Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 439-443 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Message Encryption Using Spinning Caesar XOR Binary Cryptography Algorithm (SPICA-XB)

Akrilvalerat Deainert Wierfi[1], Agung Jasuma[2], Dony Ariyus[3]

[123] Program Pascasarjana,
[123]Magister Teknik Informatika, Universitas Amikom Yogyakarta
Ngringin, Condongcatur, Depok Sub-District, Sleman Regency, Special Region of Yogyakarta 55281

E-mail: akrilvha8@gmail.com[1], agung.jasuma@students.amikom.ac.id[2], dony.a@amikom.ac.id[3]

ARTICLEINFO

Article history:
Received: 25/01/2020
Revised: 30 / 01/2020
Accepted: 01/02/2020

Keywords:
Data Security, spinning Caesar, XOR, LSB, Cryptography, Stegaografi.

ABSTRACT

Data security is a mechanism to protecting data and any attempt to impose limits on a system for access that does not have an authority (unauthorized person) causes poses a risk to valuable fan-sensitive information. To improve security in the text, images, video, and audio can be done by using two data security techniques such as cryptography and steganography. Cryptography is the process of plaintext to ciphertext randomizing using certain patterns. The secret message steganography focuses on inserting data or secret messages into other data such as text, images, video or audio. To increasing the security of data hiding, a combination of the two techniques is used wherein the initial data or message will be encrypted using the SPICA-XB algorithm which is a combination of two cryptographic algorithms namely spinning caesar and binary XOR.

1. Introduction

Data security is a mechanism to protect data as well as efforts in a system to limit unauthorized access / not allowed. When sensitive information is valuable and accessible to people who are not eligible (unauthorized person) it will lead to a lot of risk that will happen [1] [2]. One traffic exchange information over the Internet is to use e-mail. In the process of data transmission, there are some things that need to be addressed: confidentiality, data integrity, authentication and non-repudiation [3] [4] [5]. The exchange of information, especially data transmission without any security to the message or information sent to give a high enough risk. This facilitates attacks such as spoofing, hacking and eavesdropping message [6]. Of course, the email security needs to be planned and coordinated in order to protect resources (resources) and investment in it. To increase the security of communications and data can be done by encrypting the description of the message that will be sent, add a digital signature (digital signature), watermarking and authentication data.

Cryptography is a technique that is done to conceal or hide a message in the form of plain text into encrypted form. Cryptography is used to protect data from threats to information by making changes to the information so that it becomes a password that will only be understood by the sender and receiver of the message [7]. One algorithm that can be used to encrypt and decrypt messages in the email is Caesar cipher algorithm which encrypts the message carried by replacing each character alphabetic or other characters. [8] The downside of this method is to be solved by using the brute force method. Brute force is done by trying every possible key [9] as well as by matching the frequency distribution of each of the letters shown. Distribution of the letter in English to be very easy to distinguish and predict when using Caesar Cipher [10]. Therefore, in this study a modification to the algorithm Caesar Cipher so be SPICA-XB (Spinning Caesar Cipher Binary XOR). The algorithm itself is Caesar performed by spinning on its advance.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 439-443 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

SPICA-XB is a modification of the cryptographic algorithm is a classic combined with modern cryptographic algorithms. The algorithm is assumed that an algorithm like a caesar spinning wheel (spinning). SPICA-XB algorithm to process substitute key has been done turnaround. Turnover is dependent on the key policies that have been determined by the manufacturer of pre-conditions and deal with the same key. The algorithm Caesar cipher, substitution process is done by shifting the corresponding letter keys agreed while the algorithm SPICA-XB, the encryption process will be done by changing the letters that are in the form of binary ASCII 8 bits then do the summation with operassi XOR between the plain text with the key.

2. Methodology

The method used in this study using a cryptographic SPICA-XB (Spinning Caesar with XOR Binary) to encrypt a message that will be sent to your email. Messages that have been made encryption will be inserted into the image file by using the least significant bit (LSB). Rules on Spica-XB algorithm is as follows:

a. Determining the content of the plaintext and the key word and the key. The key value is the same as the keyword. When the number of characters in plaintext more of the keywords and key values, then the key will be repeated the number of characters in plaintext.
b. Pairing every character in the plaintext with the key to perform a shift in the value of each key.
c. Each letter in the plaintext will be transformed into a binary form in accordance with the 8-bit ASCII.
d. Turnover wheels start out by providing the index in alphabetical order. For example, the A index is 0, then the wheels are beginning a fixed position in the index-0 (A = A).
e. Then the encryption process will be carried out character by character with the previously performed rotation of the wheel with the key in the amount. Turnover wheel made anti clockwise. For example, if the key when it is active the letter C, the wheel will be rotated as far as the three characters in the opposite direction clockwise. After making the rotation, plain text letters will have a new key pair (middle key). Character plaintext will be encrypted when it will be done with the addition operation in the middle of key binary ASCII 8 bits. The process will be repeated until all of the characters in plaintext completed in encryption.
f. After the initial stage of the encryption is done, then the encryption process both, the XOR operation between the first encryption of the binary ASCII key beginning.

3. Analysis Methods

SPICA-XB algorithm is a modification of the algorithm Caesar Cipher. The process of encryption algorithms SPICA-XB is as follows:

a. Determine the plaintext and key
   Known plaintext encryption to be performed is "IMMEDIATE GRADUATION" with the key word is cryptography. Plaintext modification will be done by modifying the reverse and remove the space so that the plaintext is a "ADUSIWAREGES".
b. Pairing the plaintext with the key
   In this process, each letter in the plaintext will be paired with a keyword. A will be paired with K, D paired with R and so on.
c. Keywords and key value converted to binary numbers corresponding ASCII code 8 bi
d. Determine Key Values
   The key can be determined by mutual agreement of the message sender and recipient of the message is encrypted. In this study determined the key in Table 1 below:

TABLE 1
DETERMINING THE KEY

lock	K	R	I	P	T	O	G	R	A	F	I
value	10	11	8	2	7	4	9	13	17	1	3

e. Encryption Process Stage 1
   The encryption process is done with phase 1 determines the initial wheel where A = A and so on. Position alphabet still without shifting position. In the encryption process the letter A in the word

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 439-443 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

ADUSIW, key pairs A letter is K. The key K is 10, so the wheel will rotate as far as 10 characters anticlockwise (shift to the left). As the wheels would be a temporary table 1 in table 2 below:

TABLE 2
TEMPORARY 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

According to Table 2 above, the encryption is K. A further change is the letter A and K in the form of binary ASCII so too gave the A = K = 01000001dan 01001011. The next step is adding a second binary number, so the result is: 10001100. This process will be repeated for all the symbols on the plaintext. The overall encryption displayed in table 3 below.

TABLE 3
THE SUM OF THE BINARY ENCRYPTION

Pi	Ci	Plain Decimal (PD)	Cipher Decimal (CID)	PD + Acid	Binary
A	K	65	75	140	10001100
D	O	68	79	147	10010011
U	C	85	67	152	10011000
S	U	83	85	168	10101000
I	P	73	80	153	10011001
W	A	87	65	152	10011000
A	J	65	74	139	10001011
R	E	82	69	151	10010111
E	V	69	86	155	10011011
G	H	71	72	143	10001111
E	H	69	72	141	10001101
S	C	83	67	150	10010110

f. Encryption Process Stage 2

The process of encryption level 2 is performed with the XOR operation on the sum of the binary plaintext and ciphertext in binary in the first phase of the binary conversion on keywords. In Table 6 above the sum of binary numbers between the letters A and K is the encryption that is 10001100. A letter on the key note paired with K K where the conversion into ASCII binary is 01001011. To produce an XOR operation as in Table 4 below.

TABLE 4
THE XOR BINARY

Pi	lock	Binary Pi (BPI)	Binary Key (BK)	XOR (BPI, BK)
A	K	10001100	01001011	11000111
D	R	10010011	01010010	11000001
U	I	10011000	01001001	11010001
S	P	10101000	01010000	11111000
I	T	10011001	01010100	11001101
W	O	10011000	01001111	11010111
A	G	10001011	01000111	11001100
R	R	10010111	01010010	11000101
E	A	10011011	01000001	11011010
G	F	10001111	01000110	11001001
E	I	10001101	01001001	11000100
S	K	10010110	01001011	11011101

4. Results and Discussion

Based on the above plan to make further use of java language to implement a combination of two methods that SPICA-XB for cryptography and LSB to steganografinya. As a result of the encoding and the program can be viewed as in Figure 1 and Figure 2 below.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 439-443 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

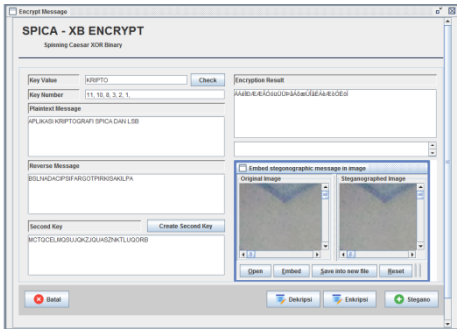

Fig 1. Interface Encryption

In Figure 1 is done by inserting the key, the key number and the message will be encrypted and pasted. The message is then reverse and matched with the number key to produce a second key, the second key after the new algorithm SPICA-XB can be used to generate a new message. New posts and lock both then combined and converted into binary form and then inserted into a picture.

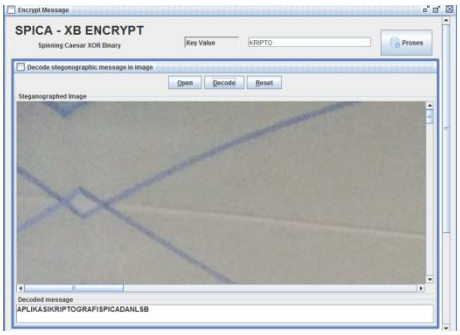

Fig 8. Interface Decryption

In figure 8 recipients will be asked to enter the key that has been agreed upon then upload images to extract secret messages, after pressing decode system will extract the message on the image, convert it into a form letter, separate secret message and the second key and then a new method SPICA-XB to solve the secret message and the last reverse the decryption to a secret message back to normal.
Tests conducted to examine whether the algorithm SPICA-XB and LSB can be combined as well as to find out the limitations and loopholes of the system. Tests carried out on 20 encryption and decryption with 4 different image detail while testing can be seen in Table 5 below.

TABLE 5
TESTING SYSTEMS

picture	lock	National character secret message	Image Size		Resolution Image (Pixel)		Decryption (Managed (B) / Fail (G))
			picture Cover	New Image	before	after	
Figure 1	crypto	<50	2.73	17.8	3120 x	3120 x	B
	crypto	> 50 <200	(MB)	(MB)	4160	4160	B
	crypto	> 200					B
	cRYPTOGRAPHY	> 200					B
	crypto	<50					B
Figure 2	beach	> 200	80.6 (KB)	1.53	1080 x	1080 x	B
	beach	> 200		(MB)	1080	1080	B
	mountain	<50					B
	beach	> 50 <200					B
	beach	<50					B
Figure 3	cRYPTOGRAPHY	> 200	40.5	643	720 X	720 X	B
	cRYPTOGRAPHY	> 200	(KB)	(KB)	1280	1280	B
	cRYPTOGRAPHY	<50					B
	cRYPTOGRAPHY	<50					B
	cRYPTOGRAPHY	<50					B

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 439-443 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

picture	lock	National character secret message	Image Size		Resolution Image (Pixel)		Decryption (Managed (B) / Fail (G))
			picture Cover	New Image	before	after	
Figure 4	rain	> 100	78	1.38 (MB)	720 X	720 X	B
	heat	> 100	(KB)		1280	1280	B
	rain	> 50 <200					B
	heat	> 50 <200					B
	rain	> 50 <200					B

5. Conclusion

Based on the results of the merger method SPICA-XB and LSB successful experiment where 20 of the secret messages embedded in the LSB algorithm successfully in the extraction and decryption methods SPICA-XB. The level of security of the algorithm increases because in order to solve the secret message that is inserted to go through several stages starting from extracting messages from the image, change the extraction results in the form of letters, separating a secret message with key 2 which is also inserted and the last step mereverse the decryption origin message back to normal.
Suggestions for further research are trying to incorporate cryptographic methods SPICA-XB with other methods of steganography to see if it can cover up weaknesses in the case if the image decryption process compresses such as delivery in Facebook, WhatsApp and Telegram.

6. References

[1] Firdaus, Alfikri Zakiy., 2011, Studi dan Analisis Dua Jenis Algoritma Block Cipher: DES dan RC5.
[2] Syafrizal, M., 2007, ISO 17799: Standar Sistem Mana-jemen Keamanan Informasi, Seminar Nasional Teknologi, ISSN: 1978-9777 Issue. 24.
[3] Dominic, Bucerzan., 2008, A Cryptographic Algorithm Based on a Pseudorandom Number Generator, 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing.
[4] O.P.Verma, et al., 2011, Peformance Analysis Of Data Encryption Algorithms, Electronics Computer Tech-nology (ICECT), 3rd International Conference. pp. 399-403.
[5] E. Surya and C. Diviya., 2012, A survey on Symmetric Key Encryption Algorithms, International Journal of Computer Science & Communication Networks, vol. 2. pp. 475-477.
[6] Munir, Rinaldi., 2006, Kriptografi, Bandung : In-formatika.
[7] Bender. 1996. Techniques For Data Hiding. IBM Sys-tems Journal.
[8] Setyaningsih, E., 2015, Kriptografi & Implementasinya Menggunakan Matlab.,Yogyakarta : Pen erbit Andi.
[9] Singh, A. Nandal., and A. & Malik, A. 2012. Imple-mentation of Caesar Cipher with Rail Fence for En-hancing Data Security. International Journal of Ad-vanced Research in Computer Science and Software Engineering (IJARCSSE). Vol 2, Issue 12.
[10] Jain, A., Dedhia., R. & Patil, A. 2015. Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communica-tion. International Journal of Computer Application. Vol 129, No. 13.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.