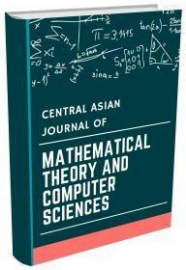

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 05 Issue: 03 | July 2024 ISSN: 2660-5309

Article

Enhancing Message Security Through Sha-256 Hash Algorithm

Najlaa muhammed mohie*

1. Department Computer Science, Faculty of Education for Pure Sciences, University of Thi-Qar, Thi-Qar, 64001, Iraq

* Correspondence: najlaamuhammed.eps@utq.edu.iq

Abstract: This study aims to enhance message security through the implementation of the SHA-256 hash algorithm within the CMC network security context. By employing MATLAB for design and simulation, the research focuses on protecting messages via fragmentation, ensuring encrypted and unencrypted chunks are properly arranged. The objective is to mitigate the impact of malicious attacks, as evidenced by simulations demonstrating the removal of error messages and the clean transmission of data. The research employs the SHA-256 hash algorithm for encrypting messages. The study uses MATLAB to simulate message encryption and decryption processes. The methodology involves: Hashing messages using the SHA-256 algorithm, Fragmenting the hashed messages for transmission, simulating malicious attacks and observing the algorithm's efficacy in error removal and data protection, Ensuring the receiver correctly reassembles and decrypts the fragmented messages. Simulation results show that the SHA-256 algorithm effectively protects messages from various types of malicious attacks. In all tested scenarios, the hashed messages were successfully transmitted, with the receiver able to cleanly receive and reassemble the data. The findings indicate a significant reduction in the vulnerability of messages to external attacks, demonstrating the robustness of the hash-based security system.

Keywords: Hash function, Encryption, Data security, Decryption

Citation: **Najlaa muhammed mohie**. Enhancing Message Security Through Sha-256 Hash Algorithm. Central Asian Journal of Mathematical Theory and Computer Sciences 2024, 5(3), 251-259.

Received: 08th July 2024
Revised: 15th July 2024
Accepted: 22th July 2024
Published: 26th July 2024

1. Introduction

The hash cryptographic algorithm, as well as other security-related subjects. This compares each form of encryption by means of safety.. Nowadays, all encryption solutions Digital technologies are used for data safeguarding and safety. Now three basic encryption technologies are used to safeguard data. The three approaches are symmetrical key, asymmetrical password and a one-way hashing. A symmetrical password is straightforward Immediately and without any delay. The unsecured data is inputted into the encryption process. mechanism, which generates data is encrypted. that the recipient decrypts. This method has been used for over forty years form the digital centuries. [1]

Asymmetrical keys employ distinct keys. One for the general population and one for privacy. The method is similar to that of a key with symmetry, with the exception that the key itself is divided into two categories. The one-sided hash employs the hash algorithm and generates no keys. A hash is a key, and all information is secure.

Two distinct encryptions have been observed. One involves hashing, while the other relies on keys. Encryption and hashing are two methods used to protect data. Privacy uses

plaintext to secure the data, while hashing uses hash tags. There are several benefits to utilizing hashing instead of key encryption systems. [2]

- It's a breeze to locate an entry once the data has been hashing.
- Random string are produced to ensure the uniqueness of each record stored within the database.
- contrasting hashes is a simpler task compared to contrasting the actual data. Can be utilized for extensive safety of data [3]

2. Materials and Methods

Problem Statement

The hashed cryptography technique employs the CMS (Cryptography Communication Syntax) protocol is used to guarantee the security of communication and minimize potential risks. risk of destructive attacks. Currently, data protection techniques and encryption technologies suffer from inadequate security. Despite being protected, a significant amount of data remains susceptible to assaults from external entities or malicious software. The reason for this is not due to the inadequacy of the data security system, but rather the increasing sophistication of attacking strategies. Presently, individuals have a tendency to use intricate coding techniques in order to target certain info on the network. They have the ability to use a multitude of strategies and coding methodologies. These antivirus and antimalware programs are inadequate in keeping pace with the latest advancements in malicious code. Most of this program is still discernible. They are unsuccessful in improving their data security measures. The current data attacker have the capability to inflict damage onto registration files, .ini files, and other essential root files.

Scope of Project

The studies will explore the following subjects

- CMS-based hashing cryptographic algorithm.

1. Intro to Cryptographic and Hash Systems for Security

Cryptography entails the generation of a confidential key. Additionally, there is a publicly available encryption key. Public keys are only allocated to incoming communication inside the network[4].

The recipient will conduct the decryption operation at the receiving end to get the message back. The most common word used for privacy in cryptography to an ordinary person is encryption and decryption and the following is a general statement for cryptography encryption and decryption: [5]:

$C = E_k (P)$ (1.1)

$P = D_k (P)$ (1.2)

Where P = plaintext

C = cipher text

E = encryption method

D = decryption method

k = the key

Equation 1.1 asserts that unencrypted data, usually referred to as plaintext, is inputted into a cryptography system, it undergoes encryption and is transformed into cipher text. A key is generated by every encryption procedure. A key may The information may be disseminated throughout the network as either public or private, depending upon the user's preferences. control over the internet connection. The user's text is "[6]."

In contrast, a hash is a block that turns plaintext to encrypted data. The hash contains a large amount of information that humans cannot understand. Only the machine understands [7].

After the hash is created, it becomes quite difficult to modify the information, and often, the transformation from output to input is prohibited. Figure 1 illustrates the hashing algorithm.

On the other hand, the hash has been clearly specified. The user's text is [8].

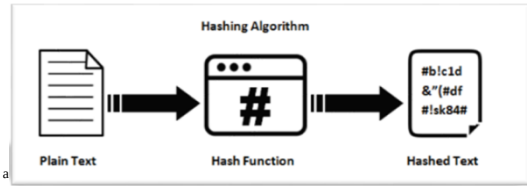

Figure 1: Development of hashed cryptographic algorithms CMS.

Figure 1shows whole procedure that took place when the hashed cryptography algorithm was called. Only one thing can be understood - the hash functions will return hash text instead of plain text as happens in case of Encryption using a cryptographic key. The importance of hash security is increasing in popularity. The hash function is a cryptographic algorithm that performs one-way encryption by generating a hashed output. messages rather than a plain text [9] Currently, most of the hashed systems were included in single term called hash function. While it is also called a cryptographic hash function only its not -as they are ordered-[]. One-Way Hashing: Many encryption algorithms nowadays depend heavily on one-way hash functions. It is used to generate a digital signature and for authenticating any entity, Figure 1: Hashed cryptography, shows the complete procedure for hashed cryptography process. All that remains to be known is that the hash algorithm puts hash text not the plain text as in key encryption. Hash based security is more and more frequently used. Again, the hash is a way of encrypting and molding to One-way encryption of plaintext message to hash[10] Nowadays, The majority of the encrypted systems are concatenated into a hash function. Since it is ordered, some individuals merely call it a cypher text hash function [11]. Modern encryption requires one-way hash functions. It is a must for digital signature and authentication. It is designed to take any length message compress it to string of fixed length, it is called as [12].

The hash system operates by first converting the unprotected information and then encrypting it through the hash algorithms. Its functionality is determined by a complicated mathematical procedure. Typically, the SHA-256 hash technique is

used before to encryption.S HA-256 stands for 256-bit data hash encryption. The National Security Agency (NSA) identified and built the algorithm. The SHA acronym stands for The Secure Hash Algorithm. It possesses the subsequent properties. [13]

- Indicator for accessible block sizes
- Absorb the size of the text after hashing.
- There is just one cycle for iterations
- Uses normal word count
- Data lengths are limited.
- Protocols influence the speed of hashing encrypted.

The evaluation The process of encrypting the system's hash may be defined as follows: [14]:

Let

m1 = message1

m2 = message2

mn = subsequence message

H = hash function

a1 = random number generator1

a2 = random number generator2

an = random number generator3

A pseudo generator is a kind of generator that creates confidential codes. The resulting code should be unique and cannot be same for every input.

The messages m1, m2, m3, etc., that are entered into the engine in the time domain may be represented as [15].

The unencrypted data may be represented as the sum of many components, denoted as m1(t), m2(t), mn(t), and so on, as shown in equation (1.3).

The process of hash creation produces a pseudo-random code called a hash, which is then multiplied by every message in the hash network. The result is 16.

Encrypted data that has been transformed using a hash function, denoted as H(m)

$$= a1m1(t) + a2m2(t) + a3m3(t) + \ldots\ldots anmn(t) \qquad (1.4)$$

It is important to mention that when you multiply anmn(t) by a multiple, it results in additional components. This message differs from the previous one, which was not encrypted. In order to comprehend the mathematical aspects of hashing systems in a practical context, let us use the following example: The user's text is a reference to a specific point or statement.

Message 1: How are you (unencrypted data)?

Random alphanumeric codes: AE00, EE99, EDR1023, ……..

The output of the message is: HowAE00, areEE99, youEDR1023 : 0045AE00#008EE99#865EDR1023

It's crucial to understand that the '#' symbol represents a space. In this scenario, The symbol '#' is utilized. Actually, it might transform into various symbols. As the number of repetitions increases with each new incoming message rises, the symbols may change. Keep in mind that each message is processed during a single iteration cycle. The latest message will utilize distinct code, resulting in the creation of a new messaging code.

When messaging are sequenced or serialized, they create a cryptography system. When messaging are encrypted, they cannot be modified, even their location. It is impossible to reintegrate the message into the hash process. If a mistake is identified, the message must be rewritten from scratch. Putting the messages in cryptographic order is the duty of the algorithm. Once more, this is managed by a complicated mathematical algorithm. To understand the mathematical analysis of cryptography, consider the following example. [18]:

let = code for cryptography

= hashed messaging

The encryption code will be placed in order for creating a series of codes that may be multiplied by the hashed messages. Thus, multiplied with an identity matrix [19]:

The last matrices results represent the hashing message's cryptographic order. The system could read it from row to row as follows: 13120809190621140

2. Cryptographic Algorithm for Hashing

An algorithm is a software that shows how hash encrypting works. The technique might be presented in several alternative ways. Often, this entails using a diverse range of programing dialects such as Java, C++, and Python. It is up to the simplicity of the coder.

Certain programming dialects may have restricted library features. For example, should a programmer pick FORTRAN, the user will be unable to provide the best graphical technique to explain the hashed cryptographic encrypting. [20].

If the programmer uses another programming language, such as Visual Basic, C++, or C, a more visually appealing representation of the encryption technique utilizing the hashing function may be presented.

It is not required to present an approach in its entirety. However, The essential components of a software that include the hash and cryptographic functions must be shown.

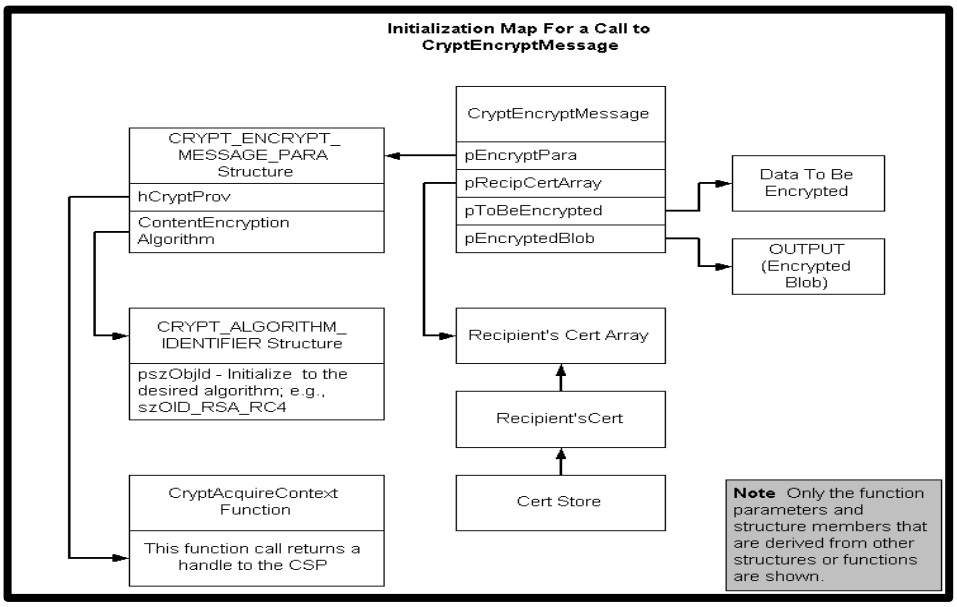

Fig 2: General hashed cryptography encryption

3. Results and Discussion

Simulation Results

This section will present the simulation based on the setting in section 1.2. The simulation results consist of few scenarios where the message being damage or attacked by the malicious. Each scenario will be discussed in the section.

i.Simulation results with scenario 1

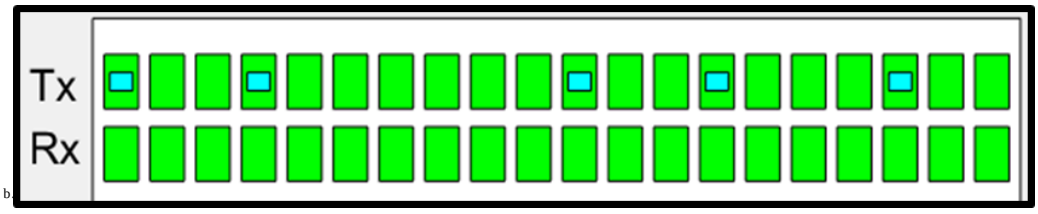

Figure 3: Malware attacks the first, fourthly, and subsequent three messages.

Figure 3 shows the condition where 5 hashed messages of the transmitter are attacked by the malicious. This is shown using light blue color.

At the receiver, Rx all the messages are cleaned and received without damage. This show that the data being protected and avoid damage by the malicious.

ii. Simulation results with scenario 2

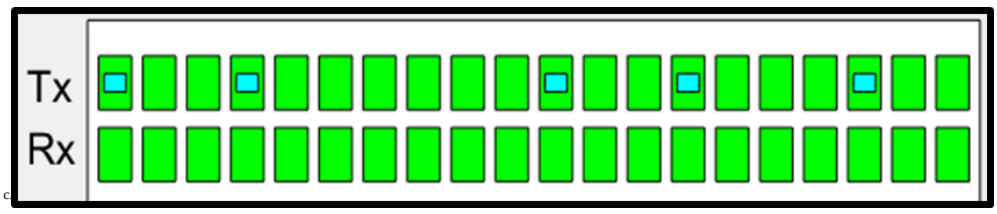

Figure 4: The attack targets four hashes messages.

As seen in Figure 4 Four hashing messages are under assault.. But at the receiver, all the messages are successfully recovered without damage.

iii.Simulation results with scenario 3

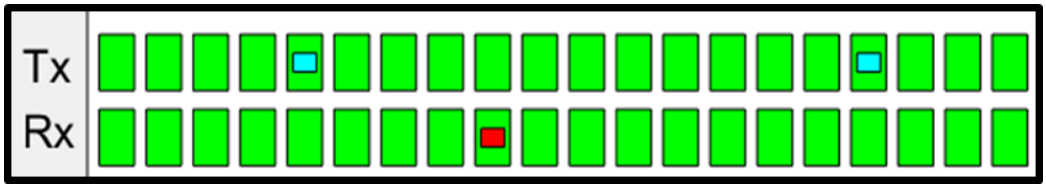

Figure 5: Malware attacks two hashed texts.

Note that when two messages are being attacked by the malicious, the data could be disappeared in the network. This is marked by red color as the fail message. When this condition happens, the transmitter has the resend the message.

iv. Other Simulation results

Besides the three main scenarios in the simulation, there are other simulation results where different colors are observed when the messages are being hashed and protected. This can be seen in Figure 3, 4, 5.

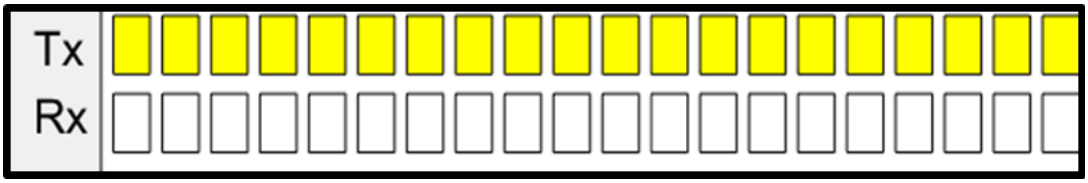

Figure 6: The transmitter buffer the messages

Figure 6 shows the messages being buffered before enter into the channels. The buffers are necessary to avoid messages collision in the channels.

For every time simulation begin, the buffers will be opened to slot in the hashed messages. Only when buffers are available, then the messages will go into the buffers. If not, the messages have to be resend as seen in Figure 7.

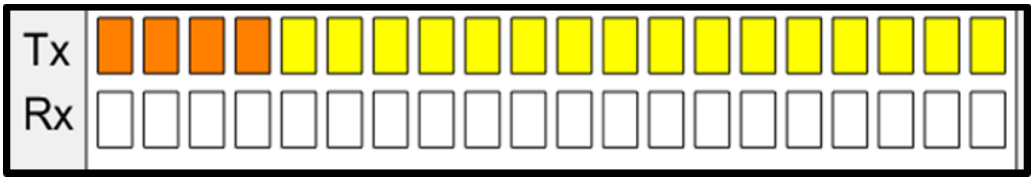

Figure 7: Some communications are resent and marked with red colours.

As show in Figure 7, there are four messages marked with red color. This indicates that the messages are not protected by hashed. Therefore, the messages have to re-hash for protection.

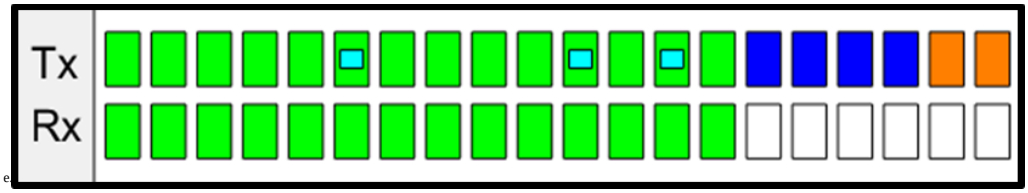

Figure8: Some messages waiting for acknowledgement

When the channels are idle, the messages can be sent without risk. On the other hand, when the channels are busy with many messages, then the transmit messages

have to wait for "ACK" to alert on the use of channels. This is important to control the traffic in the channels. The ACK basically will alert the transmitter when the channels are idle or less messages. As seen in Figure 1.10, the ACK is marked with blue colors on certain messages.

Simulation Results Observations

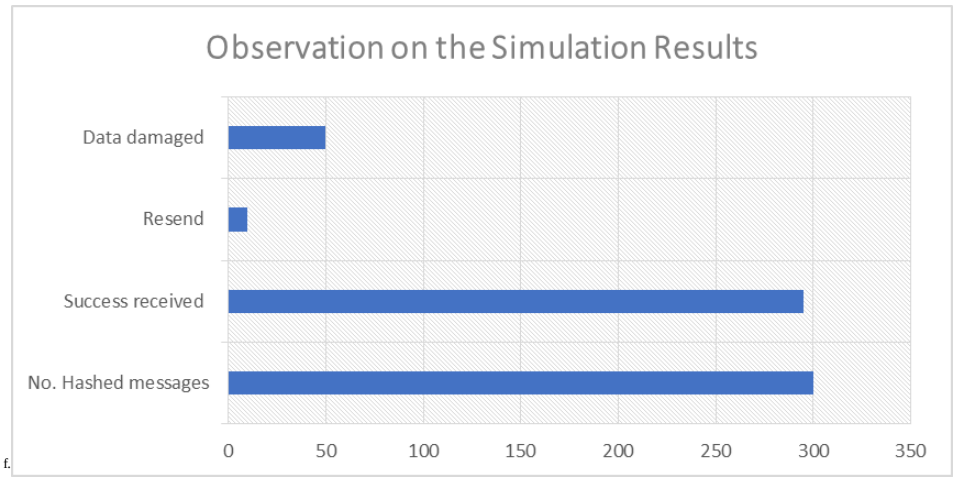

Figure 9: Observation on the outcomes of the simulations

Figure 9 shows the simulation results under few observations. Note that out of 300 priority of message being defined at the upper layer of the message block, there are 10 of the messages resend, 50 of them damaged, 300 are being successful hashed and 298 are being successful received.

The statistics have showed the hashed data protection is very useful and really can protect the data. The percentage of data loss and damage are less and still reliable in the practice.

4. Conclusion

Hashed message means the user message or plain text is being hashed or added with some characters where people cannot understand. Only human itself can understand. When messages are in hashed, we said that the messages are being protected.

The cryptography is a system that arrange the hashed message in the network. The arrangement will follow the syntax. This is important to tackle two issues. One is to prevent malicious attack and second is to control the message traffic in the network.

From the simulation results, we use green colors to represent the messages transmitted from the transmitter and successfully received by the receiver. We also use the yellow color to indicates the buffer process, the blue represents the "ACK" and the red indicates bad message.

From the observation, one can see that the receiver does the process of extracting the messages from the channels are able to avoid bad messages and avoid malicious attack.

REFERENCES

1. Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec
2. "What are MD2, MD4, and MD5?". *Public-Key Cryptography Standards (PKCS): PKCS #7: Cryptographic Message Syntax Standard: 3.6 Other Cryptographic Techniques: 3.6.6 What are MD2, MD4, and MD5?. RSA Laboratories*. Retrieved 2011-04-29.
3. Bert den Boer, Antoon Bosselaers (1991). "An Attack on the Last Two Rounds of MD4" (PDF). Archived from the original (PDF) on 2003-05-23.
4. "5.1 Security Considerations for Implementors". Retrieved 2011-07-21. Deriving a key from a password is as specified in [RFC1320] and [FIPS46-2].
5. Ronald L. Rivest Massachusetts Institute of Technology Laboratory for Computer Science NE43-324 545 Technology Square Cambridge
6. Jie Liang and Xuejia Lai Department of Computer Science and Engineering Shanghai Jiao Tong University Shanghai 200240.
7. Daemen, J. (1995). Cipher and hash function design strategies based on linear and differential cryptanalysis(Doctoral dissertation, Doctoral Dissertation, March 1995, KU Leuven).
8. S. Al-Kuwari. Engineering Aspects of Hash Functions. In International Conference on Security and Management (SAM '11), 2011.
9. R. P. Arya, "Design and Analysis of a New Hash Algorithm with Key Integration," vol. 81, no. November, pp. 33–38, 2013.
10. Joux, A. (2004, August). Multicollisions in iterated hash functions. Application to cascaded constructions. In Annual International Cryptology Conference (pp. 306-316). Springer, Berlin, Heidelberg
11. Jane Chan, Low.K.C and Shaung. H, "The Hash Security Implementation", *IEEE Trans on Data Communications*, Vol. 9, Issue 4, 2017.
12. Ja Shau Kok and Hui Ying, "Introduction to Hash Cryptography System", *IEEE Trans on Computer Science and Technology*, Vol. 10, Issue 10, 2016.
13. Sandra.L, Maggie. C and Huang Xia, "Advanced Hash Cryptography Encryption", *International Journal on Data Communications*, Vol. 99, Issue 17, pp. 8 – 23, 2017.
14. Lee Gao Xian and Chong Hua, "Data Encryption using Hashing", *International Journal on Data Communications and Computer Sciences*, Vol. 90, Issue 19, pp. 29 – 33, 2016.
15. Boysted.M and Kong.C, "Simulation on Data Encryption using Cryptography", *International Journal on Data Communications*, Vol. 66, No. 10, pp. 56 – 78, 2017.
16. Jeffy.T, Advanced Security in Data Communication, McGraw-Hill, New York, 2014.
17. Chong Wen Tze, Introduction to Data Communication and Encryption, Prentice-Hall, New York, 2015.
18. Deng Tze, Advanced Cryptography and Hashing, Prentice-Hall, New York, 2017.
19. Hao Xian and Jasua. H, Fundamental of Data Encryption, McGraw-Hill, New York, 2016.
20. Osima.M, Practical Encryption and Data Protection, Wiley & Sons, London,