PERFECT SECRECY SYSTEM BASED ON CHAOTIC KEY GENERATOR

Mahmood K. Ibrahem[1], Hussein A. Qasim[2]
College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
{mahmoodkhalel[1],hussein.ali[2]}@coie-nahrain.edu.iq
Received: 25/12/2017, Accepted: 20/03/2018

***Abstract*-Shannon defines perfect secrecy for a cryptographic system as such a cryptographic system in which the ciphertext yields no possible information about the plaintext. Diffie and Hellman suggest computationally secure cryptographic systems even if the intercepted data contains sufficient information to allow a unique solution to the cryptographic problems. In this paper, we present a new idea to cipher data with a perfect secrecy properties based on the chaotic maps for generating a one-time random key used to encrypt text data. The output of ciphertext process has been examined and shows perfect random properties, ideal performance and throughput compared with block cipher systems.**

***Keywords:*Perfect Secrecy, one-time-pad system, Chaotic Cryptography**.

I. INTRODUCTION

The security of cryptosystems is directly related to the hardness associated with the inverse encryption transformation of a system. The protection levels afforded by the encryption process can be estimated by the uncertainty facing an attacker in determining the permissible keys that used in encrypting data when transfer keys to a hostile environment. Cryptographic systems may be secured in two fundamentally different ways. In some cryptosystems, the amount of data available to the cryptanalyst is essentially insufficient to determine the enciphering and the deciphering transformations processes, no matter how much analysis time and computer power the cryptanalyst have available, a cryptosystem, in this case, is called unconditionally secure system. Shannon [1] called such secrecy as perfect secrecy and defined it as such a cryptographic system in which the ciphertext or cipher data yields any possible data about the plaintext or plain data (except its length). Shannon theorized that it is only possible if the number of possible keys is at least as large as the message itself and no key can be reused (one-time-pad key) [2]-[3]. Since then an extensive theoretical and practical work, have been done to reach a perfect simulation of the one-time-pad system. If the intercepted data contains sufficient information to allow a unique solution to the cryptographic problems, there is no guarantee that cryptanalysis attains a correct solution can be found with minimum computational time and limited computational resources while ensuring that the cryptanalytic operation, will be too complex. Diffie and Hellman [4] called a task of this magnitude as computationally unfeasible, and the associated cryptographic system as a computationally secure system. Chaotic Cryptography has been effectively used for encrypting large-scale data such as image, audio, and video data, because the chaotic map has a good characteristic like generating a key with long periodicity, pseudo randomness number, and sensitivity to change in the system parameters and initial conditions of chaotic maps. The main goal of deploying a chaotic cryptosystem is to provide encryption algorithms with several advantages over traditional encryption schemes such as high speed in encryption data, high security, and reasonable computational overheads and computational power requirements. These challenges have motivated researchers to explore novel chaotic based data encryption techniques with digital logics dealing with hiding information for fast secure communication networks [5].

In this paper, we present a new idea of perfect secrecy with its mathematical representation, proof, and implementation. Modern cryptosystems as computationally secure systems also are discussed. Three-Dimensional Lorenz chaotic map has been used to generate a one-time key that successfully used to encrypt payload data. Three-Dimensional map is a novel algorithmic operation for the random key generation with a block size equal to 64 random bits is generated at each iteration. The binary floating-point 64-bits format is used to present pseudorandom key from the IEEE-7542008 standard for floating point arithmetic [6].

II. Cryptographic System Definition

An encryption algorithm is defined as data transformations that cannot be reversed by cryptanalysis or unauthorized users, chosen from a family of uniform inverse transformations known as general cryptosystems, or sometimes called simply cipher systems. The parameters that selected the specific transformation are called the key or the encryption key that used to convert comprehensible data into incomprehensible data. The cryptosystem may take several different forms, say; a set of instructions, a program, or a piece of hardware one of which is selected by the enciphering key. Formally, a cryptosystem is a single parameter family of invertible transformation (mapping) of the *Message space(M)*into the $Cryptogram(ciphertext)space(C)$ using *finite length key (K)* [2]. A reversible encryption algorithm:

- Set $E_k : (M) \rightarrow C$ such that $E_k : (m) \rightarrow c$; where $k \in K$, $m \in M$, and $c \in C$.

And inverse of decryption algorithm:

- Set $D_k = E_k^1$.
- Set $D_k : C \rightarrow M$ such that $D_k(c) = D_k[E_k(m)] = m$

The encryption keys should uniquely define the enciphered message; i.e; $E_{k_1(m)} \neq E_{k_2(m)}\ if\ k_1 \neq k_2$. Fig.1 describes encryption and decryption processes.

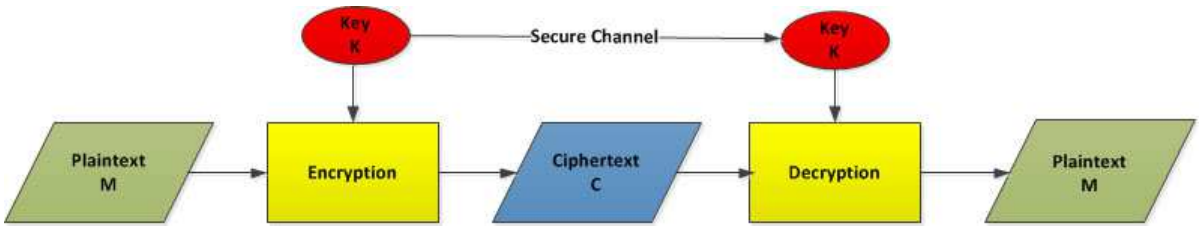


Figure 1: Cryptographic system

III. Security of Cryptographic System

Any system is said to be compromised or insecure via cryptanalysis if it is potential to recover the original data (the plaintext or plain data) from the encrypted data (the encrypted plaintext or plain data), without knowledge of the encryption key used to encrypt the data in the encryption algorithm. Security of cryptosystem does not depend on the concealment of its cipher transformation or cipher algorithm. Generally, these algorithms will be available for all to study and examine.

Security of cryptographic system is directly related to the difficulty associated with inverse encryption transformations of the system. The protection levels afforded by the encryption process can be estimated by the uncertainty facing an attacker in determining the permissible keys that used in encrypting data when transferred in a hostile environment. Shannon [1]defines the unicity distance U as a point may be reached by the cryptanalyst at which a unique solution is possible. He also provides a model for predicting the unicity distance of a cryptogram as:

$$U = H(k)/D, \tag{1}$$

$$D = r_o/r, \tag{2}$$

$$r_o = H(M)/N, \ and \ r = \log_2 L, \tag{3}$$

$$H(K) = \log_2(K), \tag{4}$$

$$H(M) = \log_2(M), \tag{5}$$

Where:

D: is the redundancy of the language,

$H(K)$: is the entropy of the message space,

N: is the length of the message,

L: No. of letters in the language,

r_o: absolute rate of the language,

r_o: rate of the message.

Cryptanalysts used the natural redundancy (difference between rate of message and absolute rate) of the language (D) to reduce the number of possible plain data or plaintexts which is measured as a function of the Entropy of the message space M, and that is why cryptographers use compression programs to reduce the size of the text before encrypting it. In addition, the entropy of the system is a measure of the size of the key space K. Unicity does not give deterministic prediction but gives probabilistic results. [1] and [3] define the unicity distance in order to be able to get some quantitative measure of:

a- The security of the cipher.

b- An indication of the amount of ciphertext needed to break the cipher.

Shannon defined a cryptographic system whose unicity distance is infinite as one that has ideal secrecy (perfect secrecy).

IV. PERFECT SECRECY

Suppose that a cipher system T of a transformation $T = \{t_1, t_2, t_3, t_4, \cdots t_n\}$, with a finite plaintext message, space of message $M = \{m_1, m_2, m_3, m_4, \cdots m_n\}$, and a finite cryptogram (cipher text) $C = \{c_1, c_2, c_3, c_4, \cdots c_n\}$. Suppose for any m_i, the priori probability of m_i being transmitted is $P(m_i)$. If the cryptanalyst intercepts a particular cryptogram c_j then for

each message m_i, can calculate in principle the posteriori probability $P_j(m_i)$ that m_i was transmitted. In another meaning $P_j(m_i)$ is the probability of m_i was transferred giving that c_j has arrived. T is supposed to have ***Perfect Secrecy***[3] if, for every transmitted message m_i and every cryptogram c_j where: $\forall(m_i, c_j) : P_j(m_i) = P(m_i)$. Therefore, the cryptanalyst who intercept c_j has acquired no further information to enable him to decide which message was transmitted during a session. In other meaning perfect secrecy means that for any message m_i, m_j and any cryptogram c_k, the total probability of all key which transform m_i into c_k is the same as of all keys which transform m_j into c_k; $P_i(c_k) = P(c_k) = P_j(c_k)$; and hence the number of keys transform m_i into c_k is the same as the number of keys which transform m_j into c_k. This leads to Shannon [1] - [3] definition of perfect secrecy, ***"In a system with perfect secrecy, the number of different keys is at least as great as the number of possible messages"***. Consider the above cryptosystem T with $P_i = 1/n$ and transformations given as $t_i(m_j) = c_s$ where $s = i + j(modn)$. For example, if $n = 3$ then $t_2(m1) = c_3, t_2(m_2) = c_1$. Fig. 2 gives the complete system for n = 5. To prove that for any n, T has perfect secrecy, we will show that $P(c_j) = P_i(c_j)$ for all m_i and c_j. If we pick an integers $i, k : 1 \leq i_k \leq n$ and $s = i + k(modn)$, then for any i, t_k is the unique transformation with $t_k(m_i) = c_s$, thus: $P(c_s) = P(m_1)P_{k_1} + P(m_2)P_{k_2} + \cdots + P(m_n)P_{k_n}$, but, $P_k = 1/n$ for all k, therefore, $P(c_s) = 1/n[P(m_1) + P(m_2) + \cdots + P(m_n)] = 1/n[\sum P(m_i)] = 1/n$ and $\sum P(m_i) = 1$. Thus, for any s, $P(c_s) = 1/n = P_i(c_s)$ for all i. For any cryptographic system to have sufficient conditions to offer perfect secrecy method

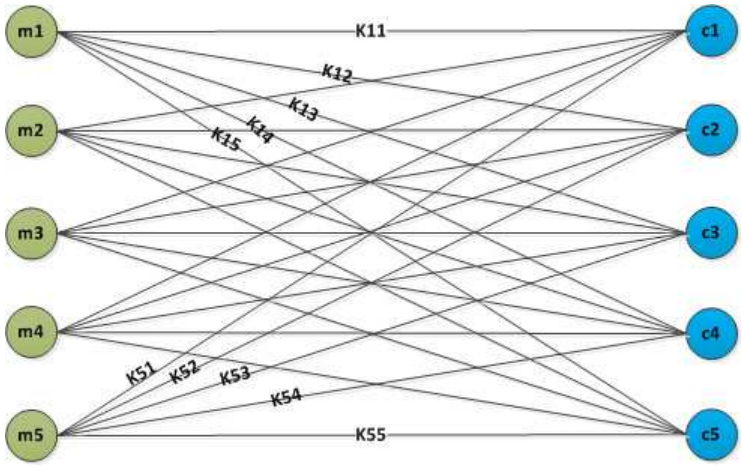


Figure 2: Perfect secrecy for n = 5

can be defined as: Let T be a cryptographic system (cipher system) in which the number of the transmitted messages, the number of keys that used to cipher message, and the number of cryptograms are all equal then T has perfect secrecy if and only if:

a- There is exactly one key encrypting each message to each cryptogram; and

b- All keys are equally likely.

V. ONE-TIME-PAD SYSTEM (OTP)

There is one particular system, which offers perfect secrecy method [7]. The One-Time-Pad (OTP) (Invented in 1917 by Gilbert Vernam and Major Joseph Mauborgne) in this system there is an upper bound N on the length of all possible messages that transmitted between users, and the number of keys which are equally likely is at least as large as N. If the message $M = \{m_1, m_2, m_3, m_4, \cdots m_n\}$ is to be encrypted then a random sequence $K = \{k_1, k_2, k_3, k_4, \cdots k_n\}$ is selected; with both the messages and the keys have same number of possibilities to be chosen, the system is described by Fig. 3 Perfect secrecy also called unconditionally secure under the assumption that the cryptanalyst has unlimited

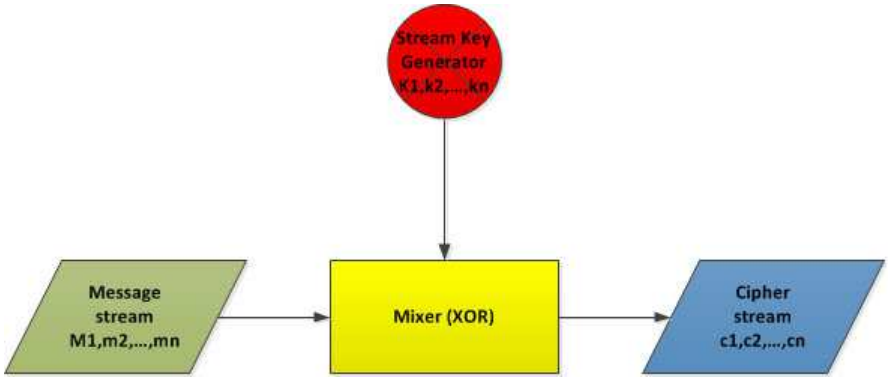


Figure 3: One time pad system

computational resources. According to Shannon, OTP systems have an entropy $H(K) = \infty$, so by (1) : $U = \infty$. One-time pad encryption scheme is successful only if both transmitter and receiver are in possession of the same key space. Therefore, both parties should exchange their keys beforehand in a secure environment. This means that the secure communications are planned and expected within a specific period session. Enough key cipher must be available for all required communications until a new exchange of keys is possible. Exchanging of cipher keys depending on the situation of the system, a large number of keys could be required for a short time period during one session, or little key cipher could be sufficient for a very long period, up to several years.

VI. CHAOTIC THEORY

A chaotic system is a non-linear behavior found in nature. The following are the most important properties of chaotic theory; a behavior of chaotic system pattern is a collection of many non- linear dynamics process. Chaotic system gives and reflects unpredictability and randomness values, and it is very sensitive to necessity in initial condition. Even two identical chaotic systems, they will quickly grow toward completely diverse states, if they are in two marginally different first states. The Butterfly effect shows that a small change in the initial conditions leads to drastic changes in the results. The following are some properties of chaos theory:

a- Unpredictability: Chaos theory shows unpredictability due to sensitivity to initial conditions.

b- Feedback: Chaos theory shows feedback-response behavior. The next value is calculated using the last output as in the case of logistic equation.

Chaotic maps classify into two categories, according to the time range that described by the equations of system, continuous systems that have differential equations, or discrete systems that have difference equations. Logistic map and Henan map are the examples of the discrete systems. The Lorenz system and Rossler system are the examples of the continuous systems [8],[9].

1) *Lorenz Map*: The Lorenz map is standout amongst the most prominent three-dimensional (3D) chaotic map; it was analyzed and presented in 1963 by Edward Lorenz. He demonstrated that a tiny change in the initial conditions, starting states or system parameters of a climate model could give high differences in the subsequent or resulting weather. This implies that a slight contrast in the start state condition absolutely affected on the output of the whole behavior of the system, which is called sensitive system depending on the initial conditions. The nonlinear dynamical system is sensitive to the initial value and is related to the periodic behavior of the system [9].
Lorenz's non-linear dynamic system introduces a chaotic map, while the word chaotic is regularly used to explain the difficult manner of chaotic non-linear dynamical systems. Chaotic theory produces obviously arbitrary conduct yet in the meantime is totally deterministic, Lorenz system exhibits chaotic random behavior. Compared with other three dimensions chaotic map such as Rossler map, the Lorenz map has randomness property, more complicated dynamical property, and number of state variables. Consequently, cryptosystem based on Lorenz system has stronger unpredictability and larger key space, so it can be a candidate to provide excellent random sequence, which is suitable for information encryption. as shown in Fig. 4. The Lorenz attractor is characterized as follow [10]:

$$\frac{dx}{dt} = \sigma(y - x), \tag{6}$$

$$\frac{dy}{dt} = x(\rho - z) - y, \tag{7}$$

$$\frac{dz}{dt} = xy - \beta z, \tag{8}$$

where, $\sigma = 10$, $\rho = 28$, $\beta = 8/3$ are the positive parameters of Lorenz system and x_0, y_0, z_0 are the initial values of Lorenz system between zero and one and t is time.

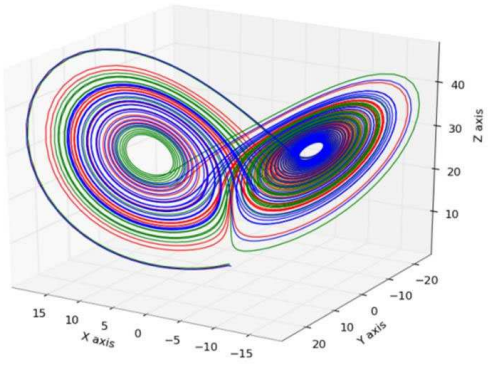


Figure 4: A plot of the trajectory of the lorenz system

2) *Generation a One Time key using chaotic Lorenz map*: One- dimensional chaotic such as logistic map has some drawback that it has low control parameters; it has only one control parameter β but faster in generating pseudo-random numbers. The higher dimensional chaotic system such as Lorenz and Rossler can be used to increase the key space, high complexity and enhances the randomness of pseudo sequence. The algorithm used for generating pseudo random numbers in this paper based on the chaotic Lorenz map given by equations (1, 2, and 3). The differential equations of Lorenz system are three dimensions, which cannot directly get values for this system equation because it has differential and must be solved using Runge Kutta (RK4) method with fourth order. This method can be summarized as [10]: Let the differential equation of Lorenz system $\frac{dx}{dt} = f(x, y, z)$ with initial condition values $\frac{dx}{dt} = x_0$, $\frac{dy}{dt} = y_0$, $\frac{dz}{dt} = z_0$, then the approximate solution of $\frac{dx}{dt}$ using Runge Kutta is given by

$$x_(n+1) = x_n + h/6 * [k_1 + 2k_2 + 2k_3 + k_4], \qquad t_{n+1} = t_n + h, \tag{9}$$

where $x_(n+1)$ is the Runge Kutta approximation of $\frac{dx}{dt}$, h is the interval size, t is time, and

$$k_1 = f(x_n, y_n, z_n), \tag{10}$$

$$k_2 = f(x_n + \frac{h}{2}k_1, y_n + \frac{h}{2}k_1, z_n + \frac{h}{2}k_1), \tag{11}$$

$$k_3 = f(x_n + \frac{h}{2}k_2, y_n + \frac{h}{2}k_2, z_n + \frac{h}{2}k_2), \tag{12}$$

$$k_4 = f(x_n + hk_3, y_n + hk_3, z_n + hk_3), \tag{13}$$

And calculating $y_(n+1)$and $z_(n+1)$ by using the same equations of RK4 that used in calculating of $x_(n+1)$ but replacing equation $\frac{dx}{dt}$ with the $\frac{dy}{dt}$ or$\frac{dz}{dt}$. Runge Kutta has error per step (h^5) and total accumulated error (h^4) and h equal to 0.5. The method that used for generating pseudo-random one time pad based on the output of Lorenz system $K = \{k_1, k_2, k_3, k_4, \cdots k_n\}$. In each iteration, to generate pseudo random number apply a xor operations to the output of $K_n = (x_{n+1}, y_{n+1}, z_{n+1})$ equations and convert to binary 8 Bytes (64 bits).This method allows producing 64 bits random sequences of bits that increasing the throughput of key generation, Fig. 5 shows the proposed scheme to generate one time key based on Lorenz system.

VII. STATISTICAL ANALYSIS

The quality of the output randomness sequences generated by the chaotic Lorenz map is the crucial elements to determine if this sequence is random or not. Indeed, the sequences must be presented individually, decorrelated with each other to measure the randomness, whatever the initial state values or initial conditions. Therefore, careful choosing of a statistical analysis should be conducted to prove the quality of the pseudo random sequences.

1) Evaluation of randomness test: The randomness test consists in evaluating the randomness sequences of the output sequences that generated by the proposed OTP key generating algorithm. In the literature, different types to evaluating statistical tests exist for analyzing the randomness level of random sequences. The NIST (National Institute of Standards And Technology) proposes 15 tests that can be applied to the pseudorandom sequences that generate from chaos maps. These

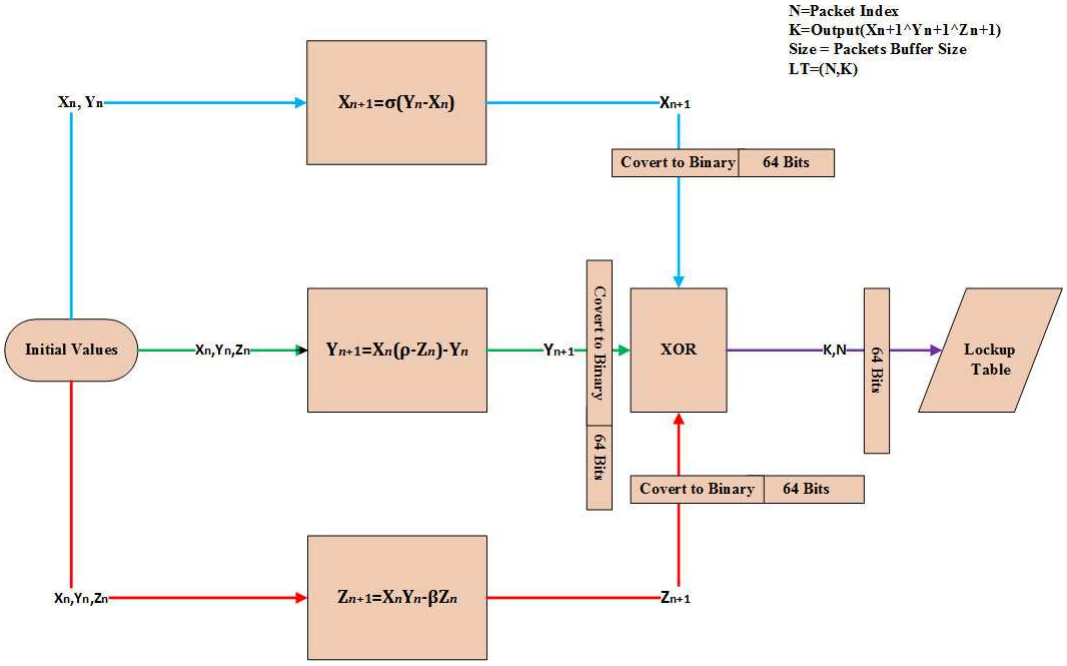


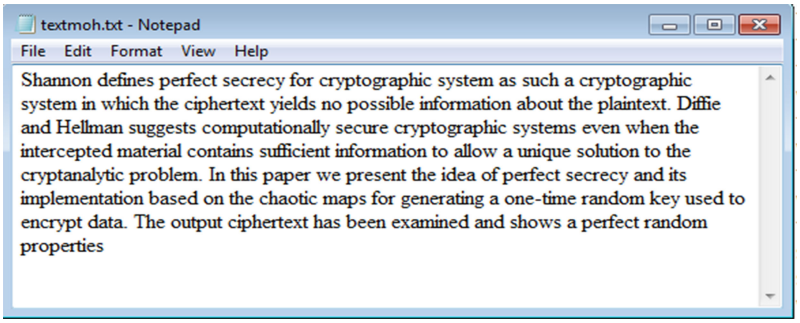
Figure 5: OTP key generation using lorenz map

tests focus on a variety of different types of no randomness that could exist in a sequence. Some tests are decomposable into a variety of subtests. Decision rules of all fifteen tests at the $\%1$ PaletteTicks Level if the computed test value is < 0.01, then conclude that the sequence is nonrandom. Otherwise, conclude that the sequence is random. Table 1 shows the randomness test of the One-Time-Pad that generated by using the Lorenz Map.

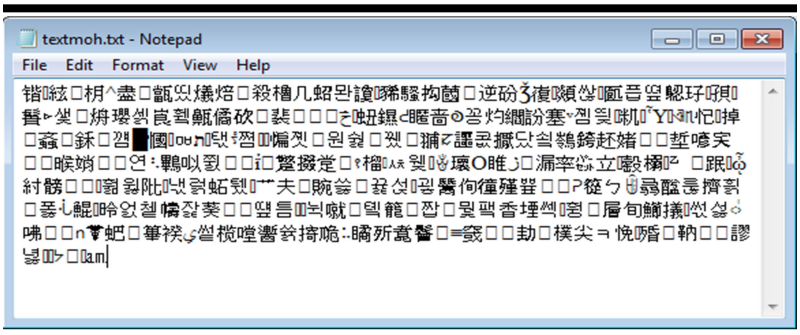
TABLE I
RANDOMNESS TEST OF THE ONE-TIME-PAD THAT GENERATE BY USING THE LORENZ MAP

Test No	Test type	P.Value	State
1	FrequencyTest	0.253551	SUCCESS
2	BlockFrequency	0.739918	SUCCESS
3	Runs	0.253551	SUCCESS
4	LongestRun	0.468595	SUCCESS
5	Rank	0.911413	SUCCESS
6	FFT	0.178278	SUCCESS
7	NonOverlappingTemplate	0.534146	SUCCESS
8	OverlappingTemplate	0.804337	SUCCESS
9	Universal	0.739918	SUCCESS
10	LinearComplexity	0.178278	SUCCESS
11	Serial	0.862344	SUCCESS
12	ApproximateEntropy	0.299251	SUCCESS
13	CumulativeSums	0.100508	SUCCESS
14	RandomExcursions	0.066882	SUCCESS
15	RandomExcursionsVariant	0.017912	SUCCESS

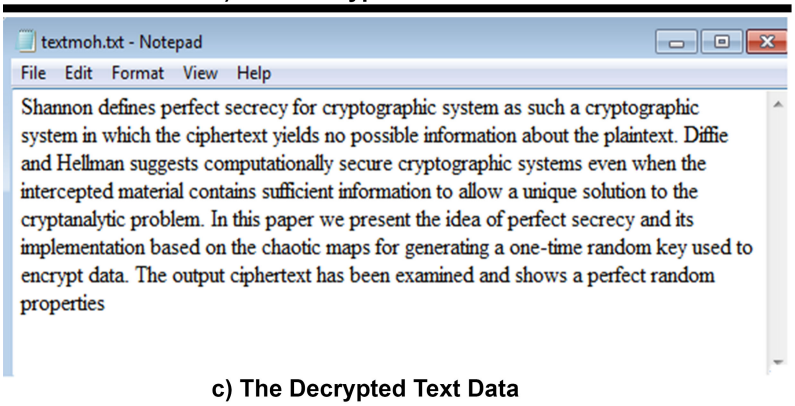
2) Encryption Quality: In this section, we demonstrates the quality of proposed encryption scheme that based on the stream cipher XOR operation to encrypt text data and chaotic Lorenz map to generate sequence of random keys. The results have been implemented using Visual C# 2012 on a laptop Windows 7, Intel Core i3 with speed 2.3 GHz, and RAM 8GB. For encryption experimentations, we used 5-text files with different size. Fig. 6 shows a text data of an original, encryption and decryption text data. From the Fig. 6, the encrypted text has been unintelligible. It is different from the original text. In addition, the decryption text is identical to the original text [11]. Table II shows MSE, PSNR, correlation coefficient (CC) measures of the tested encryption and decryption text data.



a) The Original Text Data



b) The Encrypted Text Data



c) The Decrypted Text Data

Figure 6: The original encrypted decrypted text data

TABLE II
ANALYSIS OF ENCRYPTED TEXT DATA USING PERFECT SECRECY METHOD AND LORENZ MAP

File	MSE of Encrypted data	MSE of Decrypted data	PSNR of Encrypted data	PSNR of Decrypted data	CC of Encrypted data	CC of Decrypted data
Example1.txt	458776.2	0	12.0835266723259	Infinity	0.006141	1
Example2.txt	417895.1	0	13.5023928230192	Infinity	0.006651	1
Example3.txt	478761.8	0	14.012716759745	Infinity	0.006363	1
Example4.txt	352147.2	0	175358474.33428	Infinity	0.007129	1
Example5.txt	391226.7	0	13.0607248605054	Infinity	0.005887	1

TABLE III
TIME PERFORMANCE AND ENCRYPTION THROUGHPUT MEASURES OF PROPOSED ENCRYPTION METHOD

Text data	Size in Bytes	Perfect secrecy and Lorenz chaotic maps for key generating			
		Time (ms)		ET(Byte/ms)	
		Encryption	Decryption	Encryption	Decryption
Example-1	62232	19	19	3275	3275
Example-2	74599	21.5	22	3469	3390
Example-3	542812	169	167	3211	3250
Example-4	856448	247	251	3467	3412
Example-5	822188	236	241	3483	3411

VIII. TIME ANALYSIS AND ENCRYPTION THROUGHPUT

The performance is determined by evaluating the running speed that can be measured by, the average encryption/decryption times, and the encryption throughput. The encryption throughput ET of encrypt or decrypt text data is defined as:

$$ET = \frac{textdata(Byte)}{Encryptiontime(millisecond)} \tag{14}$$

This equation permit to compare the running speed of different cryptosystems working on different platforms. Different encryption algorithms are analyzed using the same tools and the text data in section 7.2, AES with 256-bit long key size as a case study of block cipher, proposed encryption algorithm based on perfect secrecy and Lorenz chaotic maps key generation. Table III shows the time and encryption throughput for each encryption and decryption process of the proposed algorithms and Table IV shows the time and encryption throughput for each encryption and decryption process of the proposed algorithms of AES [12]. The proposed system has been implemented also for voice data and shows ideal results, for more details refer to [13].

IX. KEY SPACE ANALYSIS

The key space (R) is the total numbers of different keys used for the encryption scheme called a key space of the system. It should be large enough to resist the attacker's such as brute-force attack. In the proposed system, signed floating-point precision of used $K^{64}$for the at least $(K = N)$. For both of secret keys $x_0, y_0, z_0, \sigma, \rho, \beta$ for proposed random Lorenz

TABLE IV
TIME PERFORMANCE AND ENCRYPTION THROUGHPUT MEASURES OF AES ALGORITHMS

Text data	Size in Bytes	Perfect secrecy and Lorenz chaotic maps for key generating			
		Time (ms)		ET(Byte/ms)	
		Encryption	Decryption	Encryption	Decryption
Example-1	62232	147	138	423	450
Example-1	74599	162	169	460	441
Example-1	542812	1300	1393	417	419
Example-1	856448	2132	2170	401	394
Example-1	822188	2097	2107	392	390

function. The key space of secret keys system $10^{(64)^{i*p}}$ where i is number of messages that transmitted during one session and p is Lorenz parameters, which equal to six. In case i=one, and p=six, so the size of key space is $R = (10^{64})^{1*6} = 10^{384}$. The key space size σ R of the generated i message sequences (e.g. at least $i = 897$) is 10^{344448} these sizes of proposed system are large enough to resist the brute force attack.

X. CONCLUSIONS

This paper proposed a new idea for new encryption system based on the combination of stream cipher and Lorenz chaotic function to generate one-time pad used to encrypt and decrypt payload of text data. The experimental results show efficient text data encryption, the following conclusions are derived: A. Perfect secrecy systems resists inversion through ignorance of such a possibility. It was proved mathematically that it is unconditionally secure, and it is highly recommended whenever it can be used in classified message exchange. B. Imperfect secrecy (computationally secure) systems are based on the belief of compromisation is beyond the economic means of any interloper by creating computationally difficult problems, which belongs to NP or NP-complete problems. However cryptographic systems should be so secure that there is no best ways to break or analysis it than with a brute-force attack, which in turns should have computational complexity beyond the economic means. C. The results for encrypting and decrypting data quality showed that the proposed encryption approach has an incomprehensible text data and high quality of reconstructed text data. It has perfectly decrypting process with zero MSE, infinity PSNR, and correction equal one, due to the lossless encryption based on bitwise XOR operation of text data and stream cipher does not involve any substitution or an approximation process.

REFERENCES

[1] Shannon, Claude E., "Communication Theory of Secrecy Systems," in *Bell System Technical Journal,*pp. 656 - 715, vol. 28(4), 1949.
[2] Bruce Schneier, *Applied Cryptography, Protocols, Algorithms, and Source codes in C,* second edition, John Wiley and sons, Inc., 2015.
[3] William Stallings, *Cryptography and Networks Security,* Prentic Hall, 2011.
[4] Whitfield Diffie and Martin E. Hellmanr, "Privacy and Authentication: An introduction to cryptography," *In Proc.IEEE,*pp. 397 - 427, vol. 67(3), 1979.
[5] Piyush Kumar Shukla, A. Khare, M. A. Rizvi, S. Stalin and S. Kumar, "Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing," in *Entropy,*pp. 1387-1410, vol. 17(3), 2015.
[6] Mahmood K. Ibrahem, Hussein Ali Kassim, "Implementation of VoIP Speech Cipher with Lorenz map Key Generator", *International Journal of Scientific and Engineering Research*, pp. 533-541, vol. 8, No.7, 2017.
[7] D. Rijmenants, "The Complete Guide to Secure Communications With the One time pad Cipher," *Cipher Machines and Cryptology, 2010, http* : $//users.telenet.be/d.rijmenants$.
[8] Muhammad Iqbal, M. A. Syahbana Pane and A. P. U. Siahaan, " SMS EncryptionUsing One-Time Pad Cipher," *IOSR Journal of Computer Engineering (IOSR-JCE),* PP 54-58, Vol. 18, Issue 6, Ver. II (Nov. - Dec. 2016).
[9] Elwinus H. A. Mendrofa, Elwin Yunith Purba, Boy Yako Siahaan, and Rahmad W. Sembiring, "Collaborative Encryption Algorithm Between Vigenere Cipher, Rotation of Matrix (ROM), and One Time Pad (OTP) Algoritma,"in *Advances in Science, Technology and Engineering Systems Journal*, pp. 13-21, Vol. 2, No. 5, 2017.
[10] George Makris and Ioannis Antoniou, " Cryptography with Chaos," *In Proc., 5th Chaotic Modeling and Simulation International Conference,* June 2012.
[11] Eman Hato and Dalya Shihab, "Lorenz and Rossler Chaotic System for Speech Signal Encryption," *International Journal of Computer Applications,* vol. 128, no. 11, pp. 25-33, October 2015.
[12] F. S. Hasan, "Speech Encryption using Fixed Point Chaos based Stream Cipher (FPC-SC)," *Engineering and Technology journals,* vol. 34, no. 11, pp. 2152-2166, 2016.
[13] Mahmood K. Ibrahem, Hussein Ali Kassim, "VoIP Speech Encryption System Using Stream Cipher with Chaotic Key Generator," *J Fundam Appl Sci.,* vol. 10(6S), pp. 204-210, 2018.