Analysis of algorithms magenta with 128 bit key length accompanied by shifting hash securing data

Riandy Yap

Faculty of Computer Science and Information Technology, University of North Sumatra, Medan, Indonesia

rianz12junior@gmail.com

Abstract. The rapid developments in the computer world today has created the computer network that is so big and spacious. This network is used as a means of spreading information without knowing the law, distance and time. For that crime against the computer is also growing and increasing. This caused unrest amongst computer users (user) for key data held is considered to be unsafe and allows it to be stolen or intercepted by others. In the communication between the two sides, there is a guarantee stating that the communication occurs has been safe from the threat of a third party. The presence of a third party in a communication can interfere with the comfort of both parties. These third parties are able to retrieve important information from the communication that is going on. This course will be very detrimental to the first and second parties. On this basis the need for a technique for securing information, messages or data. To avoid this crime, it is necessary to have a security against hardware and software. Merging encryption method Cryptographic Hash Shifting Magenta and is expected to be a good solution for a method of data scrambling and key, so as to secure the data that have later. To avoid break-ins referred to above, it is necessary a good study so as to generate a key code randomization method was good and is not expected to be compromised by those who are not interested. On this basis the need for a technique for securing information, messages or data. To avoid this crime, it is necessary to have a security against hardware and software. Merging encryption method Cryptographic Hash Shifting Magenta and is expected to be a good solution for a method of data scrambling and key, so as to secure the data that have later. To avoid break-ins referred to above, it is necessary a good study so as to generate a key code randomization method was good and is not expected to be compromised by those who are not interested. On this basis the need for a technique for securing information, messages or data. To avoid this crime, it is necessary to have a security against hardware and software. Merging encryption method Cryptographic Hash Shifting Magenta and is expected to be a good solution for a method of data scrambling and key, so as to secure the data that have later. To avoid break-ins referred to above, it is necessary a good study so as to generate a key code randomization method was good and is not expected to be compromised by those who are not interested. it is necessary to have a security against hardware and software. Merging encryption method Cryptographic Hash Shifting Magenta and is expected to be a good solution for a method of data scrambling and key, so as to secure the data that have later. To avoid break-ins referred to above, it is necessary a good study so as to generate a key code randomization method was good and is not expected to be compromised by those

who are not interested. it is necessary to have a security against hardware and software. Merging encryption method Cryptographic Hash Shifting Magenta and is expected to be a good solution for a method of data scrambling and key, so as to secure the data that have later. To avoid break-ins referred to above, it is necessary a good study so as to generate a key code randomization method was good and is not expected to be compromised by those who are not interested.

1. Introduction

In today's world of computer technology, security (security) is a serious problem in securing critical data, so that data can not be stolen, intercepted or misused by unauthorized persons that could harm others. For this reason the government and other institutions is actively trying to secure their critical data as well as possible in order to avoid data breaches by another person. Although it has made various efforts in terms of security, but still there are those who are always trying and managed to break into the data using various means, the method and the existing keys.

2. Encryption and Decryption Algorithm

Encryption is the process by including the initial cryptographic input in the form of plaintext into a particular algorithm along with a key to obtain the output of some ciphertext can immediately understand other people. The encryption process usually involves a change in the form of data into a form that is difficult to be interpreted without a key. Encryption is used to ensure that messages sent can be protected from people who are not authorized to access or read the message. Encryption and decryption generally require the use of some secret information related to the key.

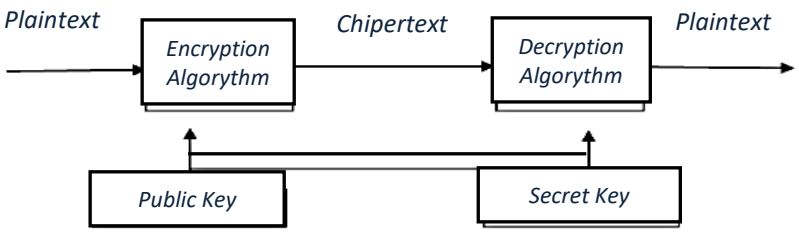

Figure 1. Encryption and Decryption of a secret key

3. Hash Function / Shifting Hash

The hash function is a function that accepts any input string length and converts it into a fixed-length output string (fixed). The resulting hash function is usually written in the notation equation as follows:$\boldsymbol{h} = \boldsymbol{H}(\boldsymbol{M})$ In the above equation, h is the resulting hash value, H is the hash function itself, and M is a message or a message that will be modified and converted into a hash value (hash value). H functions can be applied to any number of data block size, thenH function produces a value (h) with a fixed length (fixed-length output). The function H (x) is calculated for each value of (x) given. And for each value of h is generated, it is not possible to recover the value of (x) such that H (x) = h. That's why this hash function called a one-way function (one-way hash function). Therefore, for every (x) is given, not likely to find y ≠ x such that H (y) = H (x) and could not find a mate (x) and (y) such that H (x) = H (y).

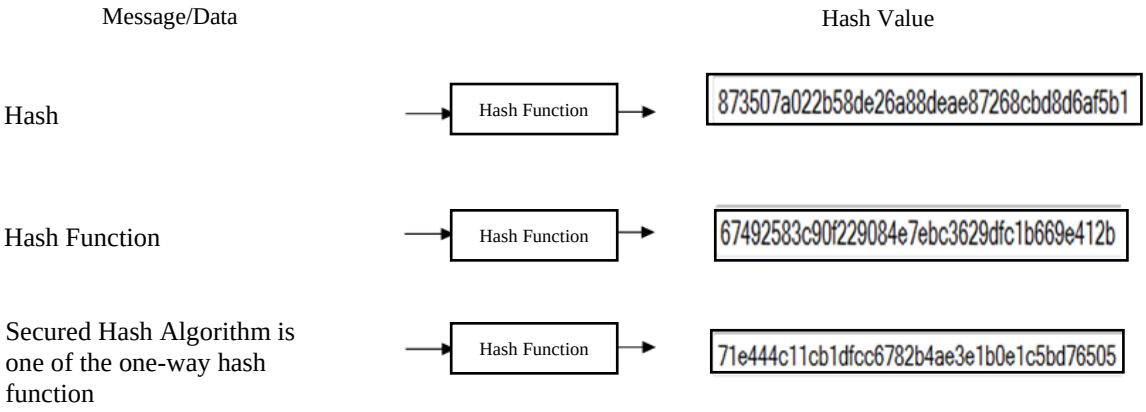

Figure 2, Exampleof Hash functions

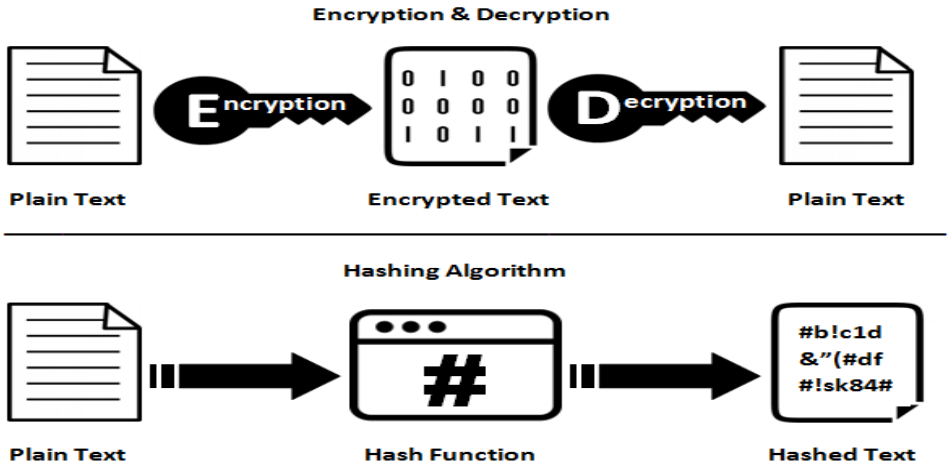

Figure 3. Comparison of Encryption and Hash Functions

In connection with it, in order to better safeguard the security of existing data combined with the hash function algorithm Magenta. At this public key algorithm, everyone can encrypt the data using the recipient's public key that has been generally known. However, data that has been encrypted can only be decrypted using the private key known only to the recipient. To further secure it, the author adds a function of the Function Shifting Hash where the key or data that has been encrypted will be split into a string that sembrang and then convert the string types with formula hashing be output has a fixed length and has a size much smaller than the size of the original string.

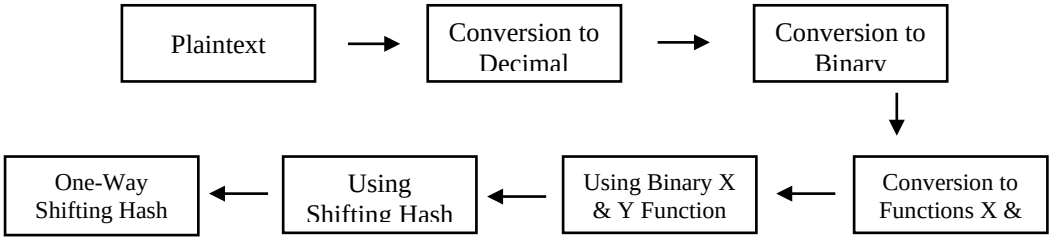

Figure 4. shifting process by using a hash algorithm formula magenta

4. Calculation Method of Algorithms Magenta

MAGENTA algorithm is based on the Fast Hadamard Transform (FHT). However, we replace the addition and subtraction on each node in a random structure by non-linear. Supposeα be a primitive element of the field GF (256) with a generating polynomial p (x) = X8 + X6 + X5 + X2 + 1 and p (α) = 0. For all xε B, defines:

$$f(X) = \begin{cases} \alpha^x x \neq 255 \\ 0 \; x = 255 \end{cases} \quad (1)$$

Then, for all (x, y)ε B2 we define:

$$A(x, y) = F(x \oplus f(y)) \quad (2)$$

and

$$PE(x, y) = (A(x, y), A(y, x)) = (f(y)), f(y \oplus f(X))) \quad (3)$$

For all (x0, ..., x15)ε B16, modification given FHT

$$T(X0, ..., x15) = II(II(II(II(x0, ..., x15)))) \quad (4)$$

wherein II (x0, ..., x15) is defined as

$$II(x_0..., x15) = (PE(x0, x8), PE(x1, x9), ..., PE(x7, x15)) \quad (5)$$

The function T (x0, ..., x15) operating on a single 128-bit parameter and returns the 128-bit output. This operation is very fast, because it can be implemented fully with bit operations. For all X = (x0, ..., x15)ε B16, defined

$$X_e = (X0, x2, ..., x14)$$

and

$$X_0 = (X1, x3, ..., x15)$$

ie, Xe consists of byte X with even index and Xo consists of byte X with an odd index. The function C consists of repeated application of variant FHT, and recursively defined for j ≥ 1 and all (x0, ..., x15) with

$$C^{(J+1)}(x_0..., x15) = T((X0, ..., x_7) \oplus Ce(j), (x_8, ..., x_{15}) \oplus Co^{(J)}) \quad (6)$$

where the initial value of C (1) = T (x0, ..., x15). For every number fixed in R, we define

$$E^{(R)}(X0, ..., x15) = Ce(r) \quad (7)$$

Initially, MAGENTA designed with r = 7: However, during the analysis by SIT GmbH [5, Appendix] was found using r = 7 makes possibility chosen plaintext attack. It is recommended that the number of revolutions is reduced to 3; and analysis in the following chapters show that the best of our knowledge this selection did not produce a significant weakness of the overall cryptographic block ciphers.

Therefore, we set r = 3.

MAGENTA complete block cipher Feistel construction famous exploit using the function E (3) as a basic module cyrypto. For x = (x0, ..., x15) ε B16 and y = (y1, ..., Y7) ε B8, one round Feistel defined as

$$Fy(X) = ((X8, ..., x15), (x0, ..., x7) \oplus E(3)(x8, ..., x15, y0, ..., Y7) \quad (8)$$

Let M = (x0, ..., x15) εB16 into one block of ciphertext (128 bits). MAGENTA algorithms supported and followed three key sizes:

128 bit: K = (K1, K2),
192 bits: K = (K1, K2, K3),
256 bit: K = (K1, K2, K3, K4),

where K1 = (y0, ..., Y7), K2 = (y8, ..., Y15), K3 = (y16, ..., y23), and K4 = (y24, ..., y31). MAGENTA algorithm uses Feistel six or eight rounds, where each round using a different key part. The algorithm is given by

$$Enck(M) = \begin{cases} F_{K_1}(F_{K_1}(F_{K_2}(F_{K_2}(F_{K_1}(F_{K_1}(M)))))) \text{ if } K = (K1\ K2)\ \varepsilon \\ F_{K_1}(F_{K_2}(F_{K_3}(F_{K_3}(F_{K_2}(F_{K_1}(M)))))) \text{ if } K = (K1\ K2\ K3)\ \varepsilon \\ F_{K_1}(F_{K_2}(F_{K_3}(F_{K_4}(F_{K_4}(F_{K_3}(F_{K_2}(F_{K_1}(M)))))))) \text{ if } K = (K1\ K2\ K3\ K4)\ \varepsilon \end{cases} \quad (9)$$

Due to the palindromic property of the equation 9 given in section 9, decryption functions can easily be expressed in terms of an encryption function with

$$dec_K(M) = V(Enck(V(M))), \quad (10)$$

where $V(x_0 \ldots x_{15}) = (X_8, x_9, \ldots, x_{15}, x_0, x_1, \ldots, x_7)$,

5. Conclusion

After analyzing the existing processes, the process of hashing algorithms combined with the method of calculation of Magenta can add strength to megamankan data to be encrypted to the recipient of the information, but in the form of a one way process that can be understood by the recipient of the message or information. Of shifting hash function that will provide the output in the form of a string of smaller size (depending on the number of shifts determined whether the shift 1,2, or 4) in order to save memory stored data.

6. References

[1] Andrias, T. (2012, November Sunday). Definition and Examples Cryptography (Cryptography) with Encryption and Decryption Process. Retrieved from Search Science: http://asalkena.blogspot.co.id/2012/11/pengertian-dan-contoh.html

[2] Ary, NA (2016, November Wednesday). Public Key Cryptography System weakness. Retrieved from Swiper Of The Net: http://kejarbelajar.blogspot.co.id/2016/11/kelemahan-sistem-kriptografi-kunci.html

[3] Babys, JY (2013). Analysis Aspects of Computer Network Security. National Seminar on Informatics (semnasIF), 7.

[4] Maizarti. (2011, April). Symmetric Cryptography. Retrieved from Forum for Science Network: https://maizarti.wordpress.com/2011/04/12/kriptografi-simetris/

[5] Purba, RA (2014). In Encryption Hash Function Analysis Idea To Record Information Security. Computer Science Research and Its Development Journal, 21-32.

[6] Rufaida, R. (2009). Hash functions and Collision Resolution Method. Department of Informatics ITB.

[7] Saso, J. (2005). Data Security Information using Classical Cryptography. DYNAMIC Information Technology Volume X, 3, 161.

[8] Revelation, F., Rahangiar, AP, & Fretes, F. d. (2012). Application of Joint RC4 algorithm and BASE64 Security System On E-Commerce. National Seminar on Information Technology Application, 2012, A47-A52.

[9] Wibisono, SH, & Santoso, D. (2010). Cryptography Application Program Design Using Magenta algorithm with a key length of 128 bits. Comtech Vol 1 No. 1, I, 216-221.