Bulletin of Electrical Engineering and Informatics
Vol. 10, No. 1, February 2021, pp. 404~411
ISSN: 2302-9285, DOI: 10.11591/eei.v10i1.2124

Improved El Gamal public key cryptosystem using 3D chaotic maps

Muna KH. Al-naamee[1], Sura Mazin Ali[2]
[1]Department of Petroleum Technology, University of Technology, Iraq
[2]College of political science, University of Mustansiriyah, Iraq

Article Info

Article history:

Received Jan 9, 2020
Revised May 10, 2020
Accepted Jun 12, 2020

Keywords:

3D chaotic maps
Cryptography
El-Gamal PKC algorithm
Information security
Random numbers

ABSTRACT

Digital information is any type of data that is stored electronically. These data need to protect its assets and unauthorized access to it and therefore need measures to protect digital privacy. This process is done in different ways, one of which is encryption. Encryption provides secure transfer of unauthorized data over insecure channels. In this paper a method is proposed to create the keys to the El Gamal PKC algorithm based on chaos theory. The proposed algorithm uses 3D chaos maps to create keys used in the encryption and decryption process using an El Gamal algorithm. The time spent encoding and decoding in milliseconds was calculated and compared with methods that used 1D and 2D chaotic maps. Also, the results obtained exceeded most of the statistical and NIST tests. The generated results are tested their reactions against many types of attacks. Then, the results showed that the proposed method had an excellent randomness efficiency for creating public and private keys for El Gamal's algorithm.

Corresponding Author:

Muna KH. Al-naamee,
Department of Petroleum Technology,
University of Technology, Iraq.
Email: 150007@uotechnology.edu.iq

1. INTRODUCTION

For large sector of society, the cryptography techniques is becoming a fundamental issue because of the need of secure communications for secure data transmission. It is expected that most of the information transmitted through unsecured channels will be encrypted by the applications that use this information, especially private and secret information. It is known that there are two types of encryption method, which are: symmetric encryption, which uses the secret key called private key encryption, this type uses the same private key for encryption and decryption, and must be known by the sender and recipient of the information. The other type is asymmetric encryption and called Public-key encryption. This type uses two keys, the public key for encryption known to the sender of the message. The second is used for decryption which is known only to the recipient of the message. These keys must be linked so that only the public key is used for encryption and the private key is used for decryption. The recipient of the message can also decrypt it if it also knows the public key. Public key cryptography was invented in 1976 by Whitfield Davy and Martin Hellman. For this reason, acronym for the names called Diffie-Hellman encryption [1-3]. El Gamal's public key cryptography (PKC) algorithm is one of the most efficient and popular algorithms that provide a high level of security. Security of the ElGamal algorithm depends on the (presumed) difficulty of computing discrete logs in a large prime modulus.

Therefore, it needs to choose random and large prime numbers, and this is the most important disadvantage of this algorithm, is the need for randomness in its public and private keys [4]. Chaotic systems are

characterized by their reliance on sensitivity to initial conditions, which are similar to random conditions or random behavior. Chaos systems are used in many applications in many functional blocks of digital communication systems, including encryption, compression and modulation [5, 6]. Many encryption technologies have been proposed. Modern cryptography technique provides essential techniques for securing information and protecting data when transmitting over unsecure channels. In ref. [7] El Gamal algorithm was developed to allow a number of senders to send an encrypted message to a single decrypted recipient. This modification provides an extra level of strength and security for the algorithm due to a number of controls and multiple monitoring. The additional number of private keys allows to add more strength and complexity to the algorithm and make it stand against the brute force or systematic attack. Ref. [8] proposed a new version of El Gamal algorithm, a triple version of the encryption and was decoded by multi-receivers. This method can be used in e-commerce. A multi-receiver version has also been developed which can be used for communication to a secure group. In ref. [9], improvement is proposed by incorporating two existing encryption schemes. It is a mixture of advanced Secure and Fast Chaos encryption and El Gamal encryption. The secure and fast chaos encryption strength is the effect of the failure to choose the number of sender keys. In another work [10], El Gamal cryptosystem (IEC) encryption system was used to encrypt long messages to make it stand up to attacks brute force attacks, mathematical attacks, Known--Plaintext attack, and low-modulus attack. And also the security of this kind of El Gamal algorithm depends on the difficulty of solving the problem of discrete logarithm and the problem of integer factorization.

In ref. [11] an El Gamal-like PKE is proposed and then, showed that the proposed El Gamal-like PKE satisfies the IND-CCA2 sense under the DDH problem in the random oracle model. The proposed El Gamal-like encryption scheme for encrypting large messages is easily proven in the standard model. However, it is contradiction for encrypting large messages efficiently. In ref. [12] the proposed algorithm uses a mixing of 3D logistic map, 3D Arnold Cat map, 2D rotation equation and Chebyshev map to set random values to generate privet and public keys that are used to encrypt and decrypt data. In ref. [13], a combination of Dept-RSA and chaotic maps has been combined to obtain a secure and more complex encryption system than other systems, using both integer factorization and chaotic maps discrete logarithm (CMDL), where the intuder passes through two levels of reverse engineering, concurrently, to return the encrypted text to its plaintext. This system is more efficient in term of performance than regular systems. In another research [14], the logistical map and the tent map, which are kinds of chaotic maps, were used to enhance the randomness of RC4 public and private keys. The experimental results showed a high security level of the proposed RC4 algorithm compared to the original RC4. Also focuses on increasing the security of original RC4 algorithm by increasing the randomness. This is done by replacing the sequential increasing of the state table with random values generated from chaotic maps. The original RC4 is vulnerable to the analytical attack of the state table because the value of initial state is not permuted.

This problem is solved in the proposed algorithm because of a random permutation of the state table using values generated from two chaotic maps Logistic and Tent. In [15] an enhanced RSA cryptography has been proposed using 1D and 2D chaos maps, the results has been good in randomization and NIST tests. The researches depend on power of chaos maps to generate the parameters of RSA cryptography. Ref. [16] a random binary sequences generator is produced that produces the bit sequence. The general structure consists of two parts. First, the mouse device as an unspecified source and the second is a 3D chaotic maps to increase randomness and key security. Images that use old technologies of encryption like AES, DES, RSA, etc. show a low level of security. This issue was resolved with chaos encryption [17]. This research work is based on the chaotic variable key generator which changes the value of encryption messages whenever a different number of keys is used [18]. In this paper, a new method has been proposed to implement 3D chaotic maps with the El Gamal algorithm. And using the 3D chaos theory, a set of random numbers is generated with a huge numbers, then only prime numbers are selected and used as the primary keys for the El Gamal encryption system. Because chaos theory relies on condition parameters, it is difficult to predict the keys. This new system was able to improve the secure and fast of El Gamal algorithm by increasing the power of key pairs and random numbers used to get more avalanche effect in the product ciphertext.The experimental results of implementation are presented, analyzed and discussed.

2. EL GAMAL PKC

The El Gamal algorithm was first described by Taher El Gamal in an article that was published in the proceedings of the CRYPTO'84 conference [19], which specializing in the development of encryption methods. This algorithm belongs to the family of public key encryption algorithms, which in its configuration depends on the discrete-log problem. This algorithm used the Die-Hellman protocol and developed it to be used as a protocol for encryption and decryption. Because of the wide use of this algorithm, it is believed that it is attacks by different types of attacks. So it constantly needs to be developed.

El Gamal public key encryption system: [20]
Key set-up:
Each party (say Bob) chooses the following parameters.
• p–anyprime number (large).
• α - primitive root of p.
• $a \in \{1, 2, 3, \ldots, p-1\}$ – random numbers.
• $\beta=\alpha^a \pmod p$ (*'a'* in a locked box).
Then:
Bob's public key is represent by (p, α, β)
Bob's secret key is represent by a
Encryption:
Choose a random $k \in \{1, \ldots, p-1\}$
The message is a number $x<p$
$E_{public-key,k}(x)=(\alpha^k \pmod p), x \bullet \beta^k \pmod p)$.
So the encrypted text is a pair of two numbers. The first masks k, and the second masks the letter x.
Decryption:
$D_{secret-key}(y_1, y_2)=y_2 \bullet (y_1^a)^{-1} \pmod p)$.
Verify that the decryption is working correctly:
$y_2 \bullet (y_1^a)^{-1}=x \bullet \beta^k \bullet (\alpha^{ak})^{-1}=x \bullet \alpha^{ak} \bullet (\alpha^{ak})^{-1}=x \pmod p)=x$

Observation. The use of the El Gamal algorithm that the encoded text is in the form of random messages. Therefore: The same x has a number of different encryptions. The problem of a discrete logarithm is difficult to solve, since it is neglecting the weak random parts and weak prime numbers. So this algorithm is strong against achosen plaintext attack(using exponential random encoding exponentk). Since this k is specified uniformly before encoding, the same plaintext can lead to different ciphertext *p-1*, one of which is selected uniformly by choosing *k* [20, 21].

3. 3D CHAOTIC MAPS

Chaos theory describes the behaviour of some nonlinear dynamic systems that in certain circumstances show dynamics sensitive to initial conditions. Edward Lorenz defines chose theory as follows: Chaos: when the present determines the future, but the approximate present does not approximately determine the future [22]. The two basic properties of chaotic systems are the sensitivity to initial conditions and mixing property. There are many types of chaotic system maps [23, 24]. Chaos theory is used to produce a series of chaos that is used to control the encryption process.

Several types of chaotic maps that could be used to produce this series. The 1D map showing complex behaviour is the logistics map, and the tent map is aiterated function, which forms a discrete-time dynamical system, also: a more complex analytical quadratic map found, and so on [21, 22]. Because of the disadvantages of the chaotic map 1D, different versions of the 2D chaotic maps were formulated. These are some of these chaos maps: Vladimir Arnold proposed a 2D cat map. Arnold Cat 2D map has chaotic behaviour along with improved, random, and dynamic 1D cat map security. Map of baker is a chaotic map representing an extension of the 1D Tent.Baker map and exhibits deterministic chaos features are used to give a great amount of diffusion. And this forms parameters for encryption key.

The 2D logistic map is a development for its predecessor 1D and to address disadvantages stated earlier. It increases the key space used as well as dependency on the control parameter [24, 25]. 3D chaotic maps then introduced which were more complicated and widely used in data encryption. The family of 3D chaotic maps have many types of 3D maps, one of them is 3D cat maps. Arnold's cat map and its variant methods are mainly used as a building block in encryption, watermarking and pattern recognition. The Arnold Cat map is a discrete chaotic map. Specifically, it is argotic and mixing, the C system, the K system and the Bernoulli system [13, 25, 26]. Arnold's 3D cat map is defined in (1)

$$\begin{bmatrix} x_{t+1} \\ y_{t+1} \\ z_{t+1} \end{bmatrix} = \mathrm{C} \begin{bmatrix} x_t \\ y_t \\ z_t \end{bmatrix} \bmod \mathrm{N} \quad (1)$$

Matrix C is defined as

$$\mathrm{C}=\begin{bmatrix} 1 & a & c \\ b & ab+1 & bc \\ d & abcd & cd+1 \end{bmatrix} \quad (2)$$

Where *x*, *y*, and *z* are state variables and *a*, *b*, *c*, *d* are positive parameters, In many applications, a 3D cat map is used over a module N as a finite state system shown in (1), where the vector $[x_t,y_t,z_t]$ and $[x_{t+1},y_{t+1},z_{t+1}]$ denote the discrete spatial coordinates at the time *t* and *t* + 1, respectively

4. PROPOSED EL GAMAL USING 3D CHAOTIC MAPS

The aim of the proposed development is to increase the confusion and diffusion of the ciphered text and this will be reached by increasing the random strength of the keys used in the encryption. Very large numeric keys are usually used in the public key cryptographic methods. From this point, the proposed study using the chaos maps to generate large, non-repetitive prime numbers (only after a very long period of repetition). These numbers will serve as p to the method of El Gamal resulting in non-repetition of the encryption of the characters in the encoded text and thus increase the strength of encryption method. The following algorithms illustrate the proposed development of the El Gamal method using chaos maps (Arnold 3D).

Algorithm (1): Arnold 3D Chaotic Map based Prime Number Generation Algorithm
Input: Arnold 3D chaotic map initial condition values.
Output: huge random prime numbers.
Begin
1. Initialize Arnold 3D chaotic map parameters.
2. Using Arnold 3D chaotic map for large time to generator random fraction numbers and stored in three buffers.
3. Each time the values stored in storage buffers are updated by converting the real numbers to integers by discardedthe fractional part.
4. Discarded each number less than 3-digit update buffers.
5. Discarded each number more than 20-digit update buffers.
6. Choose an only prime number from buffer depend on Prime number algorithm and update buffer or can convert each number not prime to prime by addition 1 and update buffers.
7. Use these buffers to choose public and private number for each block in security message.

End.

Algorithm (2): Keys Generation Algorithm
Input: Random prime number from 3D Arnold buffers.
Output: Public and Private Keys.
Begin
Buf=0;
Repeat
p − large prime number from the buffer no. Buf.
Buf=Buf +1;
If Buf>3 then Buf=1;
a − primitive root of p.
a∈ {1, 2, 3, . . . , p − 1} − random from the buffer no. Buf.
β=αa (mod p) − ('a' in a locked box).
(p, α, β) − (Bob's public key).
A − (Bob's secret key).
Until get many of keys he needed to encryption all the blocks
End.

Algorithm (3): Encryption Algorithm
Input: Message, Public Keys of Sender, Arnold 3D prime no. list, Period.
Output: Cipher Message
Begin
q=max. prime from Arnold 3D prime no. list.
Split message to many blocks as the static length in each block
Get g of public keys of the receiver
P=1;
Get g from public keys;
For I to the length of blocks do
if P>period
P=1;
end
A=fastexp(g,3D_Arnold_Prime(P),q);
B=fastexp(A, 3D_Arnold_Prime (P+1),q);
P=P+2;
cipher(I)=mod(m(I)*B,q);
Next I
Merge Cipher() blocks to Cipher message
End

Algorithm (4):Decryption Algorithm

```
Input: Cipher Message, Private Keys in Receiver, Arnold 3D prime no. list, Period.
Output:  Plain Message.
Begin
        q=max. prime from Arnold 3D prime no. list.
        Split message to many blocks as the static length in each block
        Get set of public keys of the receiver
        P=1;
        Get g from public keys;
        For I to the length of blocks do
        if P>period
        P=1;
        end
        inv_b=mod((q-1-prime(P)),q);
        Y=fastexp(g,prime(P+1),q);
        Z=fastexp(Y,inv_b,q);
        Plain(I)=mod(Z*cipher(I),q);
        P=P+1
        Next I
        Merge Plain() blocks to Plain message
End
```

The general proposed algorithms for poth encryption and decryption processes, is shwon in Figures 1 and Figure 2.

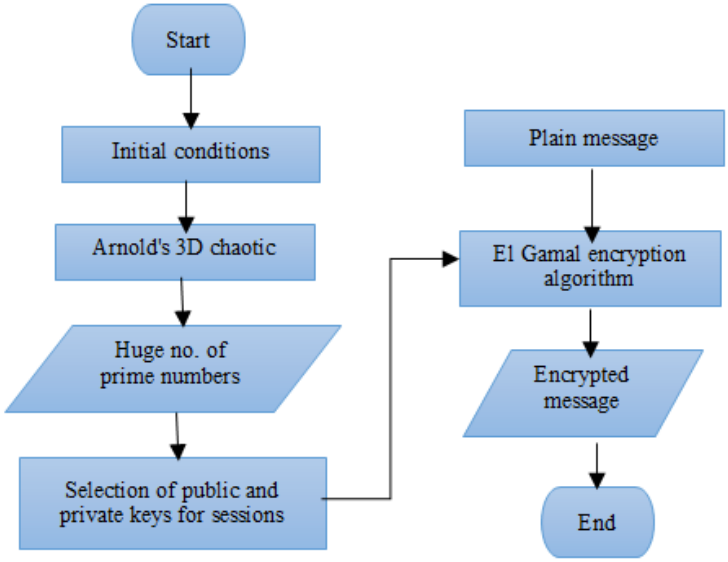

Figure 1. Algorithm flowchart of encryption

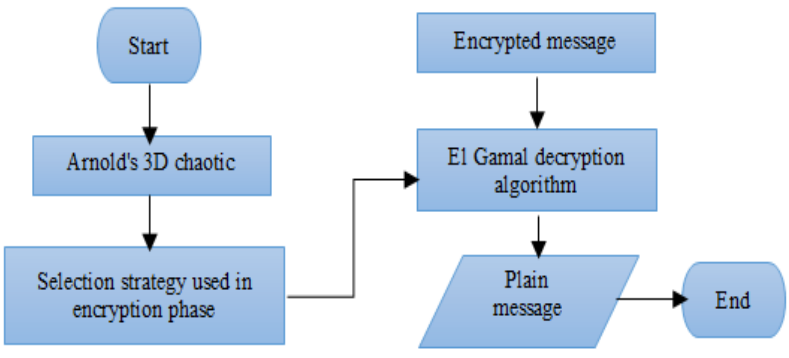

Figure 2. Algorithm flowchart of decryption

5. RESULTS AND DISCUSSION

The work of this research was tested by the evaluation scales like complexity, NIST tests and attacks such as chosen plaintext attack, known plaintext attack, and brute force attack. The method of calculating the computational complexity of coding and decoding of El Gamal method will be calculated, and the generating of the key in 3D chaotic map. The computational complexity algorithm is used to compute the running time for a certain function f is O(F(N)). In the proposed method, the encryption and decryption used the El Gamal method has the same complexity. The deference here is in the calculation of public and secret parameters. The proposed method uses different keys as *k, x, p* , so no method can find the complexity of it, because each block will be encrypted and decrypted with different keys. The key space is large enough for resisting exhaustive attacks likes brute force attack, chosen plaintext attack, and known plaintext attack. The approach utilities as a key enter more than 6 digits as (2^n) breakable in brute-force attacks. For the purpose of increasing complexity, the initial conditions in Arnold's 3D cat chaos map are the matrix *x, y, z* and also the matrix C that has values of, b, c, and d.Each one has its specified value, this will give a large space for generating some keys which is used in encryption and decryption texts (i.e. sending and receiving messages). So it's unbreakable in brute force attack. The excerpted file than will be tested for randomness using the NIST test. The results of testing are shown in Table 1. The results in Table 1 is shown that the encrypted file will pass most of tests which mean the ciphertext has a good randomness properties.

Table 1. NIST tests of El-Gamal with Arnold 3D chaotic map for an encrypted file

No.	Tests	3D	Defect Detected
1	Frequency	Success=0.989631	Too many zeroes or ones.
2	Block Frequency	Success=0.018659	Too many zeroes or ones within a block.
3	Cumulative Sums	Success=0.13547	Too many zeroes or ones at the beginning of the sequence.
4	Runs	Success=0.75008	The oscillation of the bitstream is too fast or too slow through the total number of runs (a large or small number ofruns).
5	Longest Run of ones	Success=0.979435	Deviation of the distribution of long runs of ones.
6	Rank	Success=0.000000	Deviation of rank distribution from a corresponding random sequence, due to periodicity (sub-sequence that is repeated).
7	Discrete Fourier Transform (Spectral)	Success=0.092613	The bit stream has periodic features.
8	Non-Overlapping Templates Matching's	Success=0.99957	A non-periodic templatesare too many occurrences.
9	Overlapping Template Matching's	Success=0.989165	Too many occurrences of m-bit runs of ones.
10	Universal Statistical	Discard	Compressibility (regularity).
11	Approximate Entropy	Success=0.95365	Non-uniform distribution of m-length words.
12	Random Excursion	Discard	Deviation from the distribution of random walk traffic to a given situation.
13	Random Excursion Variant	Discard	Deviation from the distribution of total traffic (across multiple random walks) to a certain state.
14	Serial	Failure=0.000000	Non-uniform distribution of words with length m. Approximate entropy style.
15	Lempel-Ziv Compression	Success=0.987865	More compressed than a really random sequence.
16	Linear Complexity	Discard	Deviation from the linear complexity distribution of finite length (sub) strings.

Also, the proposed algorithm is robust against many attacks. It is verified against these attacks, including: The key sensitivity attack test, a type of statistical attack that verifies the encryption method and the sensitivity of the secret key.Where we see through the table, that any slight change in giving the initial parameter in the chaos gives different results to the output so different from the previous one. It is robust against the chosen plaintext attack, since the attacker selects an arbitrary plaintext and encrypted to produce the corresponding ciphertext and then find the original plaintext. Because of the results of the sensitivity attack described earlier, when any part is changed, even if it is simple, it will produce a completely different ciphertext, and therefore the plaintext cannot be produced. So it is strong against this kind of attack. The proposed system is also effective against the known plaintext attack, since, it is difficult to obtain the correct private key from the value of the initial conditions, public key and known a part of plaintext. The proposed system is also tested against the two basic types of cracking methods-the brute force attack and dictionary attack. So the generated ciphertext is tested to check its reaction against these types of attacks, as below:

- Strength test was 100% approved.

- The evaluation test approved for Chuck Norris.
- It was safe to Dictionary Attack check.
- Time attack was also verified for Brute-force Attack Cracking Time estimate:
  Standard Desktop PC, Fast Desktop PC, GPU, Fast GPU, Parallel GPUs, and Medium Size Botnet. Where the results showed that each examination needs to estimate the time of the Brute-force Attack to about Infinity centillion year.

Finally, in table 2, the comparative encryption time among three ways of using chaotic maps with El Gamal encryption algorithm.

Table 2. Average encrypted time (in Seconds) of 1D, 2D, and 3D of Arnold chaotic map used with El-Gamal encryption algorithm

Algorithm	1024 KByte size	2048 KByte size	3072 KByte size	7680 KByte size
El Gamal (using 1D chaotic map)	1.8	2.91	4.31	8.92
El Gamal (using 2D chaotic map)	1.85	3.03	4.42	9.12
El Gamal (using 3D chaotic map)	2.05	3.14	4.52	9.85

6. CONCLUSION

This paper proposes using of 3D chaotic system for generating a set of random keys to encrypt and decrypt any text file of any size. The proposed algorithm has used three-dimensional Arnold Cat Map of chaotic system with El Gamal encryption algorithm. The aim of using chaos map is to diffuse and confuse the encrypted text more than once to ensure it has high security.Therefore, the most important difference between the new proposal method and the encryption of the El Gamal public key is the use of prime numbers as secret keys and these keys are changed in each session. This gives more difficulty to break from the attacker when the key buffer is created using a 3D chaotic system.The proposed algorithm is tested using NIST test and find that the encrypted file will pass most of tests which mean the ciphertext has a good randomness properties and this give a high level of security and resistance against many types of attacks as well as increase the key spaces. So, the advantage of the proposal method is increasing the randomization of secret keys via increasing the diffusion of key period, which leads to increase the security of public-key cryptography system. The disadvantage of our method is some difficulties in secret keys distribution stage.

REFERENCES

[1] G. C. Kassler, "An Overview of Cryptography," *EMBRY-RIDDLE Aeronautical University, SCHOLARLY COMMONS*, 1998, updated version pp. 1-54, 2016.
[2] D. Boneh, V. Shoup, "A Graduate Course in Applied Cryptography", *Cryptobook.us*, Septemper 2017.
[3] W. Diffie and M. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, Nov 1976
[4] J. K. Grewal, "ElGamal:Public-Key Cryptosystem," *Math and Computer Science Department, Indiana State University*, 2015.
[5] L. Kocarev, "Chaos-based cryptography: a brief overview," in *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6-21, 2001.
[6] N. Holt, "Chaotic Cryptography: Applications of Chaos Theory to Cryptography," *Rochester Institute of Technology*, e-mail:nxh7119@rit.edu, pp. 1-9, 2017.
[7] A. J. Ordonez, R. P. Medina and B. D. Gerardo, "Modified El Gamal algorithm for multiple senders and single receiver encryption," *2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, pp. 201-205, 2018.
[8] M. Mikhail, Y. Abouelseoud and G. Elkobrosy, "Extension and application of El-Gamal encryption scheme," 2014 World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, pp. 1-6, 2014.
[9] E. R. Arboleda, "Secure and Fast Chaotic El Gamal Cryptosystem," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol 8, no. 5, pp. 1693-1699, 2019.
[10] P. Sharma, A. K. Gupta, and S. Sharma, "INTENSIFIED ELGAMAL CRYPTOSYSTEM (IEC)," *International Journal of Advances in Engineering & Technology*, vol. 2, no. 1, pp. 543-551, 2012.
[11] T.-Y. CHANG, M.-Sh. HWANG , and W.-P. YANG, "Cryptanalysis on an Improved Version of ElGamal-Like Public-Key Encryption Scheme for Encrypting Large Messages," *journal: Informatica*, vol. 23, no. 4, pp. 537-562 2012.
[12] A. T. Sedeeq, A. K. Farhan, and Sh. A. Hassan, "A Proposed Public Key Encryption Based on Hybrid Chaotic Maps," *A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq*, vol. 2, no. 2, pp. 64-71, 2017.

[13] N. Tahat, A. A. Tahat, M. Abu-Dalu, R. B. Albadarneh, A. E. Abdallah, O. M. Al-Hazaimeh, "A new RSA public key encryption scheme with chaotic maps," *International Journal of Electrical and Computer Engineering (IJECE),*vol.10, no.2, pp. 1430~1437, April 2020.
[14] Sh. A. Hassan, A. T. Sadiq, and A. K. Farhan, "A Proposal To Improve Rc4 Algorithm Based On Hybrid Chaotic Maps," *Journal of Advanced Computer Science and Technology Research*, vol. 6, no. 4, pp. 74-81, 2016.
[15] A. T. Sadiqet. al., "Using Chaotic Maps to Enhance RSA Public Key Cryptography," *science Internatinal (Lahore),* vol. 30, no. 5, pp.711-715, 2018.
[16] A. K. Farhan, and H. E. M, "Mouse Movement with 3D Chaotic Logistic Maps to Generate Random Numbers," *Diyala Journal for Pure Sciences*, vol. 13, no. 3, pp. 24-39, 2017.
[17] S. Fadhel, M. Shafry, and O. Farook, "Chaos Image Encryption Methods: A Survey Study," *Bulletin of Electrical Engineering and Informatics (BEEI),* vol. 6, no. 1, pp. 99-104, March 2017.
[18] E. R. Arboleda, J. L. Balaba, J. C. L. Espineli, "Chaotic Rivest-Shamir-Adlerman Algorithm with Data Encryption Standard Scheduling," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 3, pp. 219-227, Sep 2017.
[19] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, July 1985.
[20] A. Daeri, A. R. Zerek, M. A. Abuinjam, "El Gamal public-key encryption" *International Conference on Control, Engineering & Information Technology (CEIT'14),* pp. 115-117, 2014.
[21] R. Singh, and Sh. Kumar, "Elgamal's Algorithm in Cryptography," *International Journal of Scientific & Engineering Research*, vol. 3, no. 12, pp. 1-4, 2012.
[22] P. I. Kattan, "Chaos Theory Simply Explained," *Basic Fractals/Chaos Series, Petra Books*, pp. 1-25, 2012.
[23] T. S. Parker and L. O. Chua, "Chaos: A tutorial for engineers," in *Proceedings of the IEEE*, vol. 75, no. 8, pp. 982-1008, Aug. 1987.
[24] F. Dachselt and W. Schwarz, "Chaos and cryptography," in *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498-1509, Dec 2001.
[25] Y. Wu, S. Agaian, and J. P. Noonan, "A New Family of Generalized 3D Cat Maps," *IEEE, arXiv*, 2012.
[26] M. Sharma, Sh. Shankarcharya, M. K. Kowar, "Image encryption techniques using chaotic schemes: A review," *International Journal of Engineering Science and Technology*, vol. 2, no. 6 , pp. 2359-2363, 2010.