IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Comparative Study of Encryption Algorithms for Improved Security: A Survey

Abdulrahman M.Zeyad[1*], Chandra Shekar Loganathan[2] , Gopal K Rishna[3]

[1,2] School of Computing and Information Technology, REVA University, Bengaluru, India
[3] Professor: School of Computing and Information Technology, REVA University, Bengaluru, India

Corresponding Author: amamzeyad@gmail.com, Tel.: +91-6363-861-194

DOI: https://doi.org/10.26438/ijcse/v7si14.7275 | Available online at: www.ijcseonline.org

***Abstract*—**The issue of information security is one of the most important issues of the modern day. Since the internet has become hugely wide spread, it has unbelievably helped in fast and efficient access to the cloud services and information on the cloud. The issue of securing this information has become an extremely serious problem. As previously known that the hash algorithms are one-way algorithms and cannot be retrieved. These algorithms provided a solution to the problem of analyzing the frequency of characters within a particular text by using encryption for more than characters. The proposed algorithm will provide a better model for finding scattered value. This system is characterized by its ability to face the threat of dictionary attacks, making it difficult to prepare a dictionary of scattered values. In this survey, a comparison was made between the proposed model and the MD5, SHA1 systems**.**

***Keywords*—** hash algorithm, one-way, attack dictionary, strong collision, MD5, SHA1 systems.

I. INTRODUCTION

The encryption is a process that combines mathematics and computer science. It is the science and ability to protect data from penetration. It is used in most fields and applications. The process of coding is increasing to protect data, but what is saved and secured today can be hacked tomorrow. Cryptography includes a set of algorithms and techniques to convert data into another form, whose contents appear illegible and unexplainable to anyone who does not have the authority to read or write on that data. The main purpose of using cryptographic algorithms is to protect information and data in order to achieve the privacy, integrity and accessibility of the resources and services provided by the information system. There is a range of risks that can harm computer information systems, such as those directed to the same cryptographic algorithm. For example, an analogue cryptographic algorithm may encounter attackers' risk for the contents, configuration or properties of an algorithm and to identify parts of the original message that the user wants to use. The attackers rely on the experience of a set of possible cryptographic keys on the encrypted text portion and in that case they can access the original message before encryption. With a large increase in risks that could damage data, a set of rules, techniques and antigens have been developed to protect information systems. Antibiotics are any method or means that can be used to prevent any attack that threatens the security of data and information. Antibodies may be prevented by attacking the data if possible or detecting the attack and the penetration process if the attack fails and then returns the system to normal as before the penetration or attack[1] [2][3].

CRYPTOGRAPHY:

Cryptography, or encryption, is the practice and detailed study of data concealment and messages. more precisely, it is a way to store and transfer data in a particular form so that only specific individuals who have the respective keys can read, and process it.[1][2]

The common methods of encryption are:

1. The symmetric-key cryptosystem, where the sender and receiver use same key to send and recover the message, the same key is used for encryption and decryption. [2].
2. The asymmetric-key cryptosystem, where it uses the public key to encrypt the message and private key to decrypt the message. [2].
3. Hybrid cryptosystem: combines the strengths of both methods (symmetric and asymmetric). Distributed asymmetric key replication, also known as the open meeting. Symmetry provides bulk encryption. For example, mixed encryption system is SSL [2].

1.1 MD5

The MD5 algorithm is a hash function that is widely used and produces a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it was found that there were wide vulnerabilities. It can still be used as a test to validate data integrity. Remained appropriate for purposes other than noncryptographic purposes.

One of the prerequisites for encrypting the hash function is that there must be a useless account to find a message that has two distinct values of the same value. MD5 fails as such collisions can be found in seconds on the normal home computer.

MD5 hashing algorithm and, SHA1, are in widespread use in the Transport Layer Security (TLS) protocol on which HTTPS is based. In fact, even though collisions were found with MD5 as early as 1996, it was still included in TLS as late as 2008. That said, MD5 was banned at that time in TLS certificates but not for other aspects of TLS.

MD5 was designed by Ronald Rivest in 1991 to replace the previous MD4 retailer, and was specified in 1992 as RFC 1321[2][4].

Figure 1. One MD5 operation. MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. F is a nonlinear function; one function is used in each round. Mi denotes a 32-bit block of the message input, and Ki denotes a 32-bit constant, different for each operation. ⋘ s denotes a left bit rotation by s places; s varies for each operation. ⊞ denotes addition modulo 2^{32}[1][3].

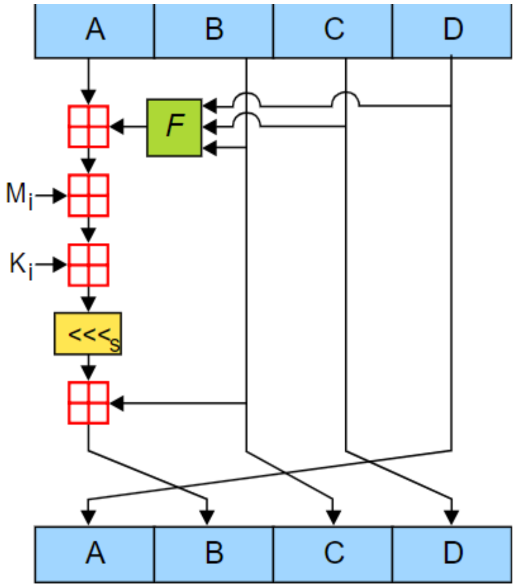

Fig.1 MD5 Algorithm

1.2 Secure Hash Algorithm (SHA)

- SHA-0: It was removed soon after publication because of “paramount flaw” and was replaced by a revised version SHA-1[2][4].

- SHA-1: It works similar to MD5 and produces a 160-bit message digest. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. It was no longer used for most cryptographic uses after 2010 because of the cryptographic weaknesses discovered in the working.[2].

- SHA-2: It was also formulated by the NSA.A family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512,they differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words[2].

- SHA-3: It was proposed 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.[1]

1.2.1 SHA-1

- Input: message of arbitrary length.
- Output: 160 bit hash code.
- The input message is broken up into chunks of 512- bit blocks (sixteen 32-bit words).In case the message is not an integer multiple of 512-bit blocks, the message is padded so that its length is divisible by 512.
- The padding works as follows: Pad the message with a single 1 followed by 0’s until the final block has 448 bits and append the size of the original message as an unsigned 64-bit integer.

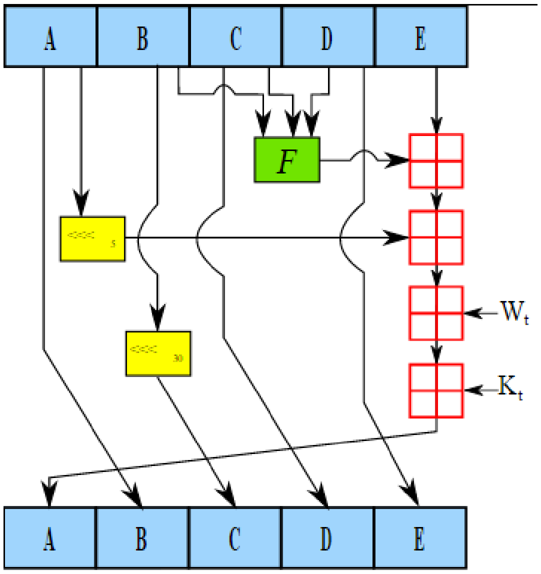

Fig.2 SHA-1 Algorithm

One iteration within the SHA-1 compression function: *A*, *B*, *C*, *D* and *E* are 32-bit words of the state; *F* is a nonlinear function that varies;
⋘n denotes a left bit rotation by n places;
n varies for each operation;
W_t is the expanded message word of round *t*;

K_t is the round constant of round t;
$\boxplus$ denotes addition modulo 2^{32}[1][3]

Here is the comparison between MD5 and SHA1. You can get a clear idea about which one is better [5][6][7].

Keys For Comparison	**MD5**	**SHA-1**
Security	Less Secure than SHA	more Secure than MD5
Message Digest Length	128 Bits	160 Bits
Attacks required to find out original message	2^{128} bit operations required to break	2^{160} bit operations required to break
Attacks to try and find two messages producing same MD	2^{64} bit operations required to break	2^{80} bit operations required to break
Speed	Faster, only 64 iterations	Slower than MDS, Required 80 iterations
Successful attacks so far	Attacks reported to some extents	No such attacks report yet
Speed: Assembly optimized	MD5 is consistently slower than SHA-1	SHA-1 is consistently faster than MD5
Produce collision	It is easy	It is not easy

Encryption algorithm applications.

1. Validation of files (Data Integrity): One of the goals in general is to preserve and access your files, they should not to be modified or tampered.
2. Digital signature science (Digital Signature - Public Key Cryptography): Files are sent with encrypted or non-encrypted messages, signatures are created as well as authentication through encryption.
3. Password (Password-Word):In order to maintain passwords in the database in encrypted form[3].

MD5:

- Unfortunately, MD5 has been completely hacked in this regard because there are multiple ways to easily find adjustments in it[8].

SHA:

- SHA-1 also has some minor adjustments in this regard that have been recently discovered, but are less severe than the problems of MD5. It's safer to use something like SHA-256 because it doesn't currently involve any known attacks against retail collisions.

II. Description Applications

There are algorithms that changes the text or message to a set of symbols and characters to obscure the decryption of message by the attackers. These can algorithms achieve one direction property [5][9].

Retail makes it difficult to even recover the original text from the value generated by this algorithm. This type of algorithm can be used to create an electronic signature that achieves the authenticity of the data, that is, from a reliable source[6][10].

The strength in any one-way algorithm is that the encrypted text is secure. Decoding from this point, we want to choose which algorithm has no inversion, which means no inversion can be found. It has to be used to create a one-way scattering algorithm that meets the first four algorithms. So we hit the irreversible matrix with the original text and use the rest of the division for a certain value. To find scattered value.

The sender calculates the scattered value of the original text using this model and then sends the message. The original and scattered value of the future, which in turn uses the same model to calculate a scattered value of the message. That arrived, and then comparison with the scattered value received from the sender, thus making sure the message is as valid as it appears in Figure number[3][10].

CONCLUSION

In this survey, we compared algorithms used in encryption to produce values and symbols scattered using these algorithms for use in data security. In future work, more will be compared for the properties they provide that make them some of the most common algorithms. There are many options available for cryptography purposes, and in this survey, we only covered MD5 SHA-1 (Hashing Algorithm). It is best to use multiple means of encryption in your applications such as AES and DES to keep Sensitive information that should be safeguarded and protected against unwarranted disclosure.

REFERENCES

[1] S. Debnath, A. Chattopadhyay, and S. Dutta, "Brief review on journey of secured hash algorithms," *2017 4th International Conference on Opto-Electronics and Applied Optics, Optronix 2017*, vol. 2018–Janua, pp. 1–5, 2018.

[2] S. Gupta, N. Goyal, and K. Aggarwal, "A Review of Comparative Study of MD5 and SSH Security Algorithm," *International Journal of Computer Applications*, vol. 104, no. 14, pp. 1–4, 2014.

[3] the free encyclopedia Wikipedia, "Cryptography/MD5,SHA." .

[4] M. J. (Mustansiriya/University) Reda, "Implementation of (MD5) Algorithm," *DIYALA JOURNAL FOR PURE SCINCES*, no. 1, pp. 131–139, 2013.

[5] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The first collision for full SHA-1," *Lecture Notes in*

Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10401 LNCS, pp. 570–596, 2017.

[6] V. Chiriaco, A. Franzen, R. Thayil, and X. Zhang, "Finding partial hash collisions by brute force parallel programming," *2017 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2017*, vol. 5, pp. 1–6, 2017.

[7] Gayan Samarakoon, "Cryptographic essence of Bitcoin part." [Online]. Available: https://hackernoon.com/cryptographic-essence-of-bitcoin-part-1-what-is-a-hash-function-f468e7f72daa.

[8] William Stallings, *Cryptography and Network Security (Various Hash Algorithms)*, Fourth Edi. 2005.

[9] R. J. Rodríguez, M. Martín-Pérez, and I. Abadía, "A tool to compute approximation matching between windows processes," *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, vol. 2018–Janua, pp. 1–6, 2018.

[10] J. Mittmann, "One-Way Encryption and Message Authentication Security of Hash Functions," p. 13, 2005.

Authors Profile

Mr. Abdulrahman Mohsen Zeyad pursued Bachelor of Information Technology at University of Modern Sciences, Sana'a –Yemen in the year 2013. He is currently doing a Master degree Data Engineering and Cloud Computing in the Department of School of Computing and Information Technology, REVA University, Bengaluru, India since 2018.

Mr. Chandra Shekar Loganathan pursued Bachelor of Electronics & Communication at MSRIT-Bangalore University in the year 1995. He is pursued currently doing a Master degree Data Engineering and Cloud Computing in the Department of School of Computing and Information Technology, REVA University, Bengaluru, India since 2018. Also working as Program Manager at CommScope, Bangalore for last 9+ years with overall industry experience of 20+ years in Telecom-Networking Technology.

Dr. Gopal Kirshna Shyam received BE and M.Tech and Ph.D in Computer science and engineering from VTU, Belagavi. His research interest includes Cloud Computing, Grid computing, High performance computing etc. He has published about 10 papers in highly reputed National/International Conferences like IEEE, Elsevier etc. and 5 papers in Journals with high impact factor like Elsevier Journal on Network and Computer Applications and International Journal of Cloud computing (INDERSCIENCE). His research articles on Cloud computing co-authored by Dr. Sunilkumar S. Manvi have been cited by several researchers. He is a lifetime member of CSI and is actively involved in motivating students/faculties to join CSI/IEEE/ACM societies.