Journal of Computer Science, Information Technology and Telecommunication Engineering
Vol. 1, No. 1, March 2020, pp. 31~36
ISSN: 2721-3838, DOI: 10.30596/jcositte.v1i1.4359

Combination Of Hybrid Cryptography In One Time Pad (OTP) Algorithm And Keyed-Hash Message Authentication Code (HMAC) In Securing The Whatsapp Communication Application

Fanny Ramadhani[1], Umaya Ramadhani Putri Nasution[2], Lutfi Basit[3]
[1]Department of InformationTechnology, Universitas Muhammadiyah Sumatera Utara, Indonesia
[2]Department of Magister Informatics, Universitas Sumatera Utara, Indonesia
[3]Department of Communication, Universitas Muhammadiyah Sumatera Utara, Indonesia

ABSTRACT

Whatsapp is a cross-platform messaging application that allows us to exchange messages without SMS fees, because WhatsApp uses the same internet data package for email, web browsing, and more. The WhatsApp application reportedly has improved the security system of applications that are end to end encryption (E2EE). This proves that the WhatsApp manager paid considerable attention to privacy and security issues for its users. In addition, it also implies an important matter where business actors have begun to realize that the application of cryptographic services is part of a very promising business strategy or even determines the present and future consequences. The consequence of implementing E2EE is the description encryption process that takes place at the application layer (OSI layer). Cryptography is a study that studies methods to send messages in secret (that is, encrypted or disguised) so that only the intended recipient of the message can decode and read the message. For this reason, cirptography is one method that can implement E2EE on whatsapp. One Time Pad (OTP) is a type of symmetry algorithm, each key is only used for one message. If the key is random (cannot be reproduced) and only used once, then the algorithm is perfectly safe. The MAC (Message Authentication Code) is an identifier to prove the authenticity of a document obtained by using meaningless messages obtained from processing some of the contents of the document using a private key.

Keyword: WhatsApp, Kriptografi, E2EE, One Time Pad (OTP), Message Authentication Code (MAC)

Corresponding Author:
Fanny Ramadhani,
Department of Information Technology,
Universitas Muhammadiyah Sumatera Utara,
Jalan Kapten Muktar Basri No 3 Medan 20238, Indonesia.
Email: fannyramadhani@umsu.ac.id

1. INTRODUCTION

Whatsapp is a cross-platform messaging application that allows us to exchange messages without SMS fees, because WhatsApp uses the same internet data package for email, web browsing, and more. The WhatsApp application reportedly has improved the security system of applications that are end to end encryption (E2EE)[9]. This proves that the WhatsApp manager paid considerable attention to privacy and security issues for its users. In addition, it also implies an important matter where business actors have begun to realize that the application of cryptographic services is part of a business strategy that is very promising or even determines the present and future [4][7].

The consequence of implementing E2EE is the description encryption process that takes place at the application layer (OSI layer). The only technique in computer science that is used to secure data is cryptography. Cryptography is a study that studies the method for sending messages in secret (that is, encrypted or disguised) so that only the intended recipient of the message can decode and read the message. For this reason, cryptography is one method that can implement E2EE on whatsapp.

Based on the type of key cryptographic algorithms are divided into two types, namely symmetry and asymmetry cryptographic algorithms. Symmetry cryptographic algorithm is an algorithm that uses

the same key when doing the encryption and decryption process, while the asymmetric cryptographic algorithm is an algorithm that has two keys, namely private key and public key.

One Time Pad (OTP) is a type of symmetry algorithm, this algorithm was invented by Major Joseph Maugborne and Gilbert Vernam in 1917. Each key is only used for one message. If the key is random (cannot be reproduced) and only used once, then the algorithm is perfectly safe. But if the key is used for two or more messages, then security is no longer guaranteed [5].

MAC (Message Authentication Code) is an ID to prove the authenticity of a document that is obtained by using a meaningless message obtained from processing part of the contents of the document using a private key. Technically, (half) the document is processed using a private key to produce a MAC message, which is simpler than the contents of the document. This MAC message is then attached to the document and sent to the recipient. The recipient then uses the same key to obtain the MAC message from the document received and compare it with the MAC message received [8].

Siti Kholilah Pulungan, (2017) uses a combination of two One Time Pad (OTP) and Micali Goldwasser algorithms in the implementation of hybrid cryptography. His research aims to increase knowledge and references about how the One Time Pad algorithm works in securing text data and how the Micali-Goldwasser algorithm works in securing keys used to secure data [5].

Patra Abdala, Mohammad Andri Budiman, Herriyance, used the Vernam Chiper cryptographic algorithm and Data Encryption Standards (DES) on an Android-based chat application [1]. Jhon Daniel Situmorang, (2013) uses the Keyed-Hash Message Authentication Code (MAC) algorithm in chat-based text messages. Mechanisms that provide message integrity checks based on secret or private keys are also commonly known as Message Authentication Codes. Usually, Message Authentication Code is used when two parties share a secret or private key to authenticate messages that are transmitted between these parties [2]. In this paper the author tries to combine cryptographic one-time pad algorithm and message authentication code to optimize data security contained in whattsapp.

2. RESEARCH METHOD

A. One Time Pad

One Time Pad (OTP) is one example of cryptographic methods with symmetric type algorithms. So that in this One Time Pad algorithm the key used for the encryption process can be reused as a key for the decryption process.

To generate a key on the One Time Pad algorithm is done randomly and the length of the number of one time pad keys must be the same as the length of the original text, so that there is no looping of keys during the encryption process. An algorithm is said to be safe, if there is no way to find the plaintext. Until now, only the One Time Pad (OTP) algorithm has been declared unbreakable [5].

1. Key Generating Process

   Random number generator is needed for things like simulations in physics, mathematics, and also very important in cryptography. One method used as a random number generator is the Linear Congruential Generator (LCG) algorithm. Linear Congruential Generator (LCG) represents one of the oldest and most popular pseudo random number algorithms. This algorithm was created by D. H. Lehmer in 1951. The theory of this algorithm is easily understood and can be implemented quickly (Bilqis, 2012). LCG is defined by the following equation (1):

   $$X_n \equiv aX_{n-1} + b(\text{mod } m) \quad (1)$$

   where
   Xn = The nth random number of the series.
   Xn-1 = Previous random number.
   a = Multiplier factor.
   b = Increment.
   m = Modulus.
   The key generator is X_0 which is called bait.

2. Encryption Process

   The encryption process is the process of changing plaintext into ciphertext by using a key with the aim of disguising or encoding plaintext so that unauthorized parties cannot find out the contents of the message. In the One Time Pad algorithm, the encryption process can be done with the following equation (2):

$C_i = P_i + K_i \pmod N$ (2)

3. Decryption process
Decryption process is the process of returning a message in the form of ciphertext into a plaintext message with the aim that the recipient has the right to be able to read the contents of the original message. In the One Time Pad algorithm, the decryption process can be carried out with the following equation (3):

$P_i = C_i - K_i \pmod N$ (3)

Where:
C_i = Ciphertext length.
P_i = Plaintext length.
K_i = Key length.
N = Number of characters.

B. Keyed-Hash Message Authentication Code Algorithm

MAC is the message authentication code. Similar to hash. The hash may already be quite commonly used by web programmers to secure passwords. Hash that is usually used for example MD5. The difference is that MAC uses keys while hashes don't. The use of keys minimizes the possibility of a MAC being falsified.

In general, MAC is a tool for the recipient to find out the sender of the message. Originally, MAC used DES with CBC operating mode (FIPS 81). But, MAC with encryption base was no longer developed. Used now is the Hashed Message Authentication Code (HMAC). In HMAC, the key is added to the message and then the hash value is taken. With HMAC we get integrity (data is not modified) and authentication (to prove who the sender really is). The HMAC can indicate who sent it, depending on the algorithm used.

With the above definition, the easiest way to create a MAC or HMAC is to connect our message with the key we have, then retrieve the hash value:

K = key
M = message
H = hash function, for example MD5 or SHA1

The output of the hash function is also called the hash value (message hash). In the above equation, h is the hash value or message digest of the H function for input M. In other words, the hash function compresses any message of any size into a message digest whose size is always fixed (and is shorter than the original message length). The picture shows an example of 3 different length messages always hashed to produce a fixed length concise message (in this example a concise message is expressed in hexadecimal code that is 128 bits in length. One decimal hex character = 4 bits). Other names for hash functions are compression or contraction (compression function), fingerprint, cryptographic or cryptographic checks, checking message integrity or message integrity check (MIC), manipulation of code manipulation or manipulation detection code (MDC) [2]. In general, the HMAC algorithm can be explained by the equation below:

HMACK (m) = h ((K opad) h ((K ipad) m)) (4)

Where
HMACk (m) : is the HMAC value of the message to be authenticated.
H : hash function used
K : Private key known by sender and recipient.
Opad : Outer pad (0x5c5c ... 5c)
IPad : Inner pad (0x36363..36)
M : message to be authenticated

Where K is the private key known to the sender and receiver, h is the hash function used, m is the message to be authenticated, opad is 0x5c5c5c ... 5c and ipad is 0x36363 ... 36 of the same length

3. RESULTS AND DISCUSSION

In this paper, the author tries to combine cryptographic one time pad (OTP) algorithm and message authentication code (MAC) to optimize data security contained in whattsapp. In this paper, whatsApp security is designed by combining the OTP and MAC algorithms with the waterfall model. The waterfall model is shown in Figure 1.

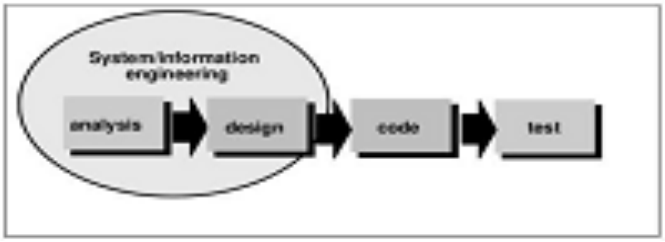

Figure 1. Waterfall Method Diagram

A. Application of One Time Pad and Keyed-Hash Message Authentication Code

As for this paper the authors made a combination of hybrid cryptography, namely one time pad (OTP) and keyed-hash message authentication code (HMAC).

- The encryption process and description of the one time pad (OTP) method.

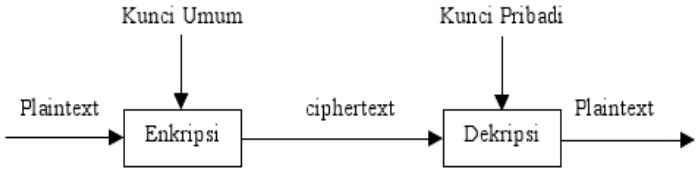

Figure 2. Data Decryption Encryption Method

- Process the keyed-hash message authentication code (MAC) method.

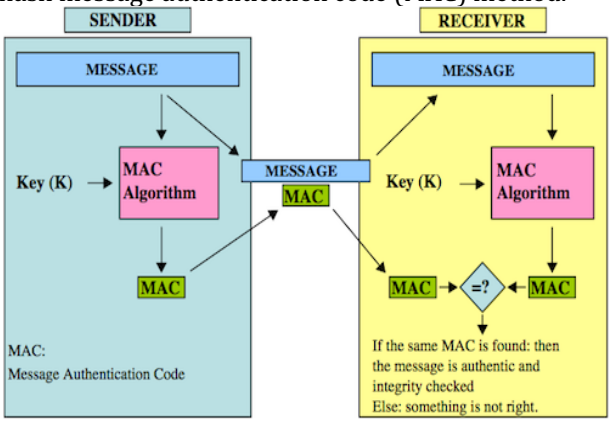

Figure 3. The method of keyed-hash message authentication code

In Figure 3 below, we can see the combination of cryptographic processes of hybrid one time pad (OTP) and keyed-hash message authentication code (MAC).

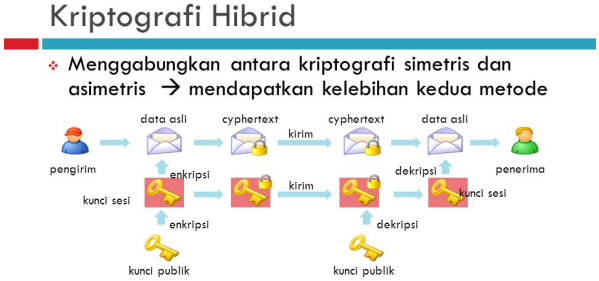

Figure 4. Application of Hybrid Cryptography

The application of the one time pad method here is used to lock the message when chatting between the sender and recipient of the message. So that if the message is considered confidential, it is not easy to spread irresponsibly. Meanwhile, the application of the keyed-has message authentication code method here as a key generator for authentic confidential orders. This keyed-hash method is like the md5 hash process. Following is the implementation of the hybrid cryptographic combination application.

Table 1. The Result Comparision

Plaintext	**GAMAS SIAGA 1**
OTP Kye	
Ciphertext	
Hash MAC	
Public key	N = 1643, Y = 305
Cipherkey	1059, 1406, 983, 218, 1369, 953, 1512, 70, 1120, 766, 652, 782, 1599, 526, 221, 1301, 1594, 714, 805, 996, 786, 1414, 823, 785, 1301, 743, 1077, 1236, 470, 886, 187, 420, 855, 158, 661, 948, 978, 1220, 294, 577, 771, 40, 523, 1236, 735, 334, 1497, 947, 236, 1036, 428, 812, 160, 1089, 1468, 1008, 259, 749, 771, 841, 678, 188, 1372, 1084, 788, 361, 42, 1421, 1182, 347, 1137, 1321, 945, 219, 1129, 802, 1467, 1362, 1626, 115, 784, 1377, 693, 1263, 805, 679, 358, 749, 213, 176, 46, 679, 1402, 831, 1338, 1076, 272, 175, 1341, 1536, 1584, 1098, 941, 1334, 1089, 1521, 1500, 908, 1195, 1036, 202, 184, 361, 1637, 46, 857, 1218, 1104, 1022, 319, 91, 1600, 1475, 395, 520, 717, 1630, 11, 1051, 505, 1183, 1064, 1600, 305, 440, 1427, 1485, 727, 1096, 81, 1338, 13, 555, 487, 969, 24, 696, 844, 964, 1341, 1491, 435, 123, 1230, 113, 523, 1544, 1278, 791, 1261, 135, 1150, 290, 590, 943, 635, 99, 908, 399, 944, 939, 916, 736, 425, 1495, 685.
Privat Key	P = 31, Q = 53

4. CONCLUSION

From the results and discussion, it can be concluded that the security of WhatsApp chat is more secure because double security is done, namely the One Time Pad algorithm and Keyed-Hash Message Authentication Code.

REFERENCES

[1] Abdala,Patra., et, al ,2016, *Implementasi Algoritma Kriptografi Vernam Chiper dan Des (Data Encryption Standard) pada Aplikasi Chating Berbasis Android,* Jurnal Ilmiah Core IT e-ISSN: 2548-3528 p-ISSN : 2339-1766.

[2] Daniel Jhon Situmorang., et, al, 2013, *Implementasi Algoritma Keyedhas Message Authentication Code (HMAC) pada pesan teks berbasis Chatting,* Pelita Informatika Budi Darma ISSN : 2301-9425, Volume: III No :2, April 2013.

[3] Husein,,Mohammad, 2014 *Kombinasi algoritma Rivest Shamir Adleman (Rsa) Dengan Metode One Time Pad(Otp) Untuk Mengoptimalkan keamanan Data*.

[4] Ismu, Hadi, Muhammad., et, al, 2017, *Known-Plaintext attact terhadap data terenkripsi WhatsApp*. *Hacking and Digital Forensics Exposed 2017 ISSN: 2338 – 0276 Yogyakarta, 5 Agustus 2017*.

[5] Kholilah,Siti. 2017. Implementasi kriptografi hybrid pada algoritma one time pad (OTP) dan algoritma micali-goldwasser. Skripsi. Universitas Sumatera Utara.

[6] Wahyuni,,Ana, *Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid: Diffie-Hellman dan RSA.* Skripsi. Universitas AKI.

[7] Fauzi, F., Al-Khowarizmi, A. K., & Muhathir, M. (2020). The e-Business Community Model is Used to Improve Communication Between Businesses by Utilizing Union Principles. *JITE (JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING)*, *3*(2), 252-257.

[8] Lubis, A. R., Lubis, M. & Al-Khowarizmi. (2020). Optimization of distance formula in K-Nearest Neighbor method. *Bulletin of Electrical Engineering and Informatics*, *9*(1), 326-338.

[9] Lubis, A. R., Lubis, M., & Azhar, C. D. (2019). The Effect of Social Media to the Sustainability of Short Message Service (SMS) and Phone Call. *Procedia Computer Science*, *161*, 687-695.