ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 22-25 (2017)

www.astesj.com

2nd International Conference of Computer, Environment, Social Science, Health Science, Agriculture & Technology (ICEST) 2017 5-7 May 2017, Medan, Indonesia

ASTESJ

ISSN: 2415-6698

Combination of Caesar Cipher Modification with Transposition Cipher

Fahrul Ikhsan Lubis*[1], Hasanal Fachri Satia Simbolon[1], Toras Pangidoan Batubara[1], Rahmat Widia Sembiring[2]

[1]*Magister Informatics, Universitas Sumatera Utara, Medan, 20155, Indonesia*

[2]*Department of Informatic, Politeknik Negeri Medan, 20155, Indonesia*

Email: fahrulikhsan30@gmail.com, hasanal.fachri12@gmail.com, toraspangidoanbatubara@gmail.com, rahmatws@yahoo.com

ARTICLE INFO

Article history:
Received: 17 March, 2017
Accepted: 20 April, 2017
Online: 13 June, 2017

Keywords:
Modification
Caesar Cipher
Transposition Cipher

ABSTRACT

The caesar cipher modification will be combine with the transposition cipher, it would be three times encryption on this experiment that is caesar modification at first then the generated ciphertext will be encrypted with transposition, and last, the result from transposition will be encrypted again with the second caesar modification, similarly at the decryption but the process is reversed. In the modification of caesar cipher, what would be done is the shift of letters are not based on the alphabet but based on ASCII table, plaintext will get the addition of characters before encryption and then the new plaintext with the addition of characters will be divided into two, they are plaintext to be encrypted and plaintext are left constantly (no encryption), The third modification is the key that is used dynamically follows the ASCII plaintext value.

1. Introduction

Cryptography is one way to conceal a message so that it is not easy to read or understood by people who are no right to access it. Cryptographic algorithm is divided into two that is classic and modern cryptographic algorithm. Classical cryptographic algorithm is an algorithm that used in antiquity that generally this algorithm only uses substitution and permutation method. Along with the development of algorithm technology it is considered less secure so then the new algorithms were created, then the modern cryptographic algorithm was born that use various method and in the process it used binary, hexadecimal, etc.

Classical cryptographic algorithm is starting to be abandoned by some people because it is considered less secure or considered it has expired, therefore it is possible to make modifications to the one of the classical cryptographic algorithm that is caesar cipher and combine it to another classical algorithm that is transposition cipher, so the results of ciphertext will be more complex and difficult to solve.

Modifications of caesar cipher have been done by other research, manipulating ciphertext by making readable ciphertext, so cryptanalis or unauthorized parties will not be suspicious if the message they are reading is a ciphertext [1]. In another research, caesar cipher was manipulated by changing the order of plaintext characters then performed substitution according to the key [2].

The modification of Caesar cipher will be executed by shifting the character based on ASCII table, plaintext will get the addition of characters before encryption and then the new plaintext with the addition of characters will be divided into two, plaintext that will be in encryption and plaintext which is left fixed (without encryption), and the last modification is to use a dynamic key following the value of plaintext ASCII.

2. Materials and Methods

In secure communication field, there are many studies which involves cryptography. Cryptography would be a well-known method for secure communication from the present of intruder. It is the algorithm method in which security goals are preferred. There are the processes to transcribe information into different form so that only authorized parties can access it. [3]

A cryptographic algorithm would be quite efficient when there is a guarantee for the data security. However, time of execution is more important, since it does not have to spend a lot of time to execute. [4]

There are two techniques of encryption: Substitution Technique and Transposition Technique. In substitution

*Corresponding Author: Fahrul Ikhsan Lubis, Magister Informatics, Universitas Sumatera Utara, Medan, 20155, Indonesia | Email: fahrulikhsan30@gmail.com

technique, the letters of plaintext are replaced by other letters or any number or by symbols. Example Caesarcipher, hill cipher, monoalphabetic cipher etc. In transposition technique, some sort of permutation is performed on plaintext. Example: rail fence method, columnar method etc[5].

Cryptography is divided into two types, Symmetric key and Asymmetric key cryptography. In Symmetric key cryptography a single key is shared between sender and receiver. The sender uses the shared key and encryption algorithm to encrypt the message. The receiver uses the shared key and decryption algorithm to decrypt the message.

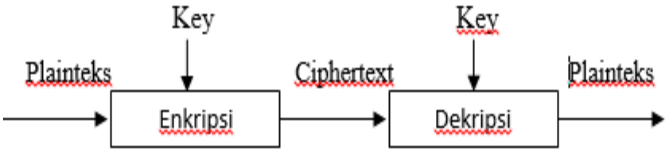

Figure 1. The encryption and decryption process of symmetric keys

In Asymmetric key cryptography each user is assigned a pairof keys, a public key and a private key. The public key isannounced to all members while the private key is kept secretby the user. The sender uses the public key which was announced by the receiver to encrypt the message. Thereceiver uses his own private key to decrypt the message[6].

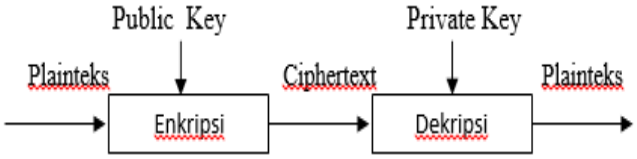

Figure 2. The encryption and decryption process of asymmetric keys.

2.1. Caesar Cipher

At the encryption of caesar cipher, each letter in the plaintext replaced with another letter with a fixed position apart by a numerical value, it is used as a secret key. [3]

Caesar cipher would be the simplest method of encryption because it is very easy to calculate but rarely used because of lack of robustness. The novelty of the introduced encryption technique is Simple in implementation but difficult in intercepting. And with caesar cipher data transmission can be successfully delivered using LASER. [7]

In cryptography, Caesar cipher is one of the simplest and most famous encryption techniques. The password includes a substitution password in which each letter in the plaintext is replaced by another letter that has a certain position difference in the alphabet. For example, if using shear 3, B will be E, U becomes X, and K becomes N so the plaintext of "buku" will become "EXNX" in encoded text. Caesar's name was taken from Julius Caesar a Roman general, consul, and dictator who used this password to communicate with his commander.

The encoding process (encryption) can mathematically use modulus operation by converting the letters into numbers, A = 0, B = 1, ..., Z = 25. The password (En) of "letter" x with shear n is mathematically written with:

$$E_n(x) = (x + n) \bmod 26$$

While in the process of solving the code (decryption), the decryption (Dn) is:

$$D_n(x) = (x - n) \bmod 26 \quad [8]$$

Caesar Cipher can be combined with the vigenere cipher [9]. But, it would be possible to combined Caesar cipher with transposition cipher for secure encryption. Because the combination of this two techniques provides more secure and strong cipher. The final cipher text is so strong that is very difficult to solve. The transposition method only change position of characters and substitution method only replaces the letter with any other letter. The above described method provides much more secure cipher with combination of both the transposition and substitution method. [10]

2.2. Transposition Cipher

Ciphertext is obtained by changing the position of the letters inside the plaintext. In other words, this algorithm transfers the sequence of letters in plaintext. Another name for this method is the permutation, because transpose each character in the text is the same as permutating the characters [11].

Examples of transposition cipher are as follows:

Plaintext: "ABCDEFGHI"

A	B	C
D	E	F
G	H	I

The result of transposition cipher is: ADGBEHCFI

Transposition is often combined with other techniques. With the power of computers, substitution and transposition encryption can be easily performed. The combination of these two classic techniques provides a more secure and strong cipher. The key is like a password for cipher text which is so strong that no one can break it. Transposition method only provides the rearrangement of characters of the plaintext. The attacker may attack on the cipher text to known plaintext. Above described method contain transposition as well as substitution method which makes secure and strong ciphertext. [12]

3. Results and Discussions

Encryption and decryption process through 3 processes. In the encryption process, the plaintext will be encrypted twice with the modified caesar cipher and once with the transposition cipher algorithm. Modifying the caesar cipher algorithm which the caesar not only uses the alphabet letters but also uses the characters in the ASCII table (32-126 characters), Key is used dynamically because the key is one of the ASCII value of one plaintext character. So, different plaintext, different key. Mathematically the process of encryption and decryption are as follows:

$$Ex = ((A-32)+K) \bmod 127)$$

$$Dx = ((A-32)-K) \bmod 127$$

3.1. Description

A=ASCII character inthe plaintext K= Key(one of the ASCII characters from plaintext mod 32).

The last modification is by adding certain words to the plaintext, in the encryption process the system will add a certain word on the back of the plaintext then plaintext divided into 2 parts: the unencrypted part, and the encrypted part. Conversely in the process of decryption, system will automatically delete the additional words so plaintext will be back to normal. The process of encryption and decryption is as follows:

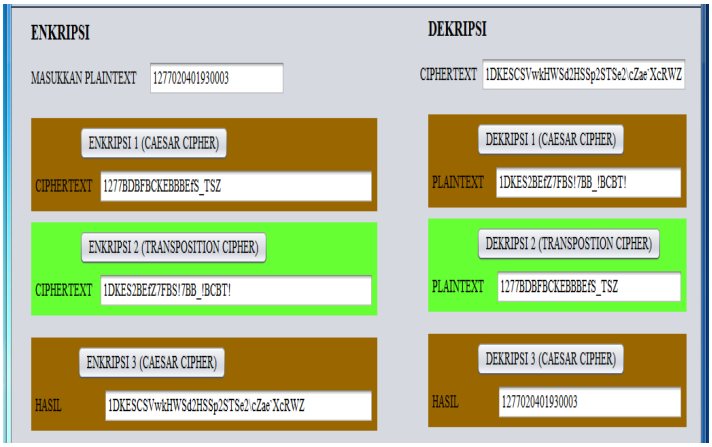

Figure 3. The process of encryption and decryption system

The explanation of the first caesar modification is as follows: The plaintext used is the NIK Number of KTP (identity Card) consisting of 16 characters, So the plaintext is 1277020401930003, then added with the word 'TAMBAH', so the plaintext on the system become 22 characters, they are 1277020401930TAMBAH. Furthermore, the plaintext is divided into two, they are the unencrypted characters and the character that will be encrypted. The unencrypted charactersare the the four characters at the beginning of the plaintext, they are '1277'and the character that will be encrypted is '02040193TAMBAH'. The key in this encryption is the ASCII value of the second character ('2') which is 50. Then put into the formula where the conversion is executedat every character on the plaintext that will be encrypted.

$$Ex = ((A-32)+K) \bmod 127)$$

The ASCII Value of character '0', which is 48.

$$Ex = ((48-32)+50) \bmod 127)$$

$$= ((16+50) \bmod 127)$$

$$= 66 \bmod 127$$

$$= 66$$

The ASCII value of 66 is character 'B'. And so on until the last character. So from the above data '1277020401930TAMBAH' become '1277BDBFBCKEBBBEfS_TSZ'

Since the encryption/decryption key depend on the ASCII value of the message so if the key character changed then all of ciphertext will be changed. As in the picture below:

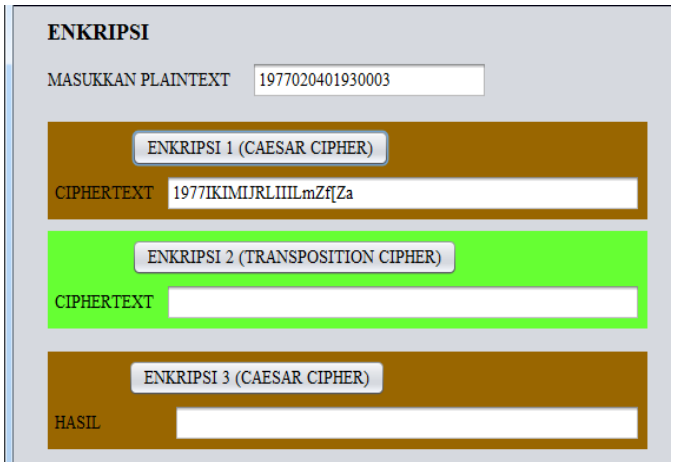

Figure 4. The process of encryption system

Then, the result of the first Caesar modification is encrypted with columnar transposition with 5 as key, since the result of the first encryption just 22 characters then the plaintext will be added 3 characters of '!'. There is not any modification at this encryption step, so it will execute as usual.

Plaintext is '1277BDBFBCKEBBBEfS_TSZ'

1	2	7	7	B
D	B	F	B	C
K	E	B	B	B
E	F	S	_	T
S	Z	X	X	X

So, the ciphertext is :

"1DKES2BEfZ7FBS!7BB_!BCBT!"

Furthermore, the result of columner transposition will be encrypted again with the second Caesar modification. The second modification is similar to the first modification. The difference is the number of unencrypted characters is 5. The word added into this step is "KRIPTOGRAFI" and the key used is the first ASCII value.

The plaintext for the second Caesar modification is '1DKES2BEfZ7FBS!7BB_!BCBT!KRIPTOGRAFI". The unencrypted characters is '1DKES'. And the character that will be encrypted is '2BEfZ7FBS!7BB_!BCBT!KRIPTOGRAFI' with The key in from the ASCII value of the first character ('1') which is 49. After all of the part has been known, then put it into the formula.

$$Ex = ((A-32)+K) \bmod 127)$$

The ASCII Value of character '2', which is 50

$$Ex = ((50-32)+49) \bmod 127) = ((18+49) \bmod 127)$$

$$= 67 \bmod 127$$

$$= 67$$

The ASCII value of 67 is character 'C'. And so on until the last character. So from the above data '1DKES2BEfZ7FBS!7BB_!BCBT!KRIPTOGRAFI' become '1DKESCSVwkHWSd2HSSp2STSe2\cZae`XcRWZ'.

Decryption is the inversion of the encryption process, if there is character addition at the encryption process then there is character reduction at the decryption process. The decryption process is refer to the following Figure 5:

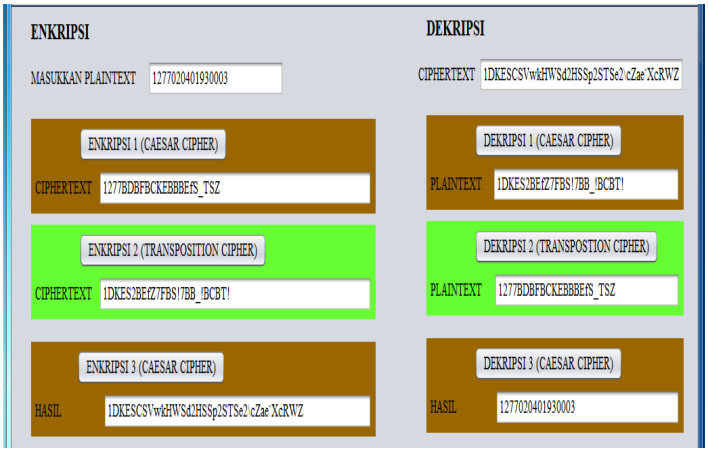

Figure 5. The process of encryption and decryption system

4. Conclusions

From the above explanation, it is known that the original plaintext and final ciphertext have different number of characters and in the process occurs 3 times encryption where each process occurs characters addition. So, the result of ciphertext is very complex and to solve it there are so many possibilities that should be tried cryptanalis such as: must find the sequence of algorithms used, determine the added character part, determine the unencrypted character part and search for the key used, this is not simple, because different plaintext, different keys will be used.

References

[1] Purnama, B. and Rohayati, H, A New Modified Caesar Chiper Cryptography Method With Legible Ciphertext From A Message To Be Encrypted, Procedia Computer Science 59: 195 – 204, 2015.
[2] Abraham, O. and Shefiu, G.,O, An Improved Caesar Cipher (Icc) Algorithm, [IJESAT], International Journal of Engineering Science & Advanced Technology 2(5):1198-1202, 2012.
[3] Han, L. C. and Mahyuddin, N. M, An Implementation of Caesar Cipher and XOR Encryption Technique in a Secure Wireless Communication, International Conference on Electronic Design (ICED):111 –116, 2014.
[4] Gowda, S, N, Innovative Enhancement Of The Caesar Cipher Algorithm For Cryptography, IEEE, 2016.
[5] Mishra, A, Enhancing Security Of Caesar Cipher Using Different, IJRET, International Journal of Research in Engineering and Technology 2(9): 327-332, 2013
[6] Jain, A., Dedhia, R., & Patil, A, Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for More Secure Communication. International Journal of Aplications 129(13): 6-11, 2015.
[7] Abedin, S., Tasbin, T. and Hira, A. Optical Wireless Data Transmission with Enhanced Substitution Caesar Cipher Wheel Encryption, International Conference on Electrical, Computer and Communication Engineering (ECCE): 552-556, 2017.
[8] Pradipta, A, Implementation Caesar Chiper Alphabet Plural Method in Criptografi for Information Security. Indonesian Journal on Networking and Security 5(3):16-19, 2016.
[9] Senthil, K., Prasanthi, K, and Rajaram, R. IEEE, 2013.
[10] Shrivastava, G., Sharma, R, and Chouhan, M, International Journal of Engineering Sciences & Research Technology 2(6): 1475-1478, 2013.
[11] Sasongko, J, Protction of Information Data Using Clasic Criptografi, Jurnal Teknologi Informasi DINAMIK 10(3):160-167, 2005.
[12] Padiya, S, D, and Dakhane, D, N, Plaintext Based Transposition Method, International Journal of Advance Research in Computer Science and Software Engineering. 2(7): 234-236, 2012.