4th ICRIEMS Proceedings
Published by The Faculty Of Mathematics And Natural Sciences
Yogyakarta State University, ISBN 978-602-74529-2-3

Cryptography System for Information Security Using Chaos Arnold's Cat Map Function

Muhamad Wildan Habiby[1,a)] , Dwi Lestari[2,b)]

Department of Mathematics, Faculty of Mathematics and Natural Science, Yogyakarta State University
Jl Kolombo No 1, Karangmalang, Depok, Sleman, Yogyakarta, Indonesia

Corresponding author: Habi_by@yahoo.com[a)],
dwilestari.math@gmail.com[b)]

Abstract. This study aims to apply the Chaos Theory in cryptography. Chaos theory is a very complex, irregular and random behavior in a deterministic system. Chaos has a random nature, a slight change of course will generate different numbers, and it is useful in generating the key. Arnold's Cat Map Chaotic function is one of the functions in chaos theory that will be used to generate the keys. Stickel's key exchange protocol will be used to determine the key generator. Furthermore, a key generator will be processed by using the chaos function arnold's cat map and will obtain the key that will be used for encryption and decryption. In the process of encryption calculation by formula $C_i = (K_i + P_i) \bmod 94$, while the decryption process performed by the calculation formula $C_i = (K_i - P_i) \bmod 94$, with C_i is ciphertext, P_i is plaintext, and K_i is Key. The simulation results showed if there is a change in the initial value of chaotic function Arnold's Cat Map, and then obtained different plaintext.

INTRODUCTION

In the recent years, information security is very essential. A secret information must not be known to the public or a handful of people who do not have any authority in such information. If the information is leaked it will be damage to the transmitter or receiver of the information. Someone who is unauthorized in such information could easily know the content of the information. Transmitters must keep the message information that is not easily known by other people, information security can be done by encrypting messages into complex codes. Therefore, a study of information security is necessary. One of the studies of information systems security is called cryptography.

Cryptography is derived from two words: *cryptos* and *graphein*. *Cryptos* means secret, and *graphein* means writing. Therefore cryptology means secret writing. Meanwhile, according to the definition, cryptography is the science that studies the secret message encryption and decryption [1]. Encryption and decryption are the processes in cryptography. One of the cryptographic algorithms is symmetric cryptographic algorithm; this algorithm uses the same key in the encryption and decryption process. Therefore, the key has to be kept secret so that cryptanalist cannot know the content of the message and to generate the key, chaos theory will be used to generate the key.

Many research have discussed such as [2] and [3] about semigroup in public cryptography. In [4, 5, 6, 7] and [8] about chaotic maps in image encryption. George Makris,et.al [9] and Piyus [10] discussed about cryptography chaos. Meanwhile, in [11, 12, 13, 14] and [15] described about Arnold Cat Map for image encryption. The research discussed about stream cipher can be seen in [16]. In this research, we used Arnold's Cat Map to determine a key generator and then applied into cryptography. Besides, the Stickel's key exchange scheme is used to obtain the initial value for generating the key. [17]

Since Chaos function is very sensitive to the initial value, if there is a slight change will generate different numbers[18]. Hence, chaos function is suitable to be used in generating the key. Arnold's Cat Map (ACM) is one of the chaos functions. ACM has the advantage of speedy encrypting data. In determining the key generator, stickel key agreement protocol on non-commutative semigroups will be used. Simulation will be given with different key such that it can be seen the ciphertext is different.

RESULTS AND DISCUSSION

Generating The Key

The key is the parameter used to transform the message encrypting and decrypting process[19]. This study uses symmetric cryptographic algorithm, in which the key has to be kept secret in order to make the message stay safely secret from third people. Arnold cat map function will use the initial value (key generator) in forming the key. Stickel's key exchange protocol based on non-commutative groups will be used and it will be generalized to non-commutative semigroups[2,3].In this case, $M_n(Z)$ is defined. It is a set of matrices n x n with integer entries and $n \geq 2$. The set $M_n(Z)$ is written in Equation (1) as follows.

$$M_n(\mathrm{Z}) = \left\{ \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} \det \neq 0 \right\} \tag{1}$$

After agreeing the key generator, then the key formation will be generated using Arnold's cat map function using a key generator that has been agreed to. It will use a stickel key agreement protocol.

The transmitter and receiver will agree on a key generator using stickel key agreement protocol $K=K_1=K_2$. Matrix K will be converted to equation 2. Value of K is transformed to decimal form by adding up all of the entries of matrix K, if $K > 1$ then $K \times 10^{-1}$, this process is conducted repeatedly until satisfy $K \leq 1$. Equation 2 will be written as follows.

$$\begin{aligned} K &= |a_{11} \times 10^{-1}| + |a_{22} \times 10^{-3}| + \ldots + |a_{ij} \times 10^{-(2n(i-1))+(2j-1)}| \\ i &= 1,\ldots,n.,\ j = 1,\ldots,n. \end{aligned} \tag{2}$$

The conversion of K value is completed to make the key generator K can be processed using ACM as the key. Stickel's key agreement process is conducted using $M_n(Z)$.

TABLE 1 Stickel's key Exchange Scheme for first parameter

Transmitter and receiver published a $M_n(Z)$ dan $A,B \in M_n(Z)$

For example: $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ dan : $B = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

Transmitter		Receiver	
1)	Secretly choosing a natural number p and q. For example : p=2 and q=2	1)	Secretly choosing a natural number r and s. For example : r=2 and s=1
2)	Calculating $U = A^2B^2$ $U = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^2 \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}^2$ $= \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$ $= \begin{bmatrix} 17 & 11 \\ 3 & 2 \end{bmatrix}$	2)	Calculating $V = A^2B^1$ $V = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^2 \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}^1$ $= \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ $= \begin{bmatrix} 6 & 5 \\ 1 & 1 \end{bmatrix}$
3)	Sending U to receiver	3)	Sending V to transmitter
4)	Receiving V from receiver	4)	Receiving U from transmitter
5)	Calculating $F_1 = A^pVB^q$ $F_1 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^2 \begin{bmatrix} 6 & 5 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}^2$ $= \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 6 & 5 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$ $= \begin{bmatrix} 77 & 48 \\ 8 & 5 \end{bmatrix}$	5)	Calculating $F_2 = A^rUB^s$ $F_2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^2 \begin{bmatrix} 17 & 11 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}^1$ $= \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 17 & 11 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ $= \begin{bmatrix} 77 & 48 \\ 8 & 5 \end{bmatrix}$

Transmitter and receiver successfully agree on an identical key generator

$F = F_1 = F_2 = \begin{bmatrix} 77 & 48 \\ 8 & 5 \end{bmatrix}$ $F = \begin{bmatrix} 77 & 48 \\ 8 & 5 \end{bmatrix}$ converted to F = 0,77480805

TABLE 2. Stickel's key Exchange Scheme for second parameter

Transmitter and receiver published a $M_n(Z)$ dan $C,D \in M_n(Z)$

For example: $C = \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix}$ dan : $D = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}$

	Transmitter		Receiver
1)	Secretly choosing a natural number k and l. For example : k=1 and l=2	1)	Secretly choosing a natural number i and j. For example : i=1 and j=3
2)	Calculating $W = C^1D^2$ $W = \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix}^1 \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}^2$ $= \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 5 & 2 \\ 2 & 4 \end{bmatrix}$ $= \begin{bmatrix} 2 & 4 \\ 15 & 6 \end{bmatrix}$	2)	Calculating $Z = C^1D^3$ $Z = \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix}^1 \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}^3$ $= \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 9 & 10 \\ 10 & 4 \end{bmatrix}$ $= \begin{bmatrix} 10 & 4 \\ 27 & 30 \end{bmatrix}$
3)	Sending W to receiver	3)	Sending Z to transmitter
4)	Receiving Z from receiver	4)	Receiving W from transmitter
5)	Calculating $L_1 = C^kZD^l$ $L_1 = \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix}^1 \begin{bmatrix} 10 & 4 \\ 27 & 30 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}^2$ $= \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 10 & 4 \\ 27 & 30 \end{bmatrix} \begin{bmatrix} 5 & 2 \\ 2 & 4 \end{bmatrix}$ $= \begin{bmatrix} 195 & 174 \\ 174 & 108 \end{bmatrix}$	5)	Calculating $L_2 = C^iWD^j$ $L_2 = \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix}^1 \begin{bmatrix} 2 & 4 \\ 15 & 6 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}^3$ $= \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 15 & 6 \end{bmatrix} \begin{bmatrix} 9 & 10 \\ 10 & 4 \end{bmatrix}$ $= \begin{bmatrix} 195 & 174 \\ 174 & 108 \end{bmatrix}$

Transmitter and receiver successfully agree on an identical key generator

$$L = L_1 = L_2 = \begin{bmatrix} 95 & 174 \\ 174 & 108 \end{bmatrix}$$

$L = \begin{bmatrix} 95 & 174 \\ 174 & 108 \end{bmatrix}$ converted to L = 0,196757508

The key generator is obtained $x = F$ = 0,77480805 and y = L = 0,196757508. Key generator will be generated to be the keys using the ACM function. Equation (3) shows ACM function will be used iteratively to get the key [18]:

$$(x_{i+1}, y_{i+1}) = \begin{cases} \left(2x_i, \frac{y_i}{2}\right), 0 \le x \le 0.5, 0 \le y \le 1 \\ \left(2x_i - 1, \frac{y_i + 1}{2}\right), 0 \le x \le 0.5, 0 \le y \le 1 \end{cases} \quad (3)$$

The result obtained from the function iterations will be taken only the first 2 digits after the decimal point and rounded down to be used as the key. The resulting numbers of the key generation will be compiled and then used as a key for encryption. The forming of these numbers will be written sequentially and alternately between x and y, started from $K = x_1\ y_1\ x_2\ y_2 \ldots$ and so on. From the key generator x and y a key will be obtained to be used in encryption and decryption process K : 771954590979103939197909 58...

Encryption Process

A message security is done through an encryption process. Firstly the message is changed to the numeric form, after that the encryption process is done by adding key blocks K which contains 2-digit number to each character of the message as well as the calculation by modulo 94. The formula used in the encryption is

$$C_i = (K_i + P_i) \bmod 94 \quad (4)$$

with

C_i = Ciphertext
K_i = Key
P_i = Plaintext

i = 1,2,3,...,n.
n = The number of message characters

For example the plaintext is
"**Motor kamu sudah bapak kirimkan lewat KAI ke stasiun tugu, nomor pengiriman 13569A67CD99.**"

The ciphertext is
"**68__1{4DPD{2{Vr:9D*9E&}D&[5aTFkt@;|L?i[U(0ENAtXtBw2e15jF.Fnfm"%F,?O=-X/cG[*~ti_{n1%xm/xo**".

Here is given another example a plaintext in English Language as follow:

"I send the solution of final exam 2017"

Meanwhile, The ciphertext is

"2s)!w]sWKx{2)#BcHQ\sS@}9&=w IJuuaX.vS3".

Decryption Process

Receiver will change the ciphertext to plaintext or the process is called decryption in order to allow the reading of the message from transmitter. This process needs identical key with the encryption process which is *K*. Decryption process has formula:

$$P_i = (K_i - C_i) \bmod 94 \tag{5}$$

with

C_i = Ciphertext
K_i = Key
P_i = Plaintext
i = 1,2,3,...,n.
n = the number of message characters.
The message from the encryption process will be changed back to the original message from ciphertext yield:
"**68__1{4DPD{2{Vr:9D*9E&}D&[5aTFkt@;|L?i[U(0ENAtXtBw2e15jF.Fnfm"%F,?O=-X/cG[*~ti_{n1%xm/xo**".

After the decryption process, plaintext will be obtained as follows:
"**Motor kamu sudah bapak kirimkan lewat KAI ke stasiun tugu, nomor pengiriman 13569A67CD99.**".
Here is given another example the decryption from the ciphertext:
"2s)!w]sWKx{2)#BcHQ\sS@}9&=w IJuuaX.vS3".
Will obtain
"I send the solution of final exam 2017".

The Examples of Different Key Generator

For example a cryptanalist figured out the key generation but with different first digit, i.e. x = 0,77580805 and y = 0,196757508. The result of the decryption process from the ciphertext "**68__1{4DPD{2{Vr:9D*9E&}D&[5aTFkt@;|L?i[U(0ENAtXtBw2e15jF.Fnfm"%F,?O=-X/cG[*~ti_{n1%xm/xo**".
will be obtained:
Mosoq jaku,snd[h^bNX/0>w x\p$cBIW+pCfsrK|e?P!?Q\.K(}hfFH^lhr6ZN?!SJ-]G`zDR$_7^FPUK-B3.nYO" .
Here is another example from the ciphertext **"2s)!w]sWKx{2)#BcHQ\sS@}9&=w IJuuaX.vS3"**, obtained a different plaintext:
"I remd/tfe,shlht=o~Hm5>r t`oTgLJX&u_mP".
A *ciphertext* obtained by cryptanalist would be different from the original message sent by the transmitter.

CONCLUSION

To secure a secret message transmission, it can be converted into a message code that cannot be understood by criptanalist. This research used Arnold's Cat Map as one of a chaotic function in generating the key. Before the key generation process, a key generator agreement process would be conducted by using stickel's key exchange scheme. After the key generator is formed, then the keys for encryption and decryption process would be obtained by using Arnold's Cat Map. The simulation results showed if there is a change in the initial value of chaotic function Arnold's Cat Map, and then obtained different plaintext.

REFERENCES

1. Anton, Howard & Rorres,Chris. *Elementary Linear Algebra : Applications Version*. New Jersey:Wiley. (2014).
2. Gerard Maze, Chris Monico, and Joachim Rosenthal,. Public key Cryptography based on Semigroup Actions. *Journal Advances in Mathematic Communication.* (2007)
3. Glenn Merlet . Semigroup of matrices acting on the maxplus projective space. *Linier algebra and its applications.* Elsevier. (2009)
4. Mina Mishra and Vijay H Mankar. Chaotic Encryption Scheme Using 1-D Chaotic Map. *Int.J.Communication Network and System Sciences.* 4, pp.452-455. (2011)
5. L. Bao, Y. Zhou, P. Chen, and H. Liu,. A New Chaotic System for Image Encryption. *International Conference on System Science and Engineering*, 69 -73 , (2012).
6. A. Gaur, and M. Gupta,. Review: Image Encryption Using Chaos Based Algorithm. *International Journal of Engineering Research and Application*, **4** (3), 904 – 907, (2014).
7. Piyush Kumar Shukla, Ankur Khare, Murtaza Abbas Rizvi, Shalina Stalin, and Sanjay Kumar. Applied Cryptography Using Chaos Function for Fast Digital Logic-Based System in Ubiquitous Computing. *Entropy Journal* 17 pp:1387-1410. (2015).
8. Govind Chandra, Naveen Chandra, and Swati Verma. A review on Multiple Chaotic Maps for image Encryption with Cryptograpic technique. *International Journal of computer applications*.**121**(13).(2015).
9. George Makris and Ioannis Antoniou. Cryptography with Chaos. *Proceeding5th Chaotic Modelling and Simulation International Conference.*(2012)
10. Piyush Kumar Shukla, Ankur Khare, Murtaza Abbas Rizvi, Shalina Stalin, and Sanjay Kumar. *Applied* Cryptography Using Chaos Function for Fast Digital Logic-Based System in Ubiquitous Computing. *Entropy Journal* 17 pp:1387-1410. (2015).
11. S. Keshari, and S.G.Modani,. Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission. *International Journal of Computer Science and Technology*, **2** (1),132 -135 , (2011).
12. F. Svanstrom, . "Properties of a Generalized Arnold's Discrete Cat Map". *Master Thesis.* (2014).
13. A. Soleymani, M. J. Nordin, and E. Sundararajan,. A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map. *The Scientific World Journal*, (2014). (http://dx.doi.org/10.1155/2014/536930)
14. P. Dureja, and B. Kochhar,. Image Encryption Using Arnold's Cat Map and Logistic Map for Secure Transmission. *International Journal of Computer Science and Mobile Computing*,. **4** (6), 194 – 199, (2015).
15. E. Hariyanto, and R. Rahim,. Arnold's Cat Map Algorithm in Digital Image Encryption. *International Journal of Science and Research*, **5** (10), 1363 - 1365,(2016).
16. D. Lestari dan Zaki Riyanto.(2012). Suatu Algoritma Kriptografi Stream Cipher Berdasarkan Fungsi Chaos. *Prosiding*,. Yogyakarta : FMIPA UNY. (2012)
17. V. Shpilrain,. Cryptanalysis of Stickel's key exchange Scheme. *International Conference on Computer Science: theory and application*, 283 – 288, (2008).
18. Alvin Susanto.___. Penerapan Teori Chaos di Dalam Kriptografi. *Jurnal Teknik Informatika*.
19. Munir ,Rinaldi. *Kriptografi*.Bandung:Informatika Bandung. (2006)