Combination of One Time Pad Cryptography Algorithm with Generate Random Keys and Vigenere Cipher with EM2B KEY

A I Permana[1], Tulus[2], Z Situmorang[3]
{raden.andraperm@gmail.com[1], tulus@usu.ac.id[2], zakarias65@ust.ac.id[3]}

Master Programs Faculty of Computer Science and Information Technology University of North Sumatera, Jl. Universitas No.9, Medan, Sumatera Utara 20222, Indonesia [1]
Faculty of Math and Science University of North Sumatera, Medan, Indonesia, Jl. Bioteknologi No.1, Medan, Sumatera Utara 20155, Indonesia[2]
Saint Thomas Catholic University, Medan, Indonesia, Jl. Setia Budi 479-F, Tanjung Sari, 20132, Medan, Sumatra Utara, Indonesia[3]

Abstract. Today, the development of information systems that focus on the use of information and communication technology is the basis for organizations to improve their competitiveness. Similarly, sending or exchanging messages is something that often happens in the world of information technology. The development of information and communication technology has triggered many parties to continue to develop the speed of sending messages, namely through the internet. Along with the development of the internet, it became a scourge for those who were haunted by worry about the security of the messages sent. The message sometimes often contains important information even very confidential and must be maintained. To maintain the security of the message, it can be done using cryptographic techniques. That is encrypting the message to be unlike the original message. In the cryptography, many algorithms are used to encrypt, including One Time Pad and Vigenere Cipher. Basically these two algorithms use the key to do encryption, for this reason, the author tries to research how to generate random keys on the One Time Pad algorithm and combined with the Vigenere Cipher algorithm with EM2B key.

Keywords: Cryptography, One Time Pad Algorithm, Generate Random Keys, Vigenere Cipher Algorithm, EM2B Keys, Security.

1 Introduction

Theft of information often occurs when sending a message with a third party who wants to know the message information sent from the sender to the recipient of the message. The third-party trying to find out information from the message sent by the sender to the recipient is often called Man In The Middle.

In 2011, Stalling W. said that Information Security also strives to maintain the very important data that we have in order to reduce the risks that will occur and increase the benefits obtained from hard work and the chance of an effort that we do.

ICMASES 2019, August 03-04, Samarinda, Indonesia
Copyright © 2020 EAI
DOI 10.4108/eai.3-8-2019.2290723

This threat can result in misuse of information from the message. Other efforts can be by changing the information from the contents of the message sent to the recipient, so that information from the message received by the recipient can be different from the message sent by the sender. The sender of the message feels that the message he sent has been sent well, so does the recipient who feels that he has received the message well. This can occur because there is no authentication from the recipient of the message that the message received is indeed from the actual sender[1]**.**

2 Method

Symmetrical algorithms or also called conventional cryptography algorithms are algorithms that use the same key for the encryption process and the decryption process[2]. The symmetrical cryptography algorithm is divided into 2 categories, namely, flow ciphers and block ciphers[3]. In the flow algorithm, the encryption process is oriented to one bit or one byte of data. As for block algorithms, the encryption process is oriented to a set of bits or bytes of data (per block). Examples of symmetric key algorithms are One Time Pad and Vigenere Cipher.

2.1 One Time Pad

One Time Pad algorithm has a way of working where the recipient of the message has the same key copy as the sender of the message and the key is only used one time for encryption and decryption. After the key is used, the pad (blocknot paper) must be immediately destroyed so that it cannot be used again for encryption and decryption of other messages. The sender and recipient must both have a large and random set of key material, as long as the combination of all messages has been sent[4].
The One Time Pad algorithm formula used is:
Encryption: $\boldsymbol{C_i = (P_i + K_i) \bmod 256}$
Decryption: $\boldsymbol{P_i = (C_i - K_i) \bmod 256}$

Where: Ci = index decimal character ciphertext
Pi = index decimal character plaintext

Here the author will use modulus 256 instead of 26 because it uses ASCII characters and is not limited to A-Z. The expected results will be more unique than using modulus 26 only.

2.2 Vigenere Cipher

The Vigenere Cipher algorithm uses an alphabet text encoding method using a row of Caesar passwords based on the letters on the keyword. Vigenere Cipher is a simple form of polyial alphabet substitution password. Vigenere Cipher is a form of alphabetic pattern substitution as expressed by Caesar Cipher, but adds a safer key. The advantages of this password compared to Caesar's password and other mono-literal passwords are that these passwords are not so vulnerable to password-breaking methods called frequency analysis. Therefore, Vigenere Cipher is very famous because it is easy to implement. This method is also strong enough to avoid cryptanalysts that use frequency analysis.
The Vigenere Cipher algorithm formula used is:
Encryption: $\boldsymbol{C_i = (P_i + K_i) \bmod 256}$

Decryption: $\boldsymbol{Pi = (Ci - Ki) \bmod 256}$

Where: Ci = index decimal character ciphertext
Pi = index decimal character plaintext

2.3 EM2B

The EM2B key algorithm is an algorithm that functions to convert the main key into a new key that is converted into ASCII characters. The EM2B algorithm develops a simple key generator algorithm to encrypt plaintext. The modulus system of adding plaintext with keys becomes an advantage in the speed of the encryption process. The EM2B algorithm also has an increment key algorithm that works if the key length is smaller than the plaintext length. Increment key is a method for adding key character lengths by summing the two previous key characters and modulated with 256 ASCII-based letters.
EM2B key formula:
$K_{i[new]} = (K_i + K_j) \bmod 256$

Where: $K_{i[new]}$ = index decimal character of new key
K_i = index decimal character of old key
$K_j = (K_i \bmod 26)$

And the EM2B formula also has the increment key formula as follows:
$IncK_i = (K_{i[max]} + K_{i[max -1]}) \bmod 256$

3 Result and Discussion

In this section, we can discuss the combination of one-time pad and vigenere ciphers using the formula described above. We will take a sample plaintext is the title of this paper, Combination Of One Time Pad Cryptography Algorithm With Generate Random Keys And Vigenere Cipher With EM2B Key. We will use the key to my own name, Aminuddin Indra Permana. Here as proof material, the author will use the Visual Studio 2010 programming language as proof of this algorithm combination[5].

Plaintext = Combination Of One Time Pad Cryptography Algorithm With Generate Random Keys And Vigenere Cipher With EM2B Key
Key = Aminuddin Indra Permana

The length of the key is not along the plaintext, then a key extension will be made which will randomize the keys using the formula $K_i = (K_j + K_m) \bmod 256$.
Where: K_i = Key character index
$K_j = K_{i-n}$
$Km = K_{i-1}$
n = initial key length
i = n + 1

And now we can also use the one time pad encryption formula as explained above to encrypt.

Plaintext = Combination Of One Time Pad Cryptography Algorithm With Generate Random Keys And Vigenere Cipher With EM2B Key
Key = Aminuddin Indra Permana¢xæ[¿#Œú cÑ5§(xÝO¼‹ìŽ • ûV8Ä¾Ø;Aèð m¼x•š7LG□²ê®lD□‹Ì´¤¼L¹uí,¢®H□Ë¯aKùe©(³□3×“ß˜
Ciphertext = „ÜÖÐÞÒÅÝ×□·Ž³Ø o¾Ê’ÁÊÛÆÂ_ÙJ{ •jŽÒ8§ x ñý („ú^÷}hvl¡8&ø,q¯Mby ————————————————————ÒÜÊöŽp ¤l’+]Î-²ã«" !º-çR¢å ¸ç0„Ï¸´mÍÉm

If we have got a ciphertext from the encryption above, then we will be able to encrypt it using the vigenere cipher encryption formula described above with the encryption object is the ciphertext that we got earlier. so later we will get ciphertext 2. If the EM2B key is not along plaintext, we will use the key extension formula as mentioned in the increment key of EM2B. After lengthening the key, use the increment key along the plaintext, then we will randomize the key with the EM2B formula[5].

As a key trigger for randomizing keys using the EM2B formula, here the author will take 2 characters from the one-time pad key as the initial trigger to determine the random key, that is ß and ˜. Then we can do the calculation to encrypt again with the formula described above.

Plaintext = „ÜÖÐÞÒÅÝ×□·Ž³Ø o¾Ê’ÁÊÛÆÂ_ÙJ{ •jŽÒ8§ x ñý („ú^÷}hvl¡8&ø,q¯Mby ————————————————————ÒÜÊöŽp ¤l’+]Î-²ã«" !º-çR¢å ¸ç0„Ï¸´mÍÉm
Key = ß˜wV5óÒ± • oN-ëÊ©ˆgF% ————————————————————ãÂ¡€_ >üÛº™xW6ôÓ²‘pO. ìËª‰hG&äÃ¢ • `?-ýÜ»šyX7õÔ³’qP/ Ì«ŠiH'åÄ£,a@ þÝ¼›zY8öÕ´“rQ0îÍ¬
EM2B = î®†^6(üÔÆžvN@ìÞ¶Ž€X0öÎ¦˜pH æ¾°ˆ`8*þÖÈ xPBîà¸ • hZ2 øÐ¨šrJ"èÀ²Šb:,ØÊ¢zRDðâº’j\4 úÒª,tL$êÂ´Œd<.ÚÌ¤|TF-òä¼

Ciphertext 2 = rŠ\.úÁ± • --ÜóðmMtXúã¼□qºÃ"£ë(>Z˜ß2vf¹□xÆL×É ÐÐž«0ö ãùoraÄ„f,0ºHÓFæäFGM°gDMV)ód [žÆ÷z›¼è æ¶G™mé

Plaintext	Generate Random Keys	Ciphertext	EM2B	Ciphertext 2
Combination Of One Time Pad Cryptography Algorithm With Generate Random Keys And Vigenere Cipher With	Aminuddin Indra Permana¢xæ[¿#Œú cÑ5§(xÝO¼‹ìŽ • ûV8Ä¾Ø;Aèð m¼x•š7LG • ²ê®l D□‹Ì´¤¼L¹uí,¢® H • Ë¯aKùe©(³ • 3 ×“ß˜	„ÜÖÐÞÒÅÝ× • · Ž³Ø o¾Ê’ÁÊÛÆÂ_Ù J{ •jŽÒ8§ x ñý („ú^÷}hvl¡8&ø,q ¯Mby ———————— ÒÜÊöŽp ¤l’+]Î-²ã«" !º-çR¢å ¸ç0„Ï¸´mÍÉm	î®†^6(üÔÆžvN @ìÞ¶Ž€X0öÎ¦˜pH æ¾°ˆ`8*þÖÈ xPB îà¸ • hZ2 øÐ¨šrJ"èÀ²Šb:,Ø Ê¢zRDðâº’j\4 úÒª,tL$êÂ´Œd<. ÚÌ¤|TF-òä¼	rŠ\.úÁ± • -- ÜóðmMtXúã¼ • q ºÃ"£ë(>Z˜ß2vf¹ • xÆL×É ÐÐž«0ö ãùoraÄ„f,0ºHÓF æäFGM°gDMV)ó d [žÆ÷z›¼è æ¶G™mé

EM2B Key				

Table 1. Result Encryption

4 Conclusion

From the above results, we can see that the result of this encryption is a random character and not only produces letters from A to Z because it uses modulus 256 which is a number of ASCII characters. And also has been through randomization of keys such as random key generator at one-time pad and EM2B on vigenere ciphers which use 256 modulus of ASCII characters as well. Which is expected to increase a security value in data transmission which is a frightening specter for those who are haunted by anxiety about data theft.

References

[1] R. Rahim *et al.*, “Combination Vigenere Cipher and One Time Pad for Data Security,” *Int. J. Eng. Technol.*, vol. 7, no. 2.3, p. 92, Mar. 2018.

[2] J. Thakur and N. Kumar, “DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis,” *Int. J. Emerg. Technol. Adv. Eng.*, vol. 1, no. 2, pp. 6–12, 2011.

[3] M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel, “An empirical study of cryptographic misuse in android applications,” in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 73–84.

[4] A. M. Elhanafi, “Analisis Dan Penerapan Algoritma Subsitusi, Encoding Triple Base 64 Dan Vigenere Cipher Untuk Keamanan Login Pada Website,” Universitas Sumatera Utara, 2014.

[5] M. E. H. A., P. E. Yunith, and Z. Muhammad, “Implemntasi Algoritma RSA dengan Kunci EM2B dalam Mengenkripsi Pesan. (Semantika),” in *Seminar Nasional Teknologi Informatika*, 2017.