IMPLEMENTATION OF HASHED CRYPTOGRAPHY ALGORITHM BASED ON CRYPTOGRAPHY MESSAGE SYNTAX

Mohammed Ahnaf Ali

A project report submitted in
fulfillment of the requirement for the award of the
Master of Electrical/Electronic Engineering with Honours

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

JULY, 2019

PTTA UTHM
PERPUSTAKAAN TUNKU TUN AMINAH

DEDICATION

I would like to thank my parents AHNAF ALI and AMAL ABDUL LATIF for giving me ethical support while I were doing this project. They always guided me to make sure I could finish my project on time and complete it successfully.

I also would like to thank my friends for their concern and help for completing my project successfully with giving suggestions and discussing together to solve the problem during my project; without them, I could not have completed this project on time.

PTTA UTHM
PERPUSTAKAAN TUNKU TUN AMINAH

ACKNOWLEDGEMENT

Praise and thanks be to **Allah** for the blessings of mind and health and "conciliating me" for completing this thesis. I would like to express my sincere gratitude to my supervisor **DR. NORFAIZA BINT FUAD** for giving me the proper of advice, guidance and encouragement for my research. He gave me many opinions and ideas for the research and writing of this thesis. Through his patience, motivation, enthusiasm and immense knowledge, I managed to complete this project perfectly and successfully!

In addition, I would like to thank my parents **AHNAF** and **AMAL** for giving me ethical support while I were doing this project. They always guided me to make sure I could finish my project on time and complete it successfully.

To UTHM and the Faculty of Electrical and Electronic Engineering Staff Thanks for providing me with an excellent research environment and the proper resources to undertake this research. To the Iraqi government and all Universities: Thank you for supporting me to complete my master's degree. Finally, yet importantly, I would like to thank a person who contributed to completing my final thesis directly or indirectly. I would like to acknowledge him/her for helping, which was necessary to complete this.

Furthermore, I also would like to thank my friends for their concern and help for completing my project successfully with giving suggestions and discussing together to solve the problem during my project; without them, I could not have completed this project on tim

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

ABSTRACT

This design and simulation research is conducted in CMC network security (message encryption context). The design will use MATLAB encryption to show simulation. The coding is designed in such a way that there is a malicious attack to destroy the data. The system will automatically protect data and thus retrieve data at the end of the system. The important study in this research is an automated learning system for deep learning to enhance security. Through system training, security can be improved. The incoming data will be checked and the system will determine whether it contains errors or false data. The system will determine after the defragmentation function, and the next thing is the key length tracking message programming. This is to make sure that the master message follows formatting in the hash. Anything that does not follow the hash format in the system or panel will be ignored. There is a transmitter transmitting the message in a series of blocks. There is a receiver receiving the message in a series of blocks. Messages in the transmitter are protected by fragmentation and arranged in encryption. This is according to the syntax algorithm. One of the two messages is deliberately rearranging and attacking by malicious. The problematic message uses light blue representation in simulation. The sent message uses the red color representation in the simulation. Hence, the fragmented CMS encryption algorithm will solve this problem and the errors in the message will be removed. The receiver must receive a clean message chain without errors. The requested messages sent from the sender and the receiver are used by the green receiver to represent. By the end of the research, the animation and animation system will be introduced to show the basic process of network enhancement with the automated learning system.

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

TABLE OF CONTENTS

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

PTTA UTHM
PERPUSTAKAAN TUNKU TUN AMINAH

LIST OF TABLES

PTTA UTHM
PERPUSTAKAAN TUNKU TUN AMINAH

LIST OF FIGURES

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

PTTA UTHM
PERPUSTAKAAN TUNKU TUN AMINAH

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Information security is defined as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction". Essentially, this means that we want to protect our data (wherever it is) and system assets from those who seek to misuse them. This means protecting them from attackers who invade our networks, viruses, natural disasters, adverse environmental conditions, power outages, theft, vandalism or other undesirable situations. In the end, we will try to secure the nose look at the most likely forms of attack, to the maximum that we can reasonably do [1].

Today, there are many encryption scheme and data protection software have been developed to protect the data or message. Some software has an ability to remove the viruses and malware. All this harmful software could be a spy or malicious who can steal information from the user or from the system transaction. Thus, security in internet network becomes more and more useful [2].

This research is about the implementation of hashed cryptography algorithm based on CMS (Cryptography Message Syntax) protocol to protect the message and eliminate the harmful attack. The research will use the MATLAB to demonstrate the protection. A hash message which contain user information. The cryptography encryption then applied to protect the data. With the CMS protocol, the encrypted data will become more secure and difficult for the computer hacker to hack the data. The demonstration can be seen after complete the research.

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

1.2 Problem Statement

Today the data protection scheme and encryption methods encountered low security. Many data under protection still being able attacked by third party or malicious. This is not because the data protection scheme is not good enough, but this is more to the attacking methods are getting more advanced. People nowadays tend to develop advanced coding to attack the wanted data in the network. They could use differences methods and coding schemes. Those antivirus software and antimalware software are not able to follow the latest development of the attacking coding. Most of this software still at the level to detect the .exe files only. They do not upgrade to the next level of data protection. The current data attackers can damage the registration files, damage the .ini files and other important root files.

Another problem facing today is the difficulties develop the anti-attacker's software. The scheme is getting more and more difficult until not many researchers want to take the challenge. Also, the current advanced data protection scheme is very difficult to learn. Each and every researcher has their own opinions and the root of study is not really standardized.

There are many research gaps found in the data protection scheme researches. The research gaps are:

- Auto update the algorithms to fight with new attackers
- The effectiveness to identify real and fake viruses
- 100% clean the network without any worms

The above three points are the new challenges for next generation of data protection schemes. They might take times to develop and test the systems. The chances of success relies on how effective people develop the coding. The artificial intelligence system may be incorporate into the system to enhance the protection.

1.3 Objectives of the Study

The objectives of the research are.

(i) To simulate the hashed cryptography algorithm.

(ii) To proposed hashed cryptography algorithm.

(iii) To evaluate the performance of the algorithm.

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

1.4 Scope of Project

The scope of the research will cover the following topics.

- The hashed cryptography algorithm using CMS
- The MATLAB

The scope also will consider the time spend in the research. This is main focus to manage time well in order to complete every section of the task in the research. This research will spend more time in learning the MATLAB compare with spend time in study the theory about the CMS. MATLAB is very difficult to learn as there are many hidden functions. Some functions are not disclosed in the help file or in the tutorial. Therefore, user has to get more information from the literature reviews in order to study more detail about the MATLAB.

Apart from the timing, the cost and the quality also the focus in the research. Although this research does not spend any cost on the hardware, so the quality will be depending on the software performance. The quality of the research will justify the accuracy and performance of the system when input parameters are entered. The quality of the research also will be compared with other people works. This can come out a standard for the data protection development system.

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

1.5 Research Contribution

The study of hashed cryptography algorithm using CMS can contribute to the next level of data protection scheme. It helps to enhance the network security by making the attackers difficult to attack the data. Some fake coding is placed upfront of real data. Thus, when attacker obtain the data, they are actually getting a fake data. The real data is being protected by hashed cryptography algorithm. The development of hashed cryptography algorithm using CMS also contribute to the academic learning. With this technique, students be able to know the modern protection scheme on the data and able to compare with the traditional data protection scheme.

The study of the hashed cryptography algorithm may also lead to the solution of security enhancement method in HAN (Home Area Network) for smart house. It may be a good idea in monetary transaction protection when comes to online banking or payments.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter shows the theory about the data protection scheme. The topics to be focused are hashed cryptography algorithm and other related topics on the security system. The chapter will begin the general theories behind all the encryption systems. The advantages and disadvantages about the types of encryptions will be shown. This is to compare the all the encryption methods in term of security.

The chapter also shows the research papers presented by other researchers. The presentation of research papers is important because it helps to know the research trends and latest technology development in the security system. Apart from that, showing the research papers also will help to find out the research gaps and hence improve overall research.

2.2 General Data Protection Scheme and Overall Study

Encryption methods for data protection and security nowadays are fully digital. Today, there are three main encryptions methods employed to protect the data. These methods are symmetric key, asymmetric key and one-way hash. The symmetric key is very simple and direct. The unencrypted data is placed into the encryption, the system will generate an encrypted data and the receiver will decrypt the data. This method has been used for about more than 40 years from the digital century [3].

The asymmetric key uses different keys. One for public and one for private. The process is the like symmetric key, except that key is classified into two. The one-

way hash uses hash method and no key is generated. The hash itself is a key and all the data have been encrypted.

There are two differences encryptions are noticed. One is hash and the other one is key. The key encryption uses plaintext to protect the data whereas the hash using the hash tags to protect the data. The advantages of using hashing over the key encryption systems are [4]:

- Easy to find the record after the data being hashed.
- Random strings are generated for hashing to avoid duplicate of data stored in the database.
- Hash to hash comparison is much easier than the comparing the data. Can be applied for huge data protection.

Another advantage of using hash protection system is a one-way system. Unlike in ordinary encryption, two process: encryption and decryption are used in protecting the data. One-way protection scheme is easier to implement compare to two process of protecting the data.

Today message encryption becomes more and more important to prevent malicious attack or third-party attack. The message like transaction of money and user information should be protected in certain level. There are many details of message encryption systems can be found in the published papers. Most of these message encryptions deploy "Message-Digest Algorithm" to protect the data. Some of them quite well-know are MD2, MD4 and MD5.

The MD2 Message-Digest Algorithm is a cryptographic hash function developed by Ronald Rivest in 1989. The algorithm is optimized for 8-bit computers. MD2 is specified in RFC 1319. Although MD2 is no longer considered secure, even as of 2014, it remains in use in public key infrastructures as part of certificates generated with MD2 and RSA. The "MD" in MD2 stands for "Message Digest [4].

The MD4 Message-Digest Algorithm is a cryptographic hash function developed by Ronald Rivest [5]. The digest length is 128 bits. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD4 algorithm is designed to be quite fast on 32-bit machines. Weaknesses in MD4 were demonstrated by Den Boer and Bosselaers in a paper published [6]. The first full-round MD4 collision attack was found by Hans Dobbertin, which took only seconds to carry out at that time [7].

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

MD5 algorithm was developed by Professor Ronald L. Rivets. According to RFC 1321, “MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA. MD5 is considered one of the most efficient algorithms currently available and being used widely today [8].

2.3 Introduction to Cryptographic and Hash System in Security

In cryptography encryption, a private key is generated. There is also a public key. The public only assigned when the message enters into the network. The decryption process will be carried at the receiver to retrieve back the message. The general expression for the cryptography encryption and decryption can written as [9]:

$$C = E_k (P) \quad (2.1)$$

$$P = D_k (P) \quad (2.2)$$

Where P = plaintext

C = ciphertext

E = encryption method

D = decryption method

k = the key

Equation 2.1 states that when the unencrypt data, also called plaintext is entered into the cryptography system, the data will be encrypted and turn into ciphertext. For every encryption, a key is generated. The key can be shared in the network as private or public depending on how the user define the network [10].

The hash on the other hand is defined as a block that transforming the plaintext into ciphertext. The hash contents many information where it cannot be understood by

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

human. Only the machine can understand [11]. Once the hash is generated, it is very hard to change the content and usually from output to input is not allowed. Figure 2.1 shows the hashing algorithm.

The hash on the other hand is defined as a block that transforming the plaintext into ciphertext. The hash contents many information where it cannot be understood by human. Only the machine can understand [11]. Once the hash is generated, it is very hard to change the content and usually from output to input is not allowed. Figure 2.1 shows the hashing algorithm [12].

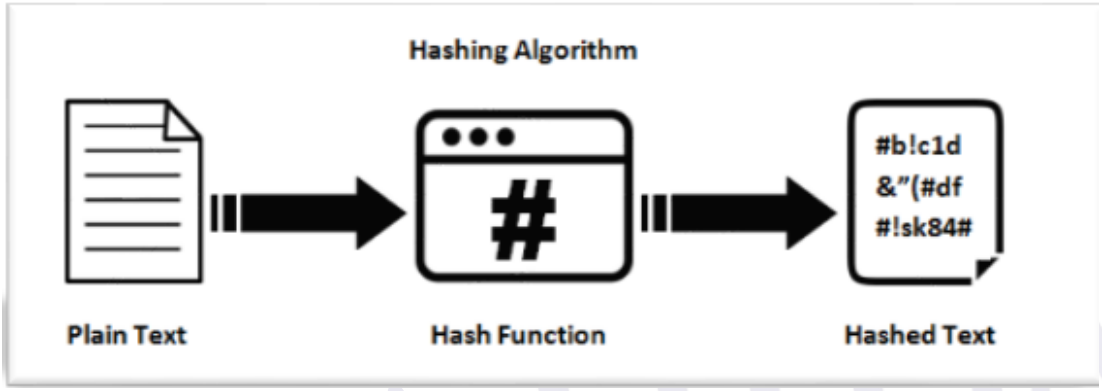

Figure 2.1: Implementation of hashed cryptography algorithm CMS.

The whole process in Figure 2.1 is called hashed cryptography algorithm. A pseudo code and flow chart explanation on the system will be explained detail in chapter 3. Only thing have to remember is the hash algorithm content hash text instead of plaintext like in key encryption. The hash security system nowadays becoming more and more popular. As mentioned, brief in chapter 1, the hash is a one-way encryption where hashed texts are used instead of plaintext. Today, most of the hashed systems are placed into a function so called hash function. Because they are placed in an order, so some people call it cryptographic hash function [13].

One-way hash function has played an important role in modern cryptography. It is one of the indispensable tools in digital signature and authentication. It can compress message with arbitrary length into a fixed length string which is called hash value [14].

This is the function that sets the random length message to a fixed-length hash result. This assignment can be distinguished by a secret key. The checksum mechanism is the only process to work with a factor proportional to the length of the message. All other operations operate in the short term due to retailing. Other applications for retail functions include digital signatures and specific identification protocols. For an

overview of application coding functions. In most applications, it is enough to provide a unique fingerprint for a message. This may mean that it is useless to find pairs of message collisions, that is, those fragmentations to the same result [15].

The operation of the hash system first converts the unencrypted data and then put them in the encrypted method using hash algorithm. The way it works depends on the complex mathematic algorithm. Usually, SHA-256 hash algorithm is applied up front the encryption. SHA-256 refers to 256-bit data hash encryptions. The algorithm was first discovered and designed by NSA. The SHA means Secure Hash Algorithm. It has the following characteristics [16]:

- Available block size indication
- Digest the size of the message after hashed
- Only one cycle of iteration
- Uses standard word size
- Limited size of data length
- Speed of hashed encryption determine by protocol

The analysis of the hash system encryption can be explained as below [17]:

Let

m_1 = message 1

m_2 = message 2

m_n = subsequence message

H = hash function

a_1 = pseudo random number 1

a_2 = pseudo random number 2

a_n = pseudo random number 3

The pseudo generator is defined as the generator that generates secret code. The code generated should not be identical and it is impossible to be identical for every output.

The message m_1, m_2, m_3 …….. added into the generator in time domain can be expressed as [18]:

Unencrypted data = $m_1(t) + m_2(t) + m_n(t) + \ldots\ldots$

$$= \sum_{n=1}^{N} m_n(t) \qquad (2.3)$$

The hash generator produces hash pseudo random code which will multiply to every message in the hash system. This produces [19]:

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

Hashed encrypted data, $H(m) = \sum_{n=1}^{N} a_n \sum_{n=1}^{N} m_n(t)$

$= a_1m_1(t) + a_2m_2(t) + a_3m_3(t) + \ldots\ldots a_nm_n(t)$ (2.4)

Note that the multiplication of $a_nm_n(t)$ is a new element. It is not the same as the previous message (unencrypted message). To understand the mathematical of hashed system linked into practical, we take an example as below [20]:

Message 1: How are you (unencrypted data)

Pseudo random code: AE00, EE99, EDR1023, ……..

The outcome of the message is: HowAE00, areEE99, youEDR1023

: 0045AE00#008EE99#865EDR1023

Note that the '#' represents a space. In this example, symbol '#' is used. But in reality, it may change to other symbols. The symbols can change as the number of iterations increased for new incoming message. Remember that only one cycle of iteration is used for a particular message. The new message coming in will use difference codes and hence generate new message code.

When the messages are placed in order or in series, they form a cryptography system. When the messages are in cryptography, they cannot be altered especially the position. There is no way return the message into hash process. The message has to re-hashed again from the beginning if the mistake is found.

Putting the messages into cryptography order is a job of algorithm. Again, this is controlled by a complex programming in mathematic form. The cryptography mathematical analysis can be understood by looking into the following example [18]:

let $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 2 & 1 & 5 \end{bmatrix}$ = code for cryptography

$\begin{bmatrix} 31 & 82 & 100 & 8 \\ 50 & 113 & 153 & 16 \\ 56 & 116 & 129 & 16 \end{bmatrix}$ = hashed message

The code for cryptography will place in order to generate a series of code that can be used to multiply with hashed message. Thus, multiply with identity matrix [19]:

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

$$= \left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 3 & 4 & 0 & 1 & 0 \\ 2 & 1 & 5 & 0 & 0 & 0 \end{array}\right]$$

$$= \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -11/S & 7/S & 1/S \\ 0 & 1 & 0 & 2/S & 1/S & -2/S \\ 0 & 0 & 1 & 4/S & -3/S & 1/S \end{array}\right]$$

$$= \begin{bmatrix} -11/S & 7/S & 1/S \\ 2/S & 1/S & -2/S \\ 4/S & -3/S & 1/S \end{bmatrix} \times \begin{bmatrix} 31 & 82 & 100 & 8 \\ 50 & 113 & 153 & 16 \\ 56 & 116 & 129 & 16 \end{bmatrix} = \begin{bmatrix} 13 & 1 & 20 & 8 \\ 0 & 9 & 19 & 0 \\ 6 & 21 & 14 & 0 \end{bmatrix}$$

The last matrix results are the cryptography order for the hashed message. It may be read by the machine from row to row as: 13120809190621140

2.4 Algorithm for Hashed Cryptography

The algorithm is a computer way to show how the hash encryption works. The algorithm can be presented in many ways. In many ways means using differences types of programming languages like Java, C++, Python and so on. It is depending on the convenient of the programmer.

Some languages the programmers choose may have limited functions in the library. For example, if programmer choose to use FORTRAN, then it is impossible for user to present best graphical solution to show the hashed cryptography encryption [18].

On the other hand, if the programmer chooses others programming languages like Visual Basic, C++ or C, a best graphical design may be available to describe the encryption operation using hash function.

For algorithm presentation, it is not necessarily having to be a complete programming. But, the main parts of the program that reflect the hash function and cryptography function must be shown.

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

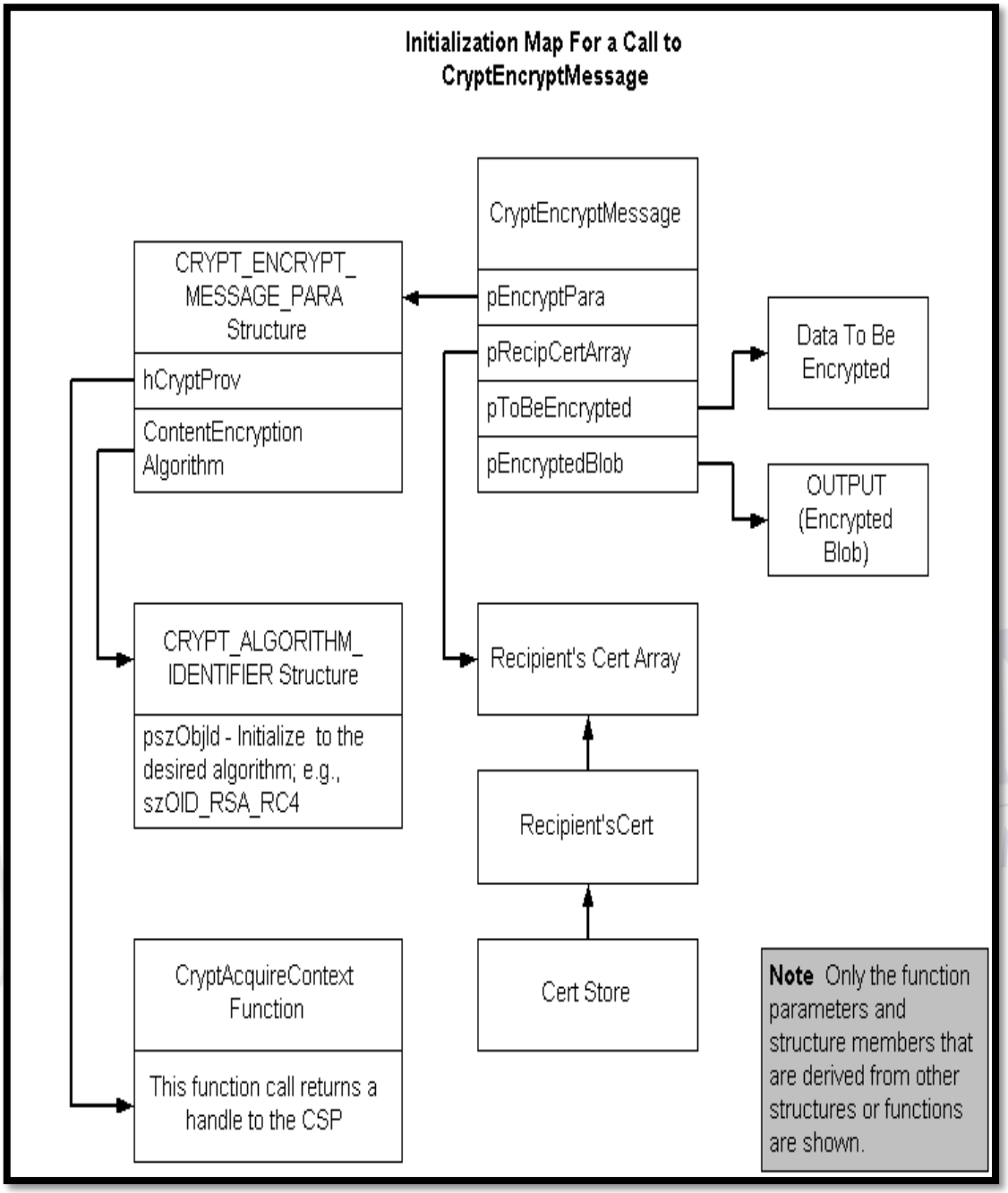

Figure 2.2: General hashed cryptography encryption [19].

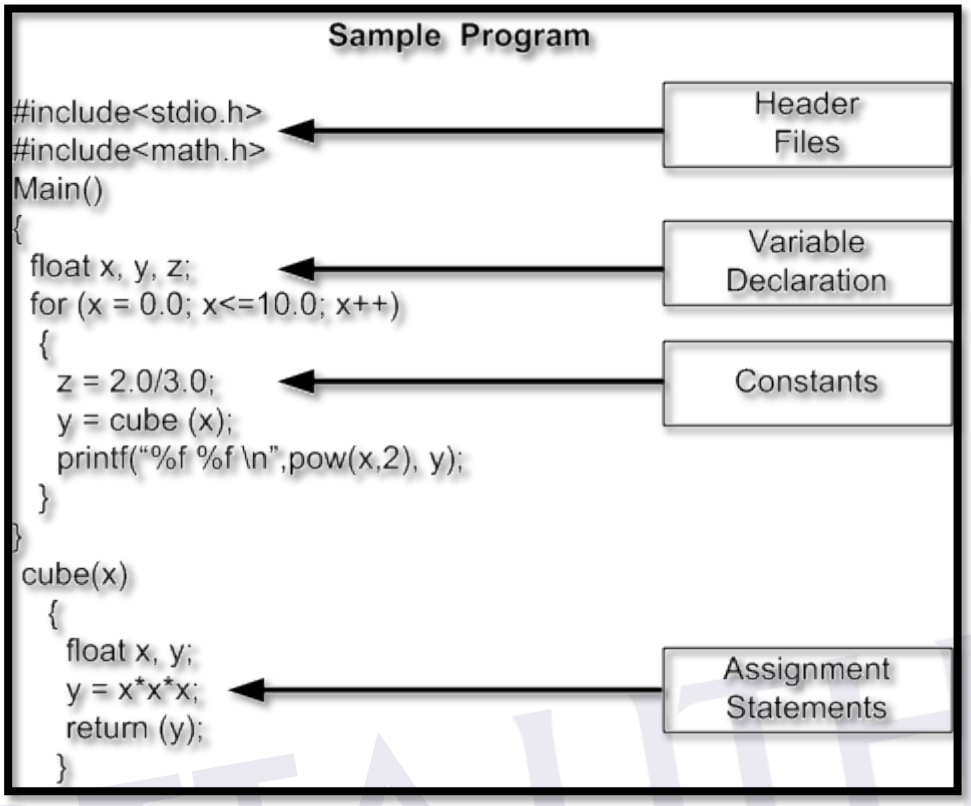

Figure 2.3: Sample program for hash functions [20]

Figure 2.2 shows the general hash function to encrypt the message whereas Figure 2.3 shows the sample program written in C to works as hash that receives the data or message. Figure 2.3 also parts of the programming language used in Figure 2.2. Thus, explanation toward Figure 2.3 is much better than in Figure 2.2 [21].

As seen in Figure 2.3, the programming indicates various functions in C that can be used to program the hash function. From the programming, cube (x) is a single matrix variable. This matrix will hold the assignments (data) temporary stored into the memory. The multiplication in the programming indicates an assigned pseudo code for hash and the results will be stored back into cube (x) variable [22].

Using the for ( ) loop function, the iteration can be controlled to read and assigned in few number of times. The for ( ) loop function is a powerful looping function. It can be controlled by assigning a starting value and end with final value. The for ( ) loop also can be represent summation in mathematics [23]

2.5 Comparison of Hashed encryption with Keyed encryption

Hash security system is very straight forward. There is no addition function like keys have to generate. One-way of generating the secret code is fast and effective. No other algorithms required to add key or retrieve the key content.

The ordinary encryption uses key method to encrypt the data. This creates two types of keys. One is for public and second is for private. Introducing the keys concept is useful and secure, but in other way round it is complicated and not easy to implement.

The following shows the advantages of hashing [24]:

- Simple to hash and no additional keys required
- Straight forward and no complicated algorithm
- Hash and hash can be map together

The disadvantages of hashed encryption are [25]:

- Limited size of message length
- Require high processor speed if the number of messages are increased

The key encryption system is shown in Figure 2.3.

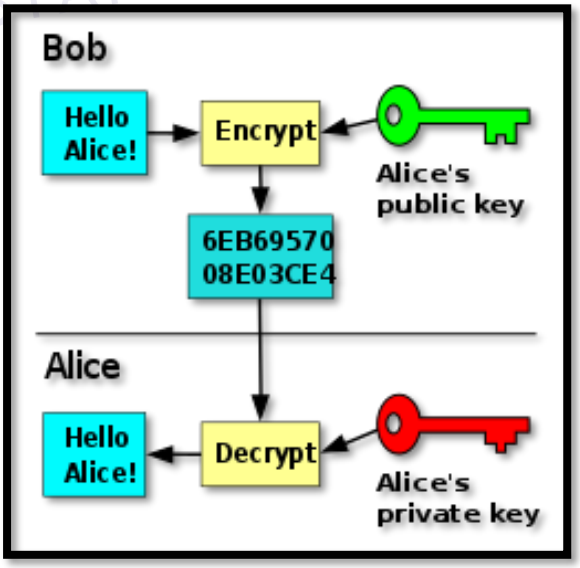

Figure 2.4: Key encryption system [26]

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

The key encryption quite similar to the hash encryption except that a key is generated each time the encryption process take place.

As seen in Figure 2.4, Bob and Alice have data to be encrypted. They send the data for encryption. Once the encryption is complete, Bob and Alice have their own key to protect the data. The key content username and password. This is additional protection that added into the system to secure the data. The key can be shared depending on the types of keys generated.

The key encryption method is very secure except that [27]:

- The key generated is not an easy algorithm
- At the receiver, decryption process will take place. This creates additional works to the system.
- When more data presents in the network, the system will become more complex and difficult to handle.

2.6 Reviews Other Related Research

Encryption process had been introduced a secure communication is needed. There were many researchers in the past had did a great job on the encryption. This section will present some of the latest encryption system. The rest of the encryption systems will be summarized into a table.

presented a review of hash function in cryptography method [28]. The paper has summarized the idea and concept of cryptography hash function using a simple diagram. Below is the diagram proposed in the paper for reader to understand the hash function in cryptography.

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

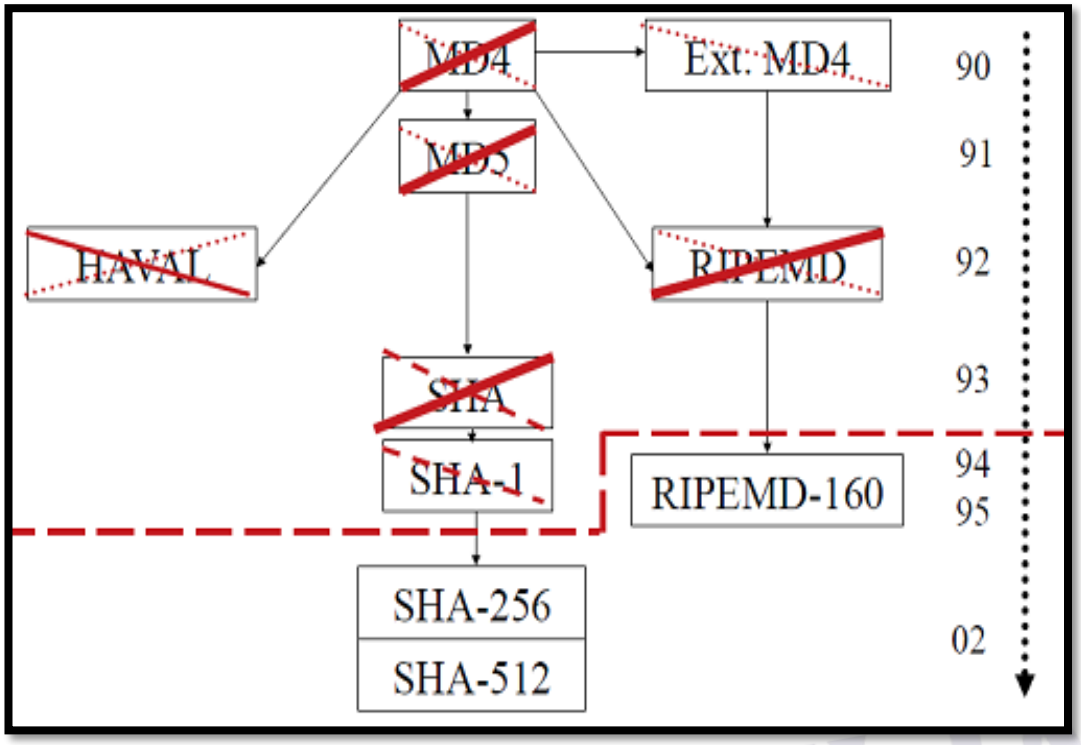

Figure2.5: Cryptography hash function

Based on the proposed diagram, there are several messages waiting for hash. These messages are placed in the hashed and then come out with hashed encryption. After the hash is produced, the block will be deleted and the hashes are sent for storage.

presents the important function contributes by hash in the cryptography system [29]. The paper explains in detail about hash functions from the unencrypted message turned in encrypted message. To make people understand the function, the paper presents the following concept.

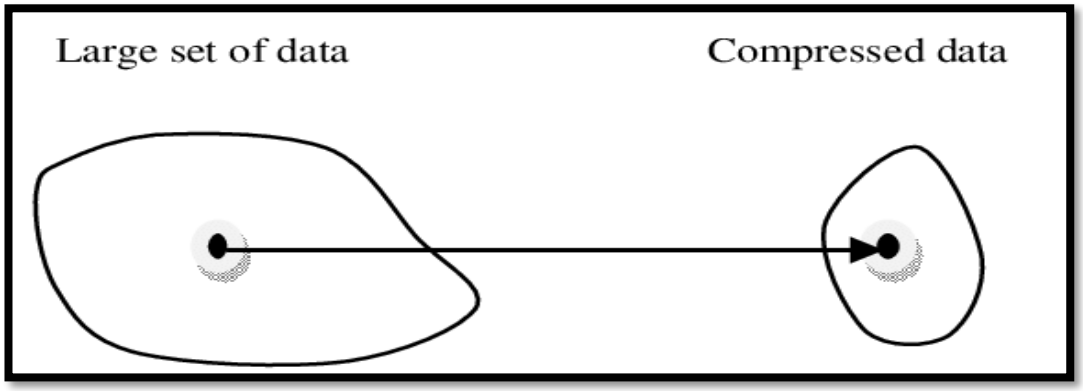

Figure 2.6: Analogy of hash function

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

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

PTTA UiTM PERPUSTAKAAN TUNKU TUN AMINAH

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, 2017.

21. Ooi Chan Sii, Theory and Practical Implementation of Data Encryption, Longman, New York, 2016.

22. Luios. H and Tan Cheng Wa, Introduction to Hash Cryptography Data Protection, Longman, New York, 2017.

23. S.K. Lee, K.C. Tan and Sandra. H, "Hash Security Enhancement", *IEEE Trans on Data Communications*, Vol. 29, Issue 42, 2017.

24. Lee Gao Xian and Hui.L "Cryptography Design and Control System", *IEEE Trans on Computer Science and Technology*, Vol. 1, Issue 20, 2017.

25. Chong Siaw Yuan, Enhance Security using Hash, Wiley and Sons, London, 2017.

26. Janet. L, Advanced Design of Hash System, Longman, New York, 2016.

PTTA UTHM PERPUSTAKAAN TUNKU TUN AMINAH

27. Qian Xian and Long.S, Basic Hash and Cryptography Design System, Pearson, New York,2016.
28. Rajeev Sobti and Geetha Ganesan, "Cryptography Hash Function: A review", *International Journal of Research Gates*, Vol. 11, Issue 10, 2016
29. Swathi Edem, G. Vivek and G. Sandhya, "Role of Hash Function Cryptography", *International Journal of Research Gates*, Vol. 1, Issue 20, 2015
30. Richa Purohit, Upendra Mishra and Abhay Bansal, "Design and Analysis of a New Hash Algorithm with Key Integration", *International of Computer Applications*, Vol. 18, No. 1, 2011
31. Rudiger and Stefan, "Cryptography Hash Functions Recent Results", *IEEE Trans on Data Communications*, Vol. 22, Issue 12, pp. 1 – 23, 2017
32. Esra'a Sameer Al-Rawashdeh, Performance Analysis for Hashing Over Encrypted Data Techniques, A Thesis Presented by Department of Computer System, University Middle East, 2017
33. Prof Mukund, R. Joshi and Renuka Avinash, "Network Security with Cryptography", *International Journal of Computer Science and Communications*, Vol. 4, Issue 1, 2015
34. George Hatzivasillis, Password Hashing Status, *Article of MDPI*, 2017

PTTA UTHM
PERPUSTAKAAN TUNKU TUN AMINAH