication, cryptography has their own importance. Our research work surveyed the existing hashing techniques like SHA-1,SHA-256 and SHA-512 algorithms. Those hashing techniques are analyzed. Based on the experimental result it was concluded that SHA-512 algorithm consumes least time for producing hash value as compared to SHA-256 and SHA-1.

References

[1] Yaser Esmaeili Salehani1, S. Amir Hossein A.E. Tabatabaei,Mohammad Reza Sohizadeh Abyaneh3, Mehdi Mohammad Hassanzadeh "NESHA-256, NEw 256-bit Secure Hash Algorithm" Sharif University of Technology, Tehran.

[2] Shay Gueron , Simon Johnson , Jesse Walker " SHA-512/256" Security Research Lab, Intel Labs, Intel Corporation, USA.

[3] H. Dobbertin, A. Bosselaers and B. Preneel, "RIPEMD-160, a strengthened version ofRIPEMD", FSE'96, LNCS 1039, Springer-Heidelberg, pp. 71–82, 1996.

[4] H. Englund, T. Johansson, and M. S. Turan, "A Framework for Chosen IV StatisticalAnalysis of Stream Ciphers",INDOCRYPT'07, LNCS 4859, Springer-Heidelberg, pp.268–281, 2007.

[5] . E. Filiol, "A new statistical testing for symmetric ciphers and hash functions", InternationalConference on Information, Communications and Signal Processing, LNCS 2119,Springer-Heidelberg, pp. 21–35, 2001.

[6] . D. Hong, D. Chang, J. Sung, S. Lee, S. Hong, J. Lee, D. Moon, and S. Chee, "New FORK-256", 2007. http://eprint.iacr.org/2007/185.

[7] D. Hong, J. Sung, S. Lee, and D. Moon, "A new dedicated 256-bit hash function: FORK-256", FSE'06, LNCS 4047, Springer-Heidelberg, pp. 195–209, 2006

[8] A. Joux , T. Peyrin, "Hash Function and the (amplified) Boomerang Attack", CRYPTO'07,LNCS 4622, Springer-Heidelberg, pp. 244-263, 2007.

[9] . S. Künzli, P. Junod, W. Meier, "Distinguishing Attacks on T-Functions", Mycrypt'05, LNCS3715, Springer-Heidelberg, pp. 2–15, 2005.

[10] . A. Klimov, A. Shamir, "New Applications of T-functions in Block Ciphers and HashFunctions", FSE'05, LNCS 3557, Springer-Heidelberg, pp. 18–31, 2005.

[11] . G. Leurent, " MD5 Is Not One-Way", FSE'08, Springer-Heidelberg, 2008.10. H. Lipmaa, "On differential Properties of Pseudo-Hadamard Transform and relatedMappings", Indocrypt'02, LNCS 2551, Springer-Heidelberg, pp.48-61, 2002.

[12] . K. Matusiewicz, S. Contini, J. Pieprzyk, "Collisions for Two Branches of FORK-256",Cryptology ePrint Archive 2006/317 (First version), Sep. 2006.

[13] . K. Matusiewicz, S. Contini, J. Pieprzyk, "Weaknesses of the FORK-256 CompressionFunction", Cryptology ePrint Archive 2006/317 (Second version), Nov. 2006.

[14] . H. Molland, T. Helleseth, "A linear weakness in the Klimov-Shamir T-function", ISIT2005, IEEE International Symposium on Information Theory, pp. 1106 – 1110, 2005.

[15] . F. Mendel, J. Lano, B. Preneel, "Cryptanalysis of Reduced Variants of the FORK-256 Hash Function", CT-RSA'07, LNCS 4377, Springer-Heidelberg, pp. 85–100, 2007.15. F. Muller, T. Peyrin, "Cryptanalysis of T-function-Based Hash functions", IC

