International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

Secure and Fast Chaotic El Gamal Cryptosystem

Edwin R. Arboleda

Abstract: ***An enhancement by combining two existing encryption schemes is proposed. It is a combination of a developed Secure and Fast Chaos cryptography and the El Gamal cryptography. The strength of Secure and Fast Chaos cryptography is the avalanche effect in choosing the number of keys of the sender. A variation in the number of keys used will result in different ciphertext for the same plain text. This is combined with the strength of the El Gamal Cryptosystem which is the difficulty of computing discrete logarithms over finite fields. Using the proposed system, the changeability of choosing the random number k by the sender of information will yield different ciphertext for the same plain text.***

Index Terms: Chaos Function, El Gamal Cryptosystem, Cryptography, Encryption, Decryption.

I. INTRODUCTION

Chaos theory is a field of study that explains a system exhibiting output that is complex, unpredictable and sensitive to the initial condition [1]. In any chaotic system, a change or changes in initial condition would yield different output making them very unpredictable in the long term [2]. Due to its unpredictability, the chaos system attracted a number of researchers in the cryptosystem and other fields [3–12].

Taher El Gamal in 1985 proposed El Gamal cryptosystem algorithm, it is a public-key cryptosystem algorithm applicable over finite fields and uses the Discrete Logarithm Problem (DLP) in its security [13]. The El Gamal Cryptosystem is a very effective application of Diffie-Hellman algorithm [14]. Randomization in the enciphering operation causes the ciphertext for a given message m not to be repeated, for example enciphering the same message twice, will yield different ciphertext {s1, s2}. Probable text attack wherein an intruder suspect a plaintext m then tries to encipher if it is really m will not succeed since the original sender chose a random number k for enciphering, and different values of k will yield different values of ciphertext {s1, s2}. Also, there is no obvious relation between the enciphering of plain texts m1, m2, and m1m2, or any other simple function of m1 and m2, due to the structure of the El Gamal system [15].

In this paper, the chaotic property of the developed secure and fast chaos algorithm [16] is combined with the El Gamal Algorithm [13]. The attractive feature of secure and fast chaos cryptography is the unpredictability on the number of keys that will be used by the sender of the information. The different number of keys will yield different encrypted message. These keys are controlled by initial conditions of the El Gamal cryptography. Both features of [13] and [16] are combined in the key generation. The main equation used in encryption in secure and fast chaos cryptography is replaced by the El Gamal equation for encryption. Likewise, the decryption process in secure and fast chaos cryptography is also replaced by the decryption algorithm of the El Gamal. The security of the proposed system comes from the multiple numbers of keys of secure and fast chaos cryptography and the difficulty of discrete logarithms of El Gamal cryptography.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
Edwin R. Arboleda, Department of Computer and Electronics Engineering, Cavite State University, Indang, Cavite, Philippines.

II. RESEARCH METHOD

II.1. Secure and Fast Chaos Cryptosystem

Khare, Shukla, and Silakari have introduced the Secure and Fast cryptosystem [16] which is a chaotic encryption algorithm using the properties of a chaotic map (sensitivity of parameters) like constant A and initial condition X_n. The developed cryptosystem depends on the number of keys which are generated by the use of the logistic map. A detail discussion on this cryptosystem can also be found in.

The Secure and Fast Chaos algorithm can be described as follows:

P_i = Plain text
C_i = Ciphertext

(i) Algorithm for key generation
1. Decide the values of the parameter (M, A, X_n).
2.Generate the pseudo-random numbers by using an equation. For n=1 to j
$X_{n+1} = \{ A^* X_n (X_n-1) \}$MOD 256
where
A= any integer (1, 2, 3,......)
X_n= initial value of chaotic function which is 2, 3,..........
j = Number of keys
X_{n+1} = keys K_1, K_2, K_3,....K_j (after applying the gray code on X_{n+1})
3. Then generate different multiple values of X_{n+1} (used for keys after applying the gray code on these values of X_{n+1}) and fixed the random numbers by using some specific condition j.
4. The complexity of keys is increased by applying a gray code on X_{n+1} so keys are independent with each other.
5. The keys are shown in 8-bit binary form.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Table 1. The sensitivity of Number of Keys J of Secure and Fast Chaos

Message	Number of Keys J	A	X_n	Keys k_j	Cipher Text
MANILA	1	2	3	10,10,10,10,10,10	G,K,D, C,F,K
MANILA	2	2	3	10,12, 10,12, 10, 12	G,M,D ,E,F,M
MANILA	3	2	3	10,12,72,10, 12, 72	G,M, ACK, C,@, TAB
MANILA	4	2	3	10,12, 72, 48, 10, 12	G,M,ACK,y, D,M
MANILA	5	2	3	48,10,22,72, 48,10	},K,B,SOH, ⎮,{
MANILA	6	2	3	72,48, 10,12, 72, 48	ENQ,g,D, E, EOT,g

(ii). Algorithm for encryption
1. Each character is shown in ASCII character, P_i = ASCII(character i).
2. ASCII character P_i is converted into 8-bit binary form.
3. Using the equation $E_{km}(P_i) = C_i$ for all i >0, and m = 1 to j for encryption, where $E_{km}(P_i)$ is a bitwise XORing on plaintext Pi with single key K_m.
4. Find the 1`s complement of ciphertext (C_i).
(iii)Algorithm for decryption
1. Find the 1`s complement of receiving ciphertext (C_i).
2. Using the equation $P_i = D_{km}(C_i)$. Where m=1 to j for decryption, where $D_{km}(C_i)$ is a bitwise XORing on ciphertext C_i with single key K_m.
3. Plain text P_i is converted into ASCII(P_i) with respect to its decimal value.
4. Then Character i = ASCII (P_i).

The Secure and Fast Chaos cryptosystem was implemented to encrypt and decrypt the message "MANILA". As discussed in [16], the chaotic property of this algorithm is if the values of any integer A, values of random number X_n and numbers of keys J are changed, the completely different ciphertext will be encrypted. However, this paper utilized only the sensitivity to numbers of keys used in its encryption. Table 1 shows that the ciphertext is different as the number of keys used for encryption is varied. For same plain text, "MANILA", if the number of keys is changed, then the ciphertexts also changed.

II.2 El Gamal Cryptosystem

The El Gamal algorithm [13] can be described as follows:
(i) Key Generation
a. Choose a random prime, p .
b. Compute a random multiplicative generator element g , such that g < p)
c. Choose a random number, x, as the private key.
d. Compute the public key , y by

$$y = g^x \,(\text{mod } p)$$

e. Make (p,g,y) public, and keep (x) as private key.

(ii) Encryption
a.To encrypt the message, m , the sender first chose a random number , k such that gcd (k,p-1)= 1
b. Compute, r and s
$r = g^k(\text{mod } p)$
$s=(y^k(\text{mod } p))(m(\text{mod } p\text{-}1))$

(iii) Decryption
To decrypt cipher text , the receiver computes $r^x(\text{mod}p)$ and take the ratio
$m=s/ r^x(\text{mod}p)$

Table 2 shows the encryption of the message "MANILA" using the El Gamal algorithm. Each character of the message is converted to its ASCII decimal equivalent for it to be used as input to the El Gamal algorithm. For the same values of p, and different values of public keys g and y and random numbers k different ASCII values of each character yielded different unique encryptions. Also, the message "MANILA" has two letters "A" and their encryption is different from each other. Even though same prime number p and same private key were used, the encryption would still be different, because of different combinations of values of public keys g and random number k when subjected to the formula $r=g^k(\text{mod } p)$ and $s=(y^k(\text{mod } p))(m(\text{mod } p\text{-}1))$ would yield different remainders.

The unique feature of the encryption and decryption of the El Gamal algorithm is the used of the remainder when a very large number is divided by a prime number. It would be very hard to pinpoint the original unique combination of divisor and dividend that yields that remainder as there is an infinite number of combinations.

Table 2 Encryption Using El Gamal Cryptosystem

Message	ASCII Decimal Equivalent	Public Keys @ p=83, (g_i ,y_i)	Random Number, k @Private key x=7	Encrypted Message, s_i
M	77	9,11	11	2310
A	65	11,16	9	2550
N	78	23,28	13	2964
I	73	33,49	17	3212
L	76	17,36	23	1976
A	65	9,11	3	195

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

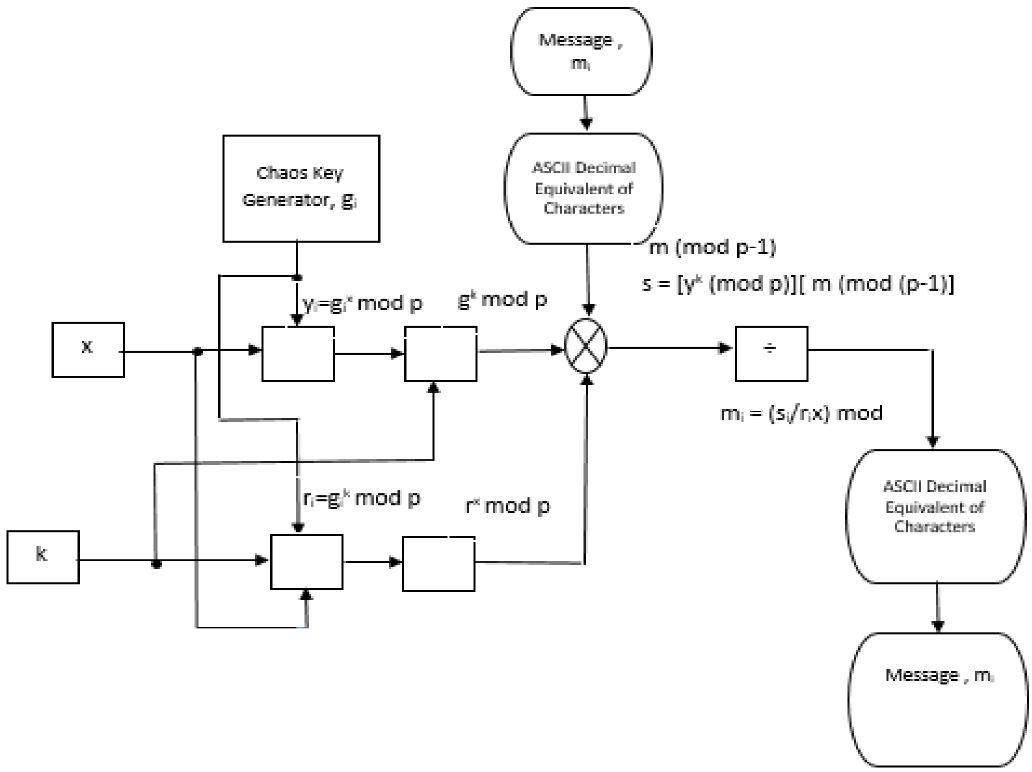

Figure 1. Block Diagram of Proposed Algorithm

II.3 Proposed Hybrid Algorithm Architecture

The proposed method is a merge between the El Gamal cryptosystem and the Secure and Fast Chaos cryptosystem. The strength of the two algorithms are combined, the repetition of multiple number keys of Secure and Fast Chaos cryptography and the use of the remainder when a large number is divided by a prime number of the El Gamal cryptosystem. Figure 1 shows the block diagram of the proposed algorithm. The addition to the conventional El Gamal cryptosystem is the multiple key generators.

This method is explained in the following algorithm:

Key Generation:

1. The sender 's message is any combination of characters that can be found in the ASCII table. It can be letters of the English alphabet, numbers, and symbols which has a corresponding decimal equivalent in the ASCII table.
2. Each character of the message is converted to its ASCII decimal equivalent.
3. The sender picks a prime number p that is greater than the character that has the highest decimal equivalent, m_h plus 1 that is $0< m_h+1 < p$.
4. The sender then decides on the number of pairs of public keys (y's and g's). The number of pair of public keys can be less than or equal to the number of messages, m and send it the receiver.
5. The receiver chooses the private key, x and keep it as a secret and computes the $\mathbf{g_i}^{x}$ and send it to the sender.
6. Based on the chosen random multiplicative generator element g , y_i is computed by the sender using the formula:

$$\mathbf{y_i = g_i^{\,x} \bmod p}$$

Encryption:

1. To encrypt a message m a random number , k is chosen by the sender such that gcd (k, p-1) = 1.
2. The sender computes for r_i

$$\mathbf{r_i = g_i^{\,k} \bmod p}$$

3. The sender computes for s_i

$$\mathbf{s_i = (y_i^{\,k} \bmod p)\,[m_i\,(mod(p\text{-}1))]}$$

4. The unique feature of the proposed method is the use of a repetitive cycle of keys. On a ten-character message and the chosen number of key pairs is 4, the fifth character will utilize the public keys $g_5=g_1$, $y_5=y_1$, therefore, $r_5=r_1$; the sixth character will utilize the public keys $g_6=g_2$, $y_6=y_2$, therefore, $r_6=r_2$; the seventh character will utilize the public keys $g_7=g_3$, $y_7=y_3$, therefore, $r_7=r_3$; the eighth character will utilize the public keys $g_8=g_4$, $y_8=y_4$, therefore, $r_8=r_4$; the ninth character will utilize the public keys $g_9=g_1$, $y_9=y_1$, therefore, $r_9=r_1$; so on and so forth.
5. The sender sends the encrypted message r_i and $\mathbf{s_i}$

Decryption:

1. To decrypt a message , the receiver uses the secret key,x to compute for

$$\mathbf{r_i^{\,x} \bmod p}$$

then

$$\mathbf{m_i = s_i \,/\, r_i^{\,x} \bmod p}$$

I. RESULTS AND ANALYSIS

III.1 Example of the Proposed Method

In this section, the message "MANILA" was encrypted and decrypted using the proposed method

Message: MANILA

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

ASCII Equivalence: M=77, A=65, N=78,I=73, L=76,A=65

1. Key Generation:

Condition: $0<m+1<p$ since $m_h=78$ for N of MANILA $m_h+1=79$ therefore p=83

The sender decided to use 4 key pairs: random numbers g_i such that $g_i<p$)

$g_1=4$; $g_2=10$; $g_3=9$; $g_4=6$ and private key x=8 (x<p)

$y_1 = g_1{}^x \bmod p = 4^8 \bmod 83= 49$

$y_2 = g_2{}^x \bmod p = 10^8 \bmod 83= 23$

$y_3 = g_3{}^x \bmod p = 9^8 \bmod 83= 16$

$y_4 = g_4{}^x \bmod p = 6^8 \bmod 83= 28$

Therefore:

Public Keys: $y_1=49$, $y_2=49$, $y_3=16$, $y_4=28$, $g_1=4$, $g_2=10$, $g_3=9$, $g_4=6$ from sender.

Private key: x=8 is from the receiver and keeps it a secret. Public keys g1,g2,g3 and g4 from the sender are sent to the receiver. The receiver computes for $g_1{}^x$, $g_2{}^x$, $g_3{}^x$, and $g_4{}^x$ and sent back to the sender.

Prior to encryption, a random number k is chosen by the sender such that gcd(k,p-1)=1 therefore k=7 because of gcd(7,83-1)=1

2. Encryption:

Message = MANILA

For M:

$r_1 = g_1{}^k \bmod p$

$r_1 = 4^7 \bmod 83$

$r_1 = 33$

$s_1 = (y_1{}^k \bmod p)\,[m_1(\bmod(p-1))]$

$s_1 = (49^7 \bmod 83)(77 \bmod 82)$

$s_1 = (40)\,(77)$

$s_1 = 3080$

For A:

$r_2 = g_2{}^k \bmod p$

$r_2 = 10^7 \bmod 83$

$r_2 = 77$

$s_2 = (y_2{}^k \bmod p)\,[m_2(\bmod(p-1))]$

$s_2 = (23^7 \bmod 83)(65 \bmod 82)$

$s_2 = (28)\,(65)$

$s_2 = 1820$

For N:

$r_3 = g_3{}^k \bmod p$

$r_3 = 9^7 \bmod 83$

$r_3 = 11$

$s_3 = (y_3{}^k \bmod p)\,[m_3(\bmod(p-1))]$

$s_3 = (16^7 \bmod 83)(78 \bmod 82)$

$s_3 = (10)\,(78)$

$s_3 = 780$

For I:

$r_4 = g_4{}^k \bmod p$

$r_4 = 6^7 \bmod 83$

$r_4 = 60$

$s_4 = (y_4{}^k \bmod p)\,[m_4(\bmod(p-1))]$

$s_4 = (28^7 \bmod 83)(73 \bmod 82)$

$s_4 = (63)\,(73)$

$s_4 = 4599$

For L:

$r_4 = g_1{}^k \bmod p$

$r_4 = 4^7 \bmod 83$

$r_4 = 33$

$s_1 = (y_1{}^k \bmod p)\,[m_5(\bmod(p-1))]$

$s_1 = (49^7 \bmod 83)(76 \bmod 82)$

$s_1 = (40)\,(76)$

$s_1 = 3040$

For A:

$r_5 = g_2{}^k \bmod p$

$r_5 = 10^7 \bmod 83$

$r_5 = 77$

$s_5 = (y_2{}^k \bmod p)\,[m_6(\bmod(p-1))]$

$s_5 = (23^7 \bmod 83)(65 \bmod 82)$

$s_5 = (28)\,(65)$

$s_5 = 1820$

Encrypted Message: $\{r_i,s_i\}$
= { 33,3080} , {77,1820} ,{ 11,780} {60, 4599}, {33,3040}, {77,1820}

3. Decryption

To decrypt the ciphertext { 33,3080} , {77,1820} ,{ 11,780} {60, 4599}, {33,3040}, {77,1820}, the receiver uses the private key x which is a number that only the receiver knows.

$s_1 = \{3080\}$

$r_1{}^x \bmod p= 33^8 \bmod 83=40$

then $m_1 = s_1 / r_1{}^x \bmod p =3080/40= 77$ = M

$s_2 = \{1820\}$

$r_2{}^x \bmod p= 77^8 \bmod 83=28$

then $m_2= s_2 / r_2{}^x \bmod p =1820/28= 65$ = A

$s_3 = \{780\}$

$r_3{}^x \bmod p= 11^8 \bmod 83=10$

then $m_3= s_3 / r_3{}^x \bmod p =780/10= 78$ = N

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Table 3 Sensitivity to the Number of Keys of the Proposed System

Message	Number of Key Pairs	Public Keys p=83, k=7	Private Key	Cipher Text s_i
MANILA	1	g1=4, y_1=49	x=8	3080,2600,3120, 2920,3040,2600
MANILA	2	g1=4, g2=10 y_1=49, y_2=23	x=8	3080, 1820,3120, 2044, 3040,1820
MANILA	3	g_1=4, g_2=10, g_3=9 , y_1=49, y_2=23, y_3=16	x=8	3080, 1820,780, 2920, 2128,650
MANILA	4	g_1=4, g_2=10, g_3=9, g_4=6 y_1=49, y_2=23, y_3=16, y_4=28	x=8	3080, 1820, 780, 4599,3040, 1820
MANILA	5	g_1=4, g_2=10, g_3=9, g_4=6, g_5=12, y_1=49, y_2= 3, y_3=16, y_4=28,y_5 =30	x=8	3080,1820, 780, 4725, 5700, 2600
MANILA	6	g_1=4, g_2=10, g_3=9, g_4= 6 g_5=12,g_6=21, y_1=49,y_2= 23 y_3=16, y_4=28, y_5 =30	x=8	3080,1820, 780, 4599, 5700, 1755

s_4 = { 4599}
$r_4^x \bmod p = 60^8 \bmod 83=63$
then $m_4 = s_4 / r_4^x \bmod p = 4599/63 = 73$ = I

s_5 = {3040}
$r_5^x \bmod p = 33^8 \bmod 83=40$
then $m_5 = s_5 / r_5^x \bmod p = 3040/40 = 76$ = L

s_6 = {1820}
$r_5^x \bmod p = 47^8 \bmod 83=28$
then $m_6 = s_6 / r_6^x \bmod p = 1820/28 = 65$ = A

I. ANALYSIS OF THE PROPOSED METHOD

III.2.A. Sensitivity to Number of Keys

It is claimed by the proposed method that changing the number of keys, would result to complete change in the ciphertexts from one another for the same plain text. In Table 3 it has been represented that difference in the number of keys used generated the different ciphertext. Also, it can be seen in Table 3 that the two letters "A" in the message "MANILA" have been encrypted as the same value of ciphertext in the case of a number of key pairs 1,2,4. When the number of key pairs is 3,5 and 6 the ciphertext for both letters are different from one another. It would be very confusing for Man in the Middle (MITM) attackers to deduce that the same value of ciphertext means same characters as it would be another puzzle for them to know the number of key pairs used by the sender.

III.2.B. Security Analysis

For an encryption algorithm, an avalanche effect is a very important characteristic. Avalanche effect can be seen when changing one bit in plaintext would result in the change in the outcome of at least half of the bits in the ciphertext The avalanche effect is present in the proposed method in terms of the number of key pair used. Changing the number of key pairs change at least half of the ciphertext. In Table 3, one random number k and one private key x were used to encrypt the message. Another implementation of the proposed method is to use not only one random number k but multiple k's for encryption.
Table 4 shows two different implementations of the proposed system. The same message was encrypted using the same prime number, public keys, and private key. The only difference is in the number of k and values of k used. The encrypted message is very much different from one another.
In Tables 3 and 4, the avalanche effect was demonstrated by the proposed method on the number of keys used and also in the number of random numbers used. Using more keys would be more secure but it would slow down the system.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Table 4 The Avalanche Effect of the Proposed System Using One K and Multiple K

MESSAGE	Parameters	Random Number	Ciphertext Si
The_quick_brown _fox_jump_over_ the_back_of_the_ lazy_dog.	p=127; g1=3 g2=5 g3=7 g9=9 g5=11 x=8	k=5	2184,6344,12524,3895,2034,3042,6405,12276, 4387,1710,2548,6954,13764,4879,1980,2470, 6222,13764,4920,1710,2756,7137,13516,4592, 1710,2886,7198,12524,4674,1710,3016,6344, 12524,3895,1764,2522,6039,13268,3895,1998, 2652,5795,14384,4264,1818,2470,6588,12028, 5002,2178,2470,6100,13764,4223,828
The_quick_brown _fox_jump_over_ the_back_of_the_ lazy_dog.	p=127; g1=3 g2=5 g3=7 g9=9 g5=11 x=8	k1=13 k2=13 k3=17 k4=19 k5=23	2184,7904,7171,6840,1921,3042,7980,7029, 7704,1615,2548,8664,7881,8568,1870,2470, 7752,7881,8640,1615,2756,8892,7739,8064, 1615,2886,8968,7171,8208,1615,3016,7904, 7171,6840,1666,2522,7524,7597,6840,1887, 2652,7220,8236,7488,1717,2470,8208,6887, 8784,2057,2470,7600,7881,7416,782

IV.CONCLUSION

The proposed system was able to combine the secure and fast cryptosystem and the El Gamal cryptosystem. It is an improvement of the secure and fast chaos cryptosystem by replacing the encryption and decryption formula by the more secure El Gamal encryption and decryption scheme. It is also an improvement of the El Gamal cryptosystem by providing a cyclical repetition on the key pair used and the number of random numbers used. The proposed method provided for the El Gamal cryptosystem ways of manipulating the number of key pairs and random numbers used for more avalanche effect in the produced ciphertext. The chaotic properties of the proposed system lie in the number of key pairs and the number of random numbers used. To make the proposed system protected from "man in the middle" attacks it is recommended that the signature scheme of El Gamal cryptosystem be integrated into the proposed system.

ACKNOWLEDGMENT

The author would like to thank the faculty members, employees, students and administration of Cavite State University especially to Dr. Hernando Robles, President; Dr. Camilo A. Polinga, VPAA; Dr. Ruel Mojica, VP-RECETS; Dr. Yolanda Ilagan, current Director of Research Center, and to Dr. David L. Cero, Dean of CEIT and Dr. Marilyn M. Escobar, former Dean, CEIT for all the support extended to him in the conduct of the study. Also, the author would like to thank the Department of Science and Technology-Philippine Council for Industry, Energy and Emerging Technology Research and Development (DOST-PCIEERD) for financially supporting his training abroad under the BCDA scholarship program in 2016. To God be all the glory!!!

REFERENCES

1. E. R. Arboleda, J. L. Balaba, and J. C. L. Espineli, "Chaotic Rivest-Shamir-Adlerman Algorithm with Data Encryption Standard Scheduling," *Bull. Electr. Eng. Informatics*, vol. 6, no. 3, pp. 219–227, 2017.
2. M. Enriquez, D. W. Garcia, and E. Arboleda, "Enhanced Hybrid Algorithm of Secure and Fast Chaos-based, AES, RSA, and El Gamal Cryptosystems," *Indian J. Sci. Technol.*, vol. 10, no. July 2017.
3. [3] S. A. S. Mustaffa, I. Musirin, M. M. Othman, M. K. M. Zamani, and A. Kalam, "Chaotic local search based algorithm for optimal DGPV allocation," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 1, pp. 113–120, 2018.
4. MA. Riyadi, MRA Khafid, N. Pandapotan, T. Prakoso, "A Secure Voice Channel Using Chaotic Cryptography Algorithm", Proc. 2nd International Conference on Electrical Engineering and Computer Science (ICECOS 2018), IEEE, 2018
5. S. A. S. Mustaffa, I. Musirin, M. M. Othman, and M. H. Mansor, "Chaotic mutation immune evolutionary programming for voltage security with the presence of DGPV," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 6, no. 3, pp. 721–729, 2017.
6. H. Ruibin, M. Lequan, and Z. Hongyan, "Research on 4-dimensional Systems without Equilibria with Application," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 16, no. 2, p. 811, 2018.
7. MA. Riyadi, MRA Khafid, N. Pandapotan, T. Prakoso, " FPGA-based 128-bit Chaotic Encryption Method for Voice Communication", In 2018 International Symposium on Electronics and Smart Devices (ISESD 2018), IEEE, 2018
8. G. Xiao, H. Liu, Y. Guo, and Y. Zhou, "Research on Chaotic Firefly Algorithm and the Application in Optimal Reactive Power Dispatch," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 15, no. 1, 2017.
9. C. Zhao and G. Wang, "Application of Chaotic Particle Swarm Optimization in Wavelet Neural Network," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 12, no. 4, p. 997, 2014.
10. M. Gholipour, Yousof; Ramezani , Amin; Mola, "Illustrate the Butterfly Effect on the Chaos Rikitake system," *Bull. Electr. Eng. Informatics*, vol. 3, no. 4, pp. 273–276, 2014.
11. Al-Khasawneh, Mahmoud Ahmad, Siti Mariyam Shamsuddin, Shafaatunnur Hasan, and Adamu Abu Bakar. "An Improved Chaotic Image Encryption Algorithm." In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), pp. 1-8. IEEE, 2018.
12. Kumar, Sunil, Manish Kumar, Rajat Budhiraja, M. K. Das, and Sanjeev Singh. "A cryptographic model for better information security." Journal of Information Security and Applications 43 (2018): 123-138.
13. T. El Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. Inf. THEORY*, vol. 31, no. 4, pp. 469–472, 1985.

14. R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
15. M. Y. Rhee, *Internet Security: Cryptographic Principles, Algorithms, and Protocols.* Chichester, West Sussex, England ; Hoboken, NJ: J. Wiley, 2003.
16. A. A. Khare, P. B. Shukla, and S. C. Silakari, “Secure and Fast Chaos-based Encryption System using Digital Logic Circuit,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 6, pp. 25–33, 2014.

AUTHORS PRIFILE

Dr. Edwin R. Arboleda was born in Indang, Cavite, Philippines on October 1979. He graduated from Polytechnic University of the Philippines with a bachelor of science degree in Electronics Engineering in May 2000 and is a licensed Electronics Engineer. He obtained his Master of Engineering degree from De La Salle University- Manila in 2009. He is a graduate of Doctor of Engineering from the Technological Institute of the Philippines- Quezon City in April 2019. He works as an Associate Professor at Cavite State University, Indang, Cavite, Philippines. His research interests include artificial intelligence, machine learning, internet security, near-infrared spectroscopy, and data mining. Email: edwin.r.arboleda@cvsu.edu.ph