Design and Implementation Randomized Cryptography Algorithm Detection Using Chaos Algorithm

[1)]Gede Arna Jude Saskara
School of Electrical Engineering and Informatics
Institut Teknologi Bandung, Jl. Ganesha 10
Bandung 40132, Indonesia
Email : jude_saskara@students.itb.ac.id

[2)]Budi Rahardjo
School of Electrical Engineering and Informatics
Institut Teknologi Bandung, Jl. Ganesha 10
Bandung 40132, Indonesia
Email : br@paume.itb.ac.id

***Abstract*— Cryptography is a science which is focused on art or technique related to a security of information. Every years many researchers developed cryptography algorithm, so a measuring tool to determine the quality of the algorithm is necessary. One aspect of measuring the quality of a cryptographic algorithm is based on its randomization. Measuring its randomization based on Chaos theory is implemented to measure stream cipher RC4 algorithm and it will use Vigenere Cipher algorithm as the comparison. Based on chaos algorithm, the entropy calculation shows that randomness of RC4 algorithm is better than Vigenere Cipher algorithm.**

Keywords—Cryptography; Chaos Theory; Random; Stream Cipher;

I. INTRODUCTION

Cryptography is a science which is focus on art or technique in relation with a security of information. Cryptography process can be divided into 2 categories: encryption and decryption process. Encryption process is used to randomize or data encode, so that the data cannot be read or understand by others. Input data for encryption process known as plain text and the output known as cipher text. A process for returning encoded message into its original form called description process. Based on its key, cryptography algorithm can be categorized into 2 categories: symmetrical key and asymmetrical key. Symmetrical key algorithm divided into 2 categories: stream cipher and cipher block.

Based on its key, there are so many kind of cryptography algorithm and to detect its quality is not easy. There are some factors that can influence cryptography algorithm, such as, diffusion, confusion, and feedback. So, a program to detect a quality of algorithm by using chaos theory is needed. An idea from chaos theory or random theory is there is a non-periodic orbit, that doesn't have persistent appearance or formulated.

For the first time, chaos system is used in cryptography algorithm to develop chiper [1]. Then, chaos system is used to build a random number that used in encription and decription process[2]. Another development from chaotic dynamic is to analyze a new methodology block chiper algorithm[3]. Using chaos theory, cryptography algorithm is measured based on its randomization. This research will use stream cipher RC4 algorithm and vigenere cipher and the quality of both cryptography algorithm will be detected by using chaos theory.

II. CHAOS THEORY

Chaos theory or random theory has thought since a long time ago. Chaos is a purely mathematical concept; it is an undeniable mathematical fact [4]. In recent years, obtained many meaningful results to chaos phenomenon's experiment, but more results come from to the nonlinear system mathematical model theoretical analysis and the computer simulation. There are some equations to describe these model: non-line iteration equation (group), non-line autonomous simultaneous differential equation and difference differential equation (group).

The nonlinear system has many kinds of forms from the non-chaotic state to the chaotic state evolutionary process. And most typical has three kinds: Time of cyclical furcation process, Intermittence the chaos process, and Half of periodic movement to chaos [5]. Chaos theory from many researchers has many principles.

Principles of Chaos:

- The Butterfly Effect, a more rigorous way to express this is by small changes in the initial conditions that lead to drastic changes in the results. Our lives are an ongoing demonstration of this principle[6].
- Unpredictability, because we can never know all the initial conditions of a complex system in sufficient detail, we cannot hope to predict the ultimate fate of a complex system [7].
- Dynamic system's order or the chaos degree [5].
- Mixing: Turbulence ensures that two adjacent points in a complex system will eventually end up in very different positions after some time has elapsed.
- Feedback: Systems often become chaotic when there is feedback present.
- Fractals: A fractal is a never-ending pattern. Fractals are infinitely complex patterns that are self-similar across

IEEE Catalog Number : CFP16B09-PRT, ISBN : 978-1-5090-1719-5

different scales. They are created by repeating a simple process over and over in an ongoing feedback loop.

III. DESIGN

In general, implementation system architecture of chaos theory to measure algorithm quality can be seen on the system architecture below :

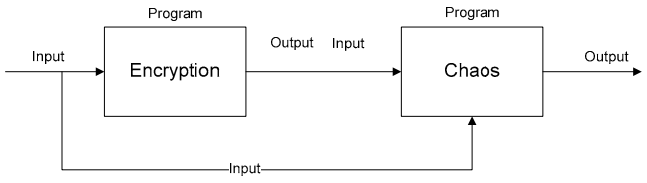

Fig. 1. General Overview System

From the general illustration above, there are two programs: a program for encryption and chaos program for measuring randomization from encryption algorithm. From Figure 1 above there is also input data on plain text message form to be processed by encryption program and serve as comparison on chaos program.

A. Encryption

Encryption program is a process from plaintext into cipher text. There are 2 types of algorithm which is used in encryption process: RC4, the most algorithm that used right now and vigenere cipher algorithm. The aim of using two algorithms is to compare which randomization is better from chaos process algorithm.

1. Vigenere Cipher [8]
   Vigenere cipher uses vigenere square to do an encryption. The left column from the square is a key alphabets and the row above is a plaintext alphabets. Mathematically, vigenere cipher encryption, for example a key with length series $k_1k_2\ldots k_m$, Plaintext is series of $p_1p_2..p_t$, and cipher text is a series $c_1c_2..c_t$, so encryption on vigenere cipher can be explained below:
   $c_i = (p_i + k_i) \bmod 26 \quad (1 \leq i \leq t)$ (1)
   and,
   $i = r \pmod m \quad (1 \leq r \leq t)$ (2)
   Example : T alphabets encrypt as S key
   $(T + S) \bmod 26 = (19 + 18) \bmod 26 = 11 = L$ (3)
   and so on.

2. RC4
   On RC4 algorithm there are two point process: initialization state and key regeneration and encryption process [9].

   (a) Initialization State
   State array initialization, there are 2 state-array that should be initialize, S and K. 256 byte S array is initialization with number from 0-255. 256 byte K array filled with 1-256 byte length continuously until all of K array is fully loaded. Then, key scheduling algorithm is done to regenerate permutation from S array based on available key.

   (b) Key Regeneration and Encryption process
   After having state array which has been randomized, we will initialization again i and j with 0. Then, do pseudo random generation algorithm or PGRA to regenerate encryption key which will be XORed with plaintext. To regenerate encryption key, PRGA increment i, adding S[i] value and S[j] exchange both value. And the key value that regenerate is S with the same number of index S[i] and S[j] modulated with 256.

B. Chaos

After encryption, data output in a cipher text form and data input on a plain text form will be processed with chaos algorithm for knowing randomization from RC4 and vigenere cipher algorithm. Based on the explanation above, there are chaos principles: butterfly effect, Unpredictability, Order, Feedback and Fractal. Encription result from encription program will be processed compatibly with the chaos principle. This research only use two of chaos principles: Unpredictability and Order.

Unpredictability and order system from the encription result can be known by mathematics process known as entropy [10][5]. To calculate Chaos and randomness, can use Shannon Entropy or Kolmogorov-Sinai Entropy because its value is almost close[11]. Entropy calculation is one of the Symbolic Dynamic calculation [12]. Symbolic dynamic is an analysis device which is commonly used[13].

Topological entropy was defined for general compact dynamical systems, in analogy with the concept of measure theoretic entropy developed earlier by Shannon and by Kolmogorov and Sinai. This research use entropy calculating which is developed by Shannon. Mathematics Shannon entropy form can be described bellow:

$$H(X) = -\sum_{i=1}^{n} P(x_i)\log_2 P(x_i) \quad (4)$$

H is a message entropy value. H can be defined by calculating P or probability from each character. n is a number of character of message which multiplied with logarithm base 2 from each character probability. Example:
Cipher text: ueihfkandl

Probability of each character from the chiper text above, is described bellow:
P(u) = 0.1, P(e) = 0.1, P(i) = 0.1, P(h) = 0.1, P(f) = 0.1,
P(k) = 0.1, P(a) = 0.1, P(n) = 0.1, P(d) = 0.1, P(l) = 0.1

Each probability above is calculated using formula (4). The result of chiper text entropy below:
H(X) = 3.321.

C. Data

The data that is used in the research this time there are 2 case, that is the case with normal input and cases with extreme input [14]. Test with normal input is a regular message sent, while the test with extreme input that is close to the limit of

maximum, minimum and median value. It aims is to determine the influence of cryptographic algorithm to the message.
The input data as follows:

Table 1. Input Data

No	Plain text	Key
1	You are going to New York	wherehere
2	Answer the phone please	Message
3	aaaaaaaaaaaa	Good
4	zzzzzzzzzzzz	runs

IV. Implementation and Evaluation

The implementation is using Matlab programming language. There are two programs in this research, first program use for encryption process. In this encryption program there are two cryptographic algorithms are RC4 and Vigenere. This program is to encrypt data stored in a Microsoft Excel file and the result is saved to Microsoft Excel to be processed using Chaos program.

At the Figure 2, it is a second program which is used for doing chaos process which will be shown on a graph form.

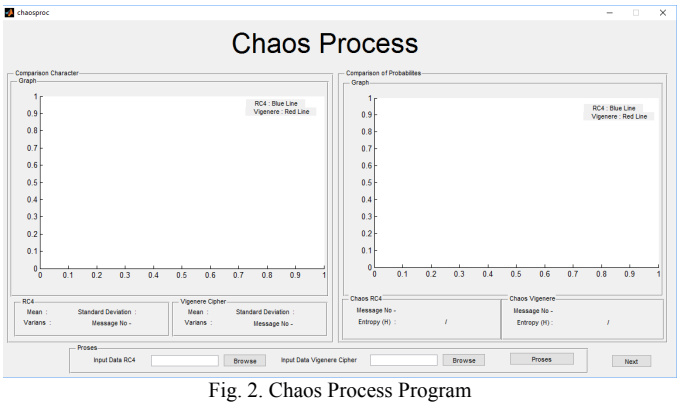

Fig. 2. Chaos Process Program

On the Figure 2, there is two browse buttons to input the result of encryption file and vigenere cipher. Process button for calculating Symbolic dynamic Entropy by Shannon and show it on the graph form, so the difference graph of RC4 algorithm and vigenere Cipher is clearly shown.

After implementing the program, the data will be analyzed. The data is below:
Plain text : You going to New York
Key : wherehere
All of the data above will be encrypt with RC4 or vigenere cipher and then analyzed by using Chaos Algorithm.
From the data above the result as:

Plain text : You going to New York
key : wherehere
Cipher text RC4 : G™˜\ë%☼ íÍwþë7oÄµt◄ tù!²”-x
Cipher text Vigenere : tvyqeyiqkjprxd sqr cdosyo
Comparison chart of probability character result from encription process using RC4 algorithm with vigenere chiper is below

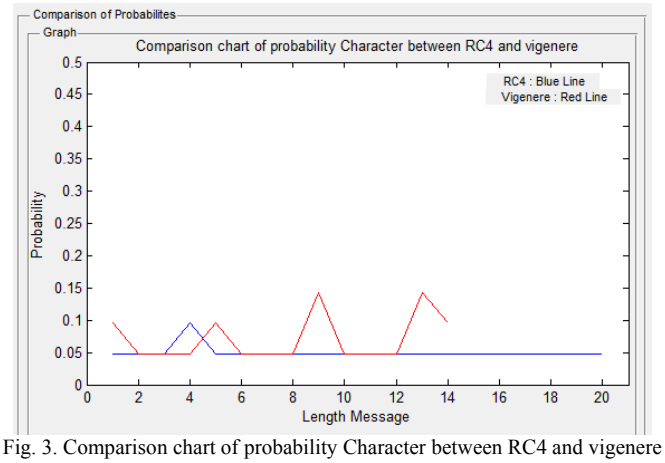

Fig. 3. Comparison chart of probability Character between RC4 and vigenere

From Figure 3, it can be seen that red line is probability character as a result from encription process with vigenere algorithm. The result of Vigenere Chiper encription's character is shorter than blue line which is a probability character from encription's result by using RC4. It means that there are many repeated characters on vigenere cipher algorithm.

Probability character from red line is bigger than blue line probability which have almost the same of mean probability from each character. By using Shannon estropy calculation, result is 4.488 bigger than Vigenere chiper algoithm result 3.863 from maximum value 4.643.

Encription process from another data is described below:

Table 2. Result Encrypt RC4

Plain text	RC4 Cipher text
You going to New York	G™˜\ë%☼ íÍwþë7oÄµt◄ tù!²”-x
Answer the phone please	4n°“ì²í³%FDš‘œ3¿┘ £è LE
aaaaaaaaaaaa	I☼ ŸF#Ã=(LWV┘ ú
zzzzzzzzzzzz	`8ºØRIÐ¸và [0

Table 3. Result Encrypt Vigenere Cipher

Plain text	Vigenere Cipher text
You going to New York	tvyqeyiqkjprxd sqr cdosyo
Answer the phone please	mrjnexdelwrpnszirglkedi
aaaaaaaaaaaa	goodgoodgoodg
zzzzzzzzzzzz	pslqpslqpslqp

Table 2 and Table 3 are result encryption program from another data. After processed with chaos program by calculating entropy value obtained the following result:

Table 4. Result Entropy

No	Entropy RC4	Entropy Vigenere	Entropy Max
1	4.483	3.863	4.643
2	4.523	3.762	4.523
3	3.700	1.526	3.700
4	3.700	1.987	3.700

Chart form of Result Entropy (Table 4) is below:

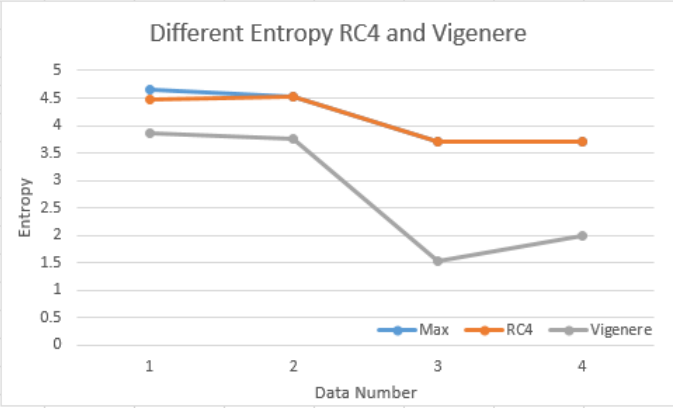

Fig. 4. Differential Chart of Entropy RC4 and Vigenere Cipher

From Figure 4, entropy result of RC4 is bigger and almost reach maximun value than vigenere chiper entropy result. These result shows algorithm encription RC4 is more unpredictable or more chaos than algorithm encription Vigenere Chiper.

V. Conclusion

Based on this research, it can be concluded that this program can measure the quality of an algorithm from its randomization. Randomization from chaos program can be detected by calculating entropy each algorithm, which is algorithm RC4 is more randomized than vigenere cipher. Next, this method can be used to detect the quality of other cryptography algorithm easily.

References

[1] Matthews, R. (1984). "On the derivation of a "Chaotic" encryption algorithm". *Cryptologia 8*(1). 29-41

[2] Geng, Z. (2011). "Block Cipher Design: Generalized Single-Use-Algoritm Based on Chaos". *Tsinghua Science And Technology ISSN 1007-0214 13/15 pp194-206 Volume 16 Numer 2, April 2011*.

[3] Sulistyo, B. (2011). "New Methodology of Block Cipher Analysis Using Chaos Game".

[4] Baranger, M. (2004). "Chaos, Complexity, and Entropy*"* USA

[5] Hong, Z. (2010). "Chaos Theory and its Application in Modern Cryptography". *2010 International Conference on Computer Application and System Modeling*.

[6] Ghys, E. (2012). "The Butterfly Effect". *12th International Congress on Mathematical Education, COEX, Seoul, Korea*.

[7] Kocarev, L. (2001). "Chaos-Based Cryptography: A Brief Overciew". *IEEE.*

[8] Munir, R. (2006). "Kriptografi*"*. *Bandung: Informatika*.

[9] Stallings, W. (2005). "The RC4 Stream Encryption Algorthm"

[10] Lesne, A. (2011). "Shannon entropy: a rigorous mathematical notion at the crossroads between probability, information theory, dynamical systems and statistical physics". *France*.

[11] Frigg, R. (2005). "Chaos and randomness: An equivalence proof of a generalized version of the Shannon entropy and the Kolmogorov–Sinai entropy for Hamiltonian dynamical systems". *Chaos, Solitons and Fractals 28*.

[12] Williams, S.G. (2005). "Introduction to Symbolic Dynamics". *Proceedings of Symposia in Applied Mathematics*

[13] Gullick, D. (1992). "Encounter with Chaos". *McGraw Hill*.

[14] Rahardjo, B. (2014). "Keamanan Perangkat Lunak". *PT Insan Infonesia*.