International Journal of Informatics and Computer Science (The IJICS)
Vol 2 No 1, March 2018
ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 26-31

Implementation of Triple Transposition Vegenere Cipher Algorithm and Cipher Block Chaining for Encoding Text

Fitarius Humendru, Taronisokhi Zebua

Department of Computer Science STMIK Budi Darma, North Sumatra, Indonesia

Abstract – Security of confidential text data and personal is very important so that the data is not misused by other parties. Many cryptographic algorithms can be used to secure data to keep the originality of confidential data. This study describes the use of triple transposition vegenere cipher algorithm which is combined with cipher block chaining mode for encoding text data with the aim to optimizing randomize of ciphers generated so that the security of confidential of data text is more optimal.

Keywords – Cryptography, Triple Transposition Vegenere Cipher, Cipher Block Chaining, Data, Text

1 INTRODUCTION

Security of confidential or private data text data nowadays is one of the most important things to do because currently the distribution of information of data is often done. Ignoring securing confidential data is very fatally and can disadvantage the owner of the information itself. One effort that can be done is to utilize cryptographic techniques so that data transmitted through communication channels can be safe[1]. Cryptographic techniques can change two-way communication with the process of encryption and decryption[2]. Using cryptographic techniques can increase data attackers' complexity to find out the original meaning of the data easily.

Data randomization effectively will add complexity to finding the original patterns and meanings of confidential data. This research describes combining the triple transposition vegenere cipher algorithm to perform text encoding and cipher block chaining operation modes used to optimize randomization of encoded text data. Secret text that is secured is encoded based on the triple transposition vegenere cipher algorithm three times the transposition and substitution process, then the resulting cipher binaries will be scrambled again based on the cipher block chaining operation mode.

Implementation of the triple transposition vegenere cipher algorithm and the cipher block chaining operation mode to secure confidential data can generate the more random ciphertext of secret data and can increase the hassle of finding the original pattern and meaning of the text data.

2 THEORY

2.1 Cryptography

Study of mathematical techniques covering data security aspects is generally referred to as cryptography[3][4]. Confusion and diffusion in reconstructing the resulting cipher is the main achievement of cryptographic techniques. Objectives that must be achieved in the application of cryptographic techniques are confidentiality, data integrity, authentication and non-repudiation[5][6].

Cryptographic techniques will encrypt the original data to be a cipher called the encryption process and the decryption process to restore the cipher to be original data. The process of encryption and decryption requires a structured algorithm and the key that used to encryption and decryption processes.

2.2 Triple Transposition Vegenere Cipher Algorithm

Tiple Transposition Vegenere Cipher (TTVC) algorithm is the development of the vegenere cipher algorithm. This algorithm will encryption and decryption a data by doing two processes is transposition and substitution. this process is doing three times. Transposition process is doing based on columnar transposition and substitution is doing based on vegenere cipher. Each process is used a different key, meaning that there are three keys for the substitution process and three keys for transposition processes[7].

Workflow of Triple transposition vegenere cipher in the encryption and decryption process can be presented in Figure 1 below.

ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 26-31

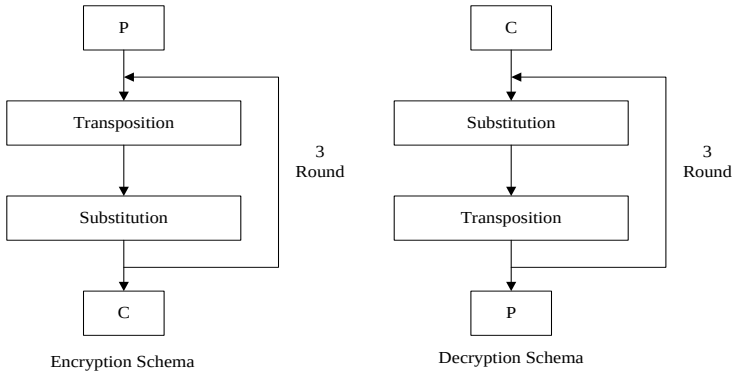

Figure 1. Encryption and Decryption Scheme Based on Triple Transposition Vegenere Cipher
Source : M. Linda Caroline, 2011[8]

Based on Figure 1 above, it can be seen that the original data encryption process is done alternately starting from the transposition process based on columnar transposition (T) and substitution (S) is doing based on the vegenere algorithm. This process is carried out in three rounds with different keys for each process. The decryption process is the opposite of the encryption process, the key used remains the same as the key of an encryption process. The formulations for the encryption and decryption process[8] are :

Encryption formulation : C = (S3(T3(S2(T2(S1(T1(P)))))) .....(1)
Decryption formulation : P = (T1(S1(T2(S2(T3(S3(C)))))) .....(2)

Formulation that wi use for substitution is vegenere algorithm formulation are :
Encryption formulation = Ci = (Pi + Ki) mod 256 .....(3)
Decryption formulation = Pi = (Ci + Ki) mod 256 .....(4)
In this case uses 256 as modulus value.

2.3 Cipher Block Chaining Mode

Cipher Block Chaining (CBC) is one of the operating modes commonly used in modern cryptographic algorithms. This operating mode is very superior in randomization binary of data that is loaded in blocks. The cipher block chaining operation mode will perform encryption and decryption process that interdependent between the binary blocks of the original binary data. In this case, the previous binary-block binary will be feedbacked in the process of encryption or decryption of the current block, so the block cipher is generated entirely depends on all blocks biner of plaintext[5][9]. Scheme of encryption and decryption process based on cipher block chaining mode are presented in figure 2 below.

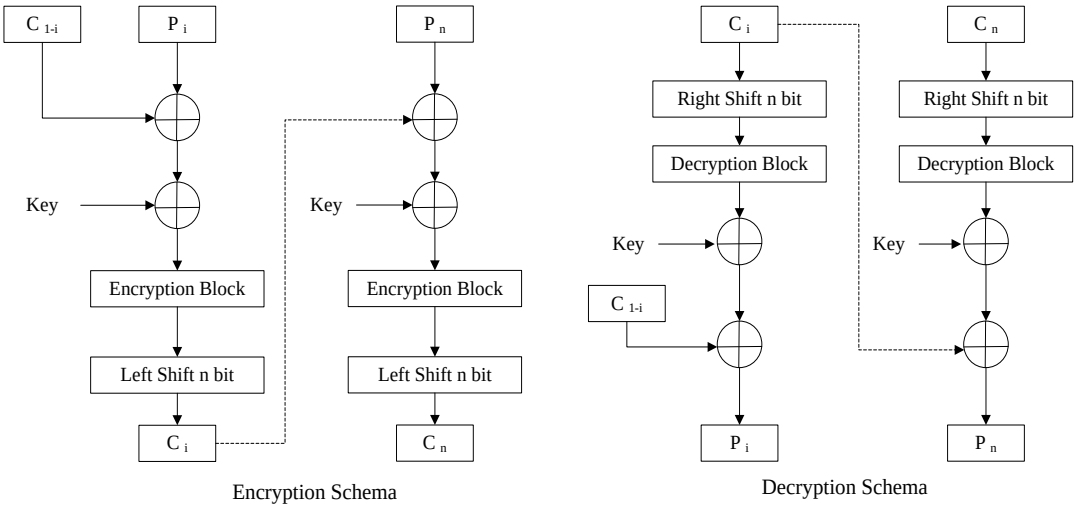

Figure 2. Encryption and Decryption Scheme Based on Cipher Block Chaining
Source : T. Zebua, 2015[5]

ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 26-31

Based on the above scheme, it is known that block of plaintext binary and initial cipher (C1-i) block will be processed with XOR. Variable of C1-i in CBC is often called C0 or initial vector (IV) or initial cipher. Initial cipher and the number of bits is determined by the user as an initialization vector. The number of C0 bits and keys must be same as the length of a plain bit block or cipher. The number of shift bits can be determined by the user included the position of shifted (left to right or right to left), number of bits that shifted as default in CBC is 1 bit.

Displacement of bit in decryption process is reversed position of encryption and the number of bits is same[10]. Based on this description, it can be formulated that:

Encryption Formulation : Ci = Shift 1 bit to left ((Pi ⊕ Ci) ⊕ Key) .....(5)

Decryption Formulation : Pi = (Shift 1 bit to Right(Ci) ⊕ Key) ⊕ Ci) .....(6)

3 RESULT AND DISCUSSION

Results of the implementation triple transposition vegenere cipher algorithm that combination with the cipher block chaining mode to secure text data are presented in the figure 3 bellow.

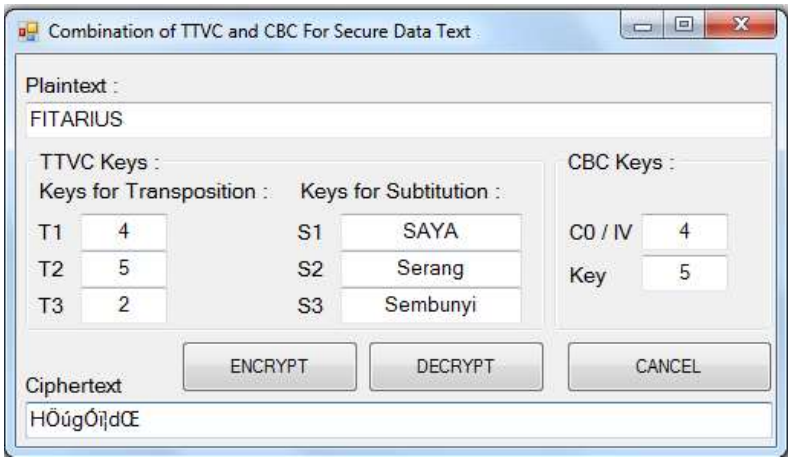

Figure 3. Result of Implementation Combination TTVC algorithm and CBC Operation Mode

Combination process of Triple Transposition Vegenere Cipher (TTVC) and Cipher Block Chaining (CBC) mode for secure the text in this study begins by encrypt the text data based on the triple transposition vegenere cipher algorithm, then binary of cipher that resulted will be randomized based on the cipher block chaining mode. The encryption process can be presented in the diagram below.

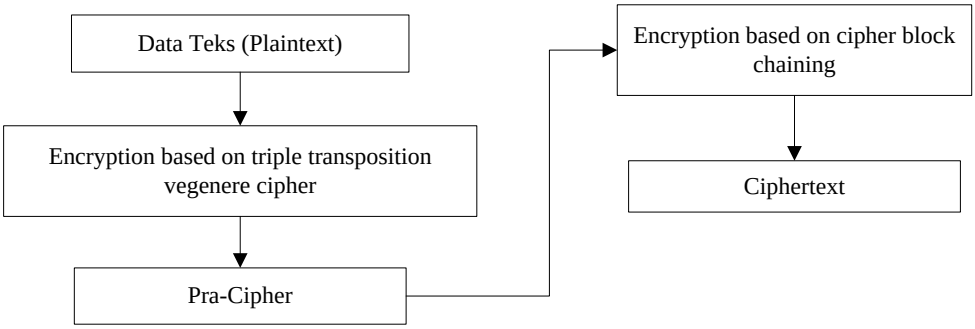

Figure 4. Ecryption Process Scheme Base on Combination of TTVC Algorithm and CBC Mode

Decryption process of ciphertext to be plaintext begins with the decryption process of ciphertext based on the cipher block chaining, then the plaintext obtained from the cipher block chaining decryption process will be decrypted again based on the triple transposition vegenere cipher process. Decryption process diagram is shown in figure 5.

ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 26-31

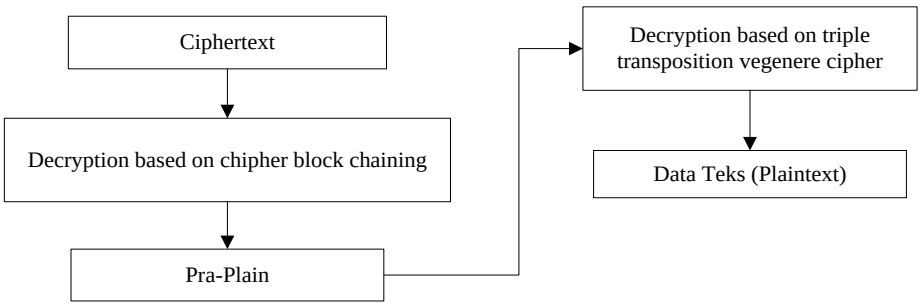

Figure 5. Decryption Process Sheme Based on TTVC Algorithm and CBC Mode

Text that used as samples in this research is FITARIUS, the key used in the encryption and decryption process based on the triple transposition vegenere cipher algorithm is:
The key for columnar transposition is T1 = 4, T2 = 5, T3 = 2 and keys for vegenere cipher is S1 = SAYA, S2 = Serang, S3 = Sembunyi

Based on figure 4 above, the encryption process begins based on the triple transposition vegenere cipher algorithm, then the pre-cipher obtained is scrambled again based cipher block chaining mode.

1. Encryption process based on triple transposition vegenere cipher (equation 1)
   a. First Transposition
      Value of key for each transposition (T1, T2, T3) is used as the number of transposition table columns that are formed.

F	I	T	A
R	I	U	S

      Cipher retrieval starts in each column, so the first transposition (T1) cipher is generated FRIITUAS.

   b. First Subtitution
      Cipher of first transposition (T1) will be substituted based on the vegenere cipher algorithm and the key used is the S1 key (follow equation 1), so that the S1 cipher is generated ™“¢ Š§– Š”
      Cipher S1 will use as plaintext on second transposition process

   c. Second Transposition

™	“	¢	Š	§
–	Š	”	X	X

      Character of X in the 5th and 6th columns in the last row are additional characters to fill in the blank fields. The second transposition cipher is ™-"š¢"ŠX§X. Cipher T2 is used as plaintext on the second substitution process.

   d. Second Subtitution
      Second subtituion using key S2 and cipher T2 is used as plaintext in this process (follow equation 1). Cipher S2 is ìûûûÝ½¹ and this cipher is used as plaintext in third transposition process.

   e. Third Transposition

Ì	Û
□	Û
□	Û
Ý	½
□	¹

      Cipher T3 is ì□□Ý□ûûû½¹ and is used as plain for third substitution process.

   f. Third Subtitution
      Cipher T3 will be substituted based on vegenere cipher algorithm with S3 key (follow equation 1), so the cipher (cipher of S3) generated is **?j}?Žitd□-** This cipher is the final result of encryption process based on triple transposition vegenere cipher. Biners of this cipher will be random based cipher block chaining mode.

ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 26-31

2. Encryption process based on cipher block chaining (follow equation 5)
   The number of group bits is 40 bits and C0 / IV = STMIK, Key = HUMEN, Shift 1 bit from left to right.
   The cipher generated based triple transposition vegenere cipher encryption process is **?j}?Žitd-**
   Biners of this cipher characters is :
   0011111101101010011111010011111110001110011010010111010001100100000100000000011110
   Separate these bits into two groups with the number of bits each group is 40 bits and begin from left to right

   P1 = 0011111101101010011111010011111110001110
   P2 = 0111010010111010001100100000100000000011110

   Encrypt P1, P2 for resulted C1, C2 based on equation 5, then resulted:
   C1 = 0100100011010110111110100110011100010110
   C2 = 1101001111101111101001100110010010001100
   Combine bits of C1 and C2, then split into 8 bits each group and then convert to be a characters:
   0100100011010110111110100110011100010110110100111110111110100110011001000100011100
   So, the cipher of text that resulted is **HÖúgÓï¦dŒ**

3. Decryption Process
   Decryption process begins based on the cipher block chaining decryption (use equation 6). The plaintext obtained from this decryption process will be used as a cipher in the decryption process based on the triple transposition vegenere cipher (see figure 5 above).
   a. Decryption process based on cipher block chaining mode
      Value of C0, keys and the shift value used in the decryption process are the same as the values used in the encryption process. It's just that the bit position shifted in the decryption process is the bit in the right position (because bit displacement position on encryption process is from left to right), the number of shifts is the same. The initial stage is to convert the ciphertext into binary, then group the binary according to the number of bits agreed upon in the encryption process. Follow the equation 6 to do the decryption process. Plaintext that resulted will be converted to characters and resulted characters **?j}?Žitd-** (this is the result of encryption process based on triple transposition vegenere cipher).
   b. Decryption process based on triple vegenere cipher
      Ciphertext that used in the decryption process based on the triple transposition vegenere cipher is the plaintext that is generated from the decryption process of cipher block chaining. The decryption process is carried out based on equation 2. Value of key that used is the same value as the encryption key value. Based on equation 2, plaintext is resulted is same as before, that is **FITARIUS**.

4 CONCLUSION

The results of analysis of the previous chapters, it can be concluded, where the conclusions are likely to be useful for the readers. Thus, the writing of this article can be more useful. The conclusions are as follows:

1. Combination of triple transposition vegenere cipher algorithm with cipher block chaining mode, able to increase randomness to encoded text of data, so as to be able to hide the patterns and original meaning of data text.
2. Randomizing binary-binary of confidential data based on cipher block chaining mode able to realize confusion and diffusion for the attackers to know the original meaning of data.
3. The combination of triple transposition vegenere cipher with cipher block chaining mode is very well if developed and used to improve the optimization of classic cryptographic algorithms.

REFERENCES

[1] E. Setyaningsih, "Penyandian Citra Menggunakan Metode Playfair Cipher," *J. Teknol.*, vol. 2, no. 2, pp. 213–219, 2009.
[2] N. Widyastuti, "Pengembangan Metode Beaufort Cipher Menggunakan Pembangkit Kunci Chaos," *J. Teknol.*, vol. 7, no. 1, pp. 73–82, 2014.
[3] W. Stallings, *Cryptography and Network Security*, V. New York: Prentice Hall, 2011.
[4] M. E Saleh, A. A. Aly, and F. A. Omara, "Data Security Using Cryptography and Steganography Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 6, pp. 390–397, 2016.
[5] T. Zebua, "Pengamanan Data Teks Dengan Kombinasi Cipher Block Chaining dan LSB-1," in *Seminar Nasional Inovasi dan*

ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 26-31

Teknologi (SNITI), 2015, pp. 85–89.
[6] A. Latif, "Implementasi Kriptografi Menggunakan Metode Advance Encryption Standard (AES) untuk Pengamanan Data Teks," *J. Ilm. Mustek Anim Ha*, vol. 4, no. 2, pp. 163–172, 2015.
[7] A. A. Lubis, N. P. Wong, I. Arfiandi, V. I. Damanik, and A. Maulana, "Steganografi pada Citra dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher," *JSM Mikro Ski.*, vol. 16, no. 2, pp. 125–134, 2015.
[8] M. Linda Caroline, "Metode Enkripsi Baru : Triple Transposition Vigènere Cipher," Bandung, 2011.
[9] D. Rosmala and R. Aprian, "Implementasi Mode Operasi Cipher Block Chaining (CBC)," *J. Inform.*, vol. 3, no. 2, pp. 55–66, 2012.
[10] E. Setyaningsih, *Kriptografi & Implementasinya Menggunakan Matlab*. Yogyakarta: Andi, 2015.