Encryption Method Based on Using Logistic Map for E-Government Purposes

Suhiar Mohammed Zeki

University of Technology / Computer Science Department.

Abstract

E-Government can be defined as the utilization of the data and correspondence advancements (ICTs) in order to improve the activities/services of the open division associations. Encryption is the process of the utilizing the algorithms to transform the information to unreadable form of the unauthorized users. The logistic map is a discrete recursive numerical capacity that maps the yield of one cycle of the capacity onto the contribution of the following. In this paper a proposed encryption method using the logistic map is presented. In the proposed work the logistic map is utilized for private keys generation. Also the seeds of the logistic map are considered private keys.

الخلاصة

الحكومة الإلكترونية هي استخدام تكنولوجيا المعلومات والاتصالات (ICTs) لتحسين أنشطة مؤسسات القطاع العام. إن عملية التشفير هي عملية استخدام خوارزمية لتحويل المعلومات لجعلها غير مقروءة للمستخدمين غير المصرح لهم. الخريطة اللوجيستية عبارة عن رياضيات متكررة منفصلة الدالة التي تعيّن إخراج تكرار واحد للدالة على إدخال التالي. في هذه الورقة ، يتم تقديم طريقة تشفير مقترحة باستخدام الخريطة اللوجستية. في الطريقة المقترحة ، يتم استخدام الخريطة اللوجستية لإنشاء المفاتيح الخاصة. أيضا بذور الخريطة اللوجستية تعتبر مفاتيح خاصة.

1. Introduction

E-government alludes to the conveyance of public or neighborhood data of government and administrations by utilizing the Internet and other advanced intends to natives or organizations (agency) or other legislative offices. E-government is a one stop Internet entryway to real taxpayer driven organizations. E-government support the following services [1]:

- The arrangement of important government data in electronic structure in order to provide it an auspicious way to the residents.
- Best management movement to the natives.
- Reinforce of the general population by providing the access to the data without the organization.
- Improved profitability and cost reserve funds in working with providers and clients of government.
- Cooperation in open strategy basic leadership.

The three principle target bunches that can be recognized in e-governance ideas are government, natives and organizations/intrigue gatherings. The outer vital goals center around residents and organizations and intrigue gatherings, the inside destinations center around government itself. Government to Citizen (G2C) can be defined as those services in which the government provides one-stop, on-line access to information and services to the citizens. Government to Business (G2B) can be defined as the government which manages the businesses such as suppliers by utilizing the Internet and other ICTs. Government to Government (G2G)manages services that happen between the various governments associations/organizations [2].With the real progressions in innovation and hardware field, one relentless obstruction has demonstrated to be one of the significant difficulties, specifically: Data Security. To get associated safely and rapidly through the electronic information move through the web, the information ought to be encrypted. Encryption can be defined as the operation of changing the secret data (plain text) into encrypted data (cipher text), in order to ensure misunderstanding or changed with ease by the unwanted persons. It can also be defined as the science which utilizes the mathematics in the encryption and decryption of data [3].The chaotic dynamic system is a critical system that appears to have apparently uncoordinated behavior as a result of its responsive to dependence on its primary conditions and cannot be determined with extreme precision. The behavior of the chaotic system is unpredictable. So it looks like noise. The close relationship between the encryption and the clutter makes the chaos-based cryptographic algorithm a natural prospect for the secure communication and encryption. The similar characteristics of the cryptographic algorithms and chaotic maps have can be classified as the sensitivity to the changes in the initial conditions, the arbitrary control and behavior, and unstable periodic orbits with long periods [4]. The Logistic map can be defined as the one-dimensional map which is utilized in order to prototype clear nonlinear discrete systems. The Logistic map can be explained by the recursive function as follows:

.... Esq. (1). $x_{n+1} = L\left(r, x_n\right) = r \cdot x_n \cdot \left(1 - x_n\right)$

Where r is the parameter of logistic map and xn∈[0,1] . Consider the logistic map L: 0,1 0,1 [ ] → [ ], given by Equation (1), the parameter r lies in interval [0,4] . The return map of the Logistic function is given in Figure (1) for r = 4.The affectability of the Logistic guide to beginning condition could be seen by plotting circle outlines regarding two starting conditions with little contrast. The orbit drawing which is corresponding to the two initial conditions 0.350 and 0.351 for fixed values of r = 4 is drawn in Figure (2). There is fitting sensitivity to the initialcondition.Bifurcation diagram and Lyapunov exponent of Logistic map should be calculated and plotted in order to view the chaotic properties. Figure (3) shows the Bifurcation diagram of Logistic map with respect to “r” are calculated and plotted in. Figure (4) shows the Lyapunov exponent of Logistic map with respect to “r” are also calculated and plotted in. Regarding Figure (3) and Figure (4), Logistic map is chaotic when parameter “r” lies in interval [3.6, 4][5].

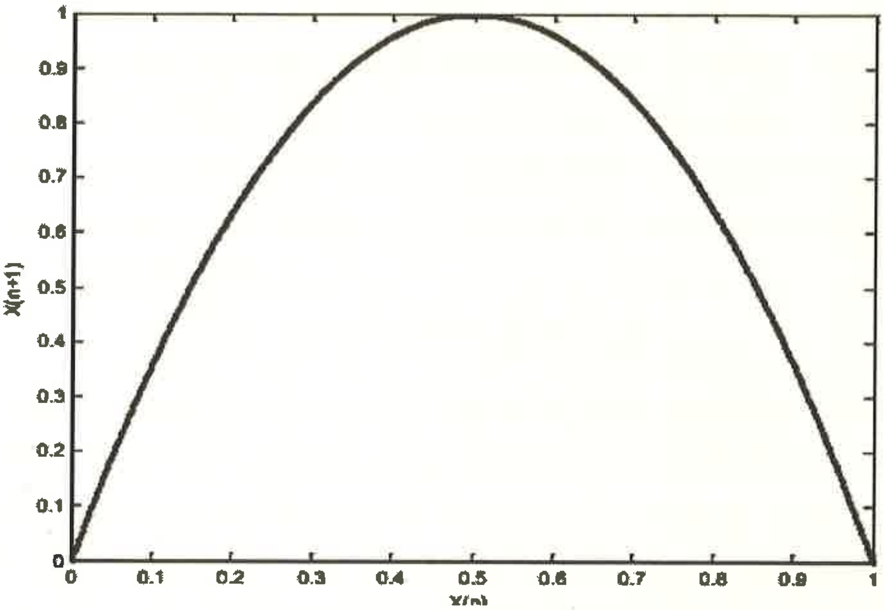


Figure (1): The Return map of logistic map with respect to $r = 4$

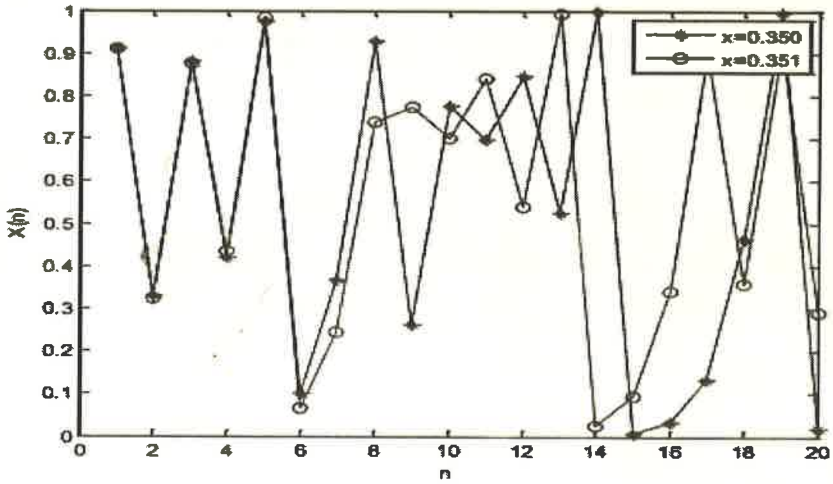


Figure (2): Orbit diagrams of logistic map with respect to two initial conditions 0.350 and 0.351 (r = 4).

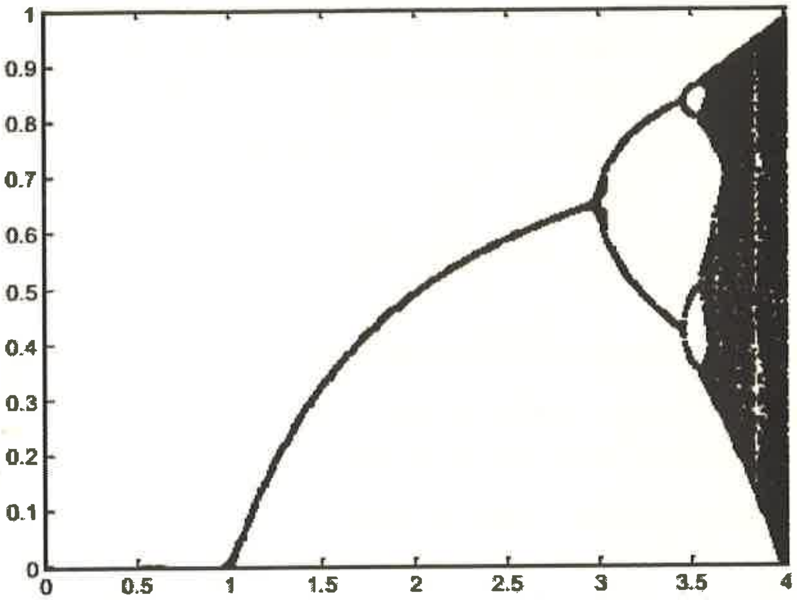


Figure (3): Bifurcation diagram of logistic map with respect to *r*.

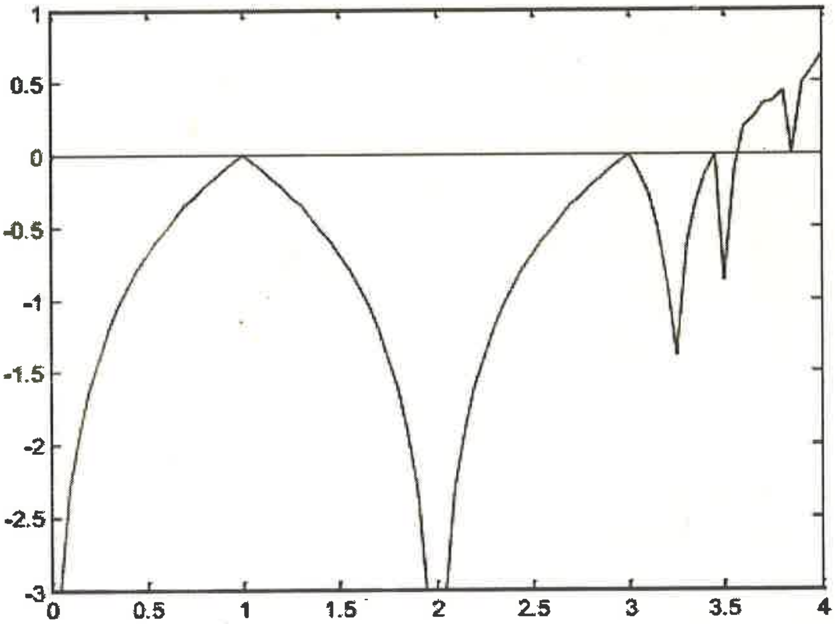


Figure (4): Lyapunov Exponent of Logistic map with respect to *r*.

2. Related Work

In [6] they proposed developed an effective and necessary methodology, which is considered a key factor for the success ofe-government. The presented e-government method is a cooperation of the encryption utilizing the identity and the biotechnology. This modern method can be effectively improving the security of the authentication systems, which supply a dependable identity with a high degree of confidence. In addition, the proposed method illustrates the feasibility of utilizing the limited case of machines as a formal method of analyzing the proposed protocols.

In [7] they introduce the general model of date encryption, points out using different arithmetic according to the degree of cryptograph. After analyzing the disadvantage of the model, it adds the identity validation part to revise the model. Then it explains the procedure of data encryption in E-government, such as how to do identity validation, and how to manage the secret keys.

In [8] they proposed a confidenceprototypein order to ensure the communication and the interaction between e-government web services. The proposed prototype is based on the trusted third party which is managed by any government agency in order to supply an identity to both parties (the web service provider and the service provider), which then can be utilized when the parties or participants communicate and can identify on each other through this trusted third party identity.

In [9] they create new security structure for e-government based on the immune factor, and describe a new policy for the deployment of the e-government system based on the immune factor. The system was developed by adopting new model and algorithm in order to provide the needs of the practical security and supply strong protection.

3. The Proposed Method

Without a secure and reliable infrastructure, organizations, such as governments, will leave data unsafe and vulnerable to the attacks. Governments are always looking for ways in order to provide safe and reliable services. Data encryption is important to E-government information safety. In the proposed method the e-government encryption is presented based the using of logistic map. The logistic map is utilized in the proposed method in order to generate the encryption key. The initial parameters of the logistic map which are x0 and r are considered private keys. After the application of the logistic map sequence of values will be generated. The middle value of these values will be used as the encryption key after converting it to integer value since the values which are generated using the logistic map are float values. After the generation of the encryption key the encryption steps will be applied. Figure (5), figure (6), algorithm (1), and algorithm (2) illustrate the proposed method in details

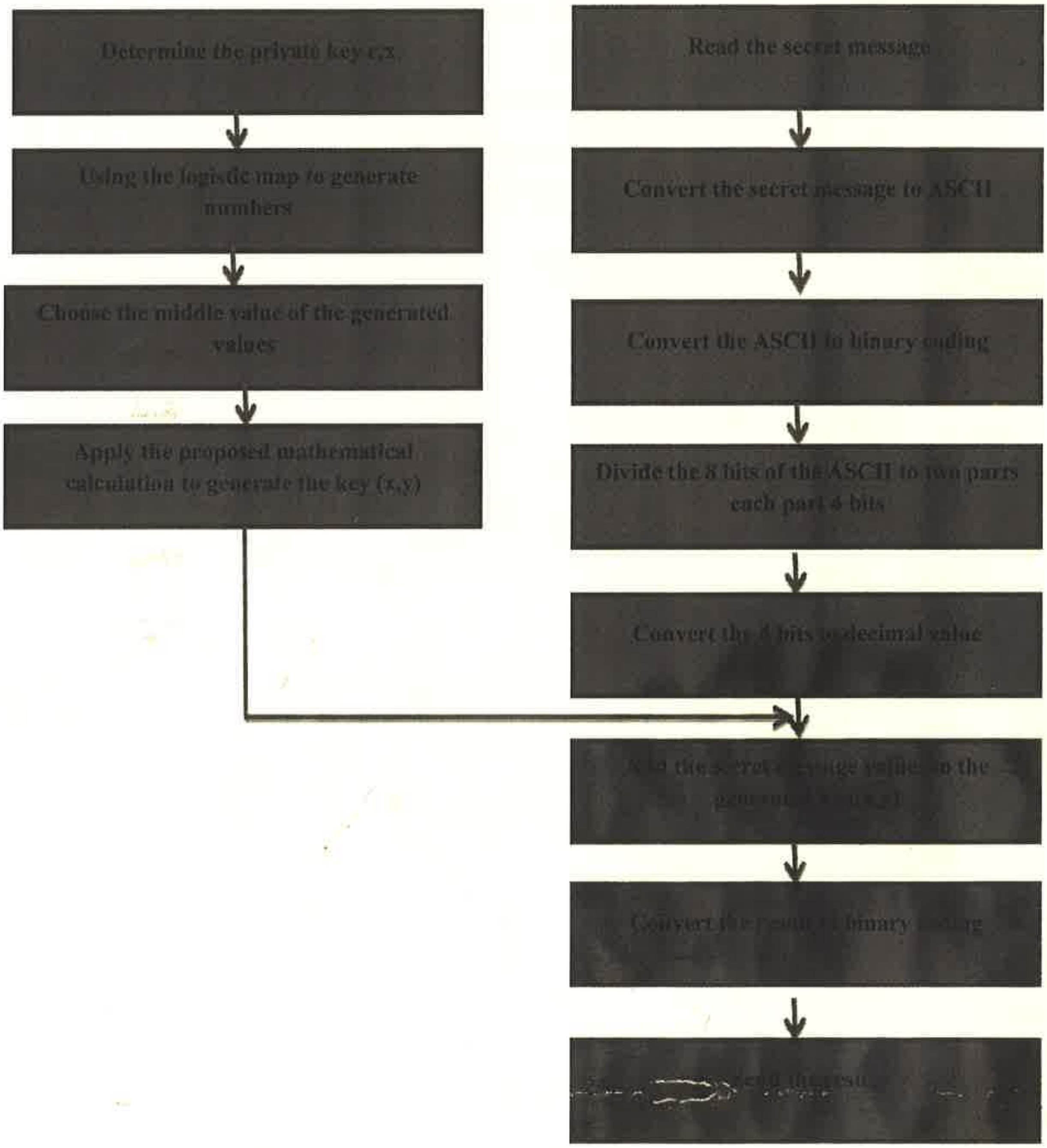

Determine the private key r,x
Using the logistic map to generate numbers
Choose the middle value of the generated values
Apply the proposed mathematical calculation to generate the key (x,y)
Read the secret message
Convert the secret message to ASCII
Convert the ASCII to binary coding
Divide the 8 bits of the ASCII to two parts each part 4 bits
Convert the 4 bits to decimal value
Add the secret message value to the generated key (x,y)
Convert the result to binary coding
send the result

Figure (5): The proposed method (encryption stage)

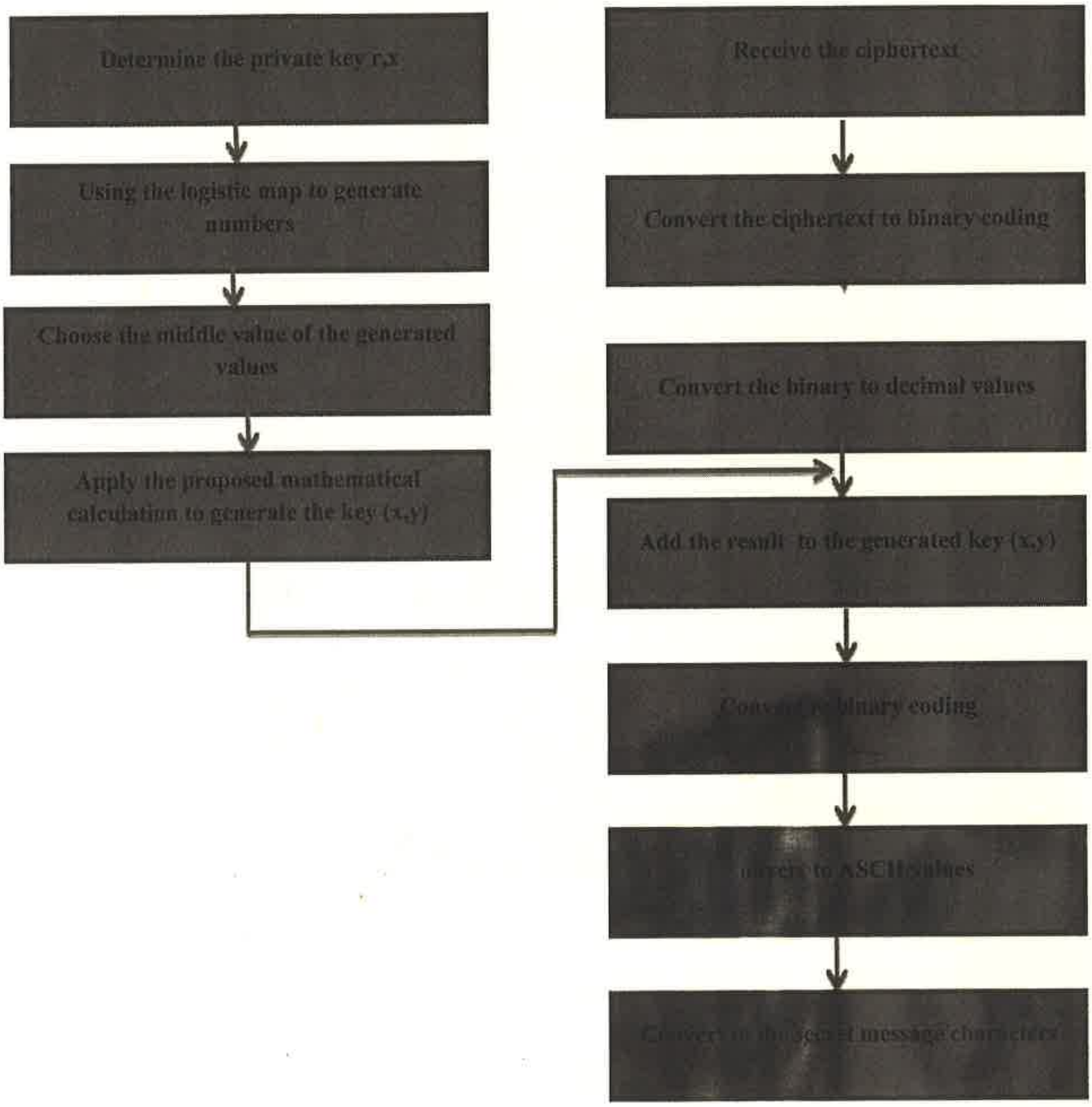

Determine the private key r,x
Using the logistic map to generate numbers
Choose the middle value of the generated values
Apply the proposed mathematical calculation to generate the key (x,y)
Receive the ciphertext
Convert the ciphertext to binary coding
Convert the binary to decimal values
Add the result to the generated key (x,y)
Convert to binary coding
Convert to ASCII values
Convert to the secret message characters

Figure (6): The proposed method (decryption stage)

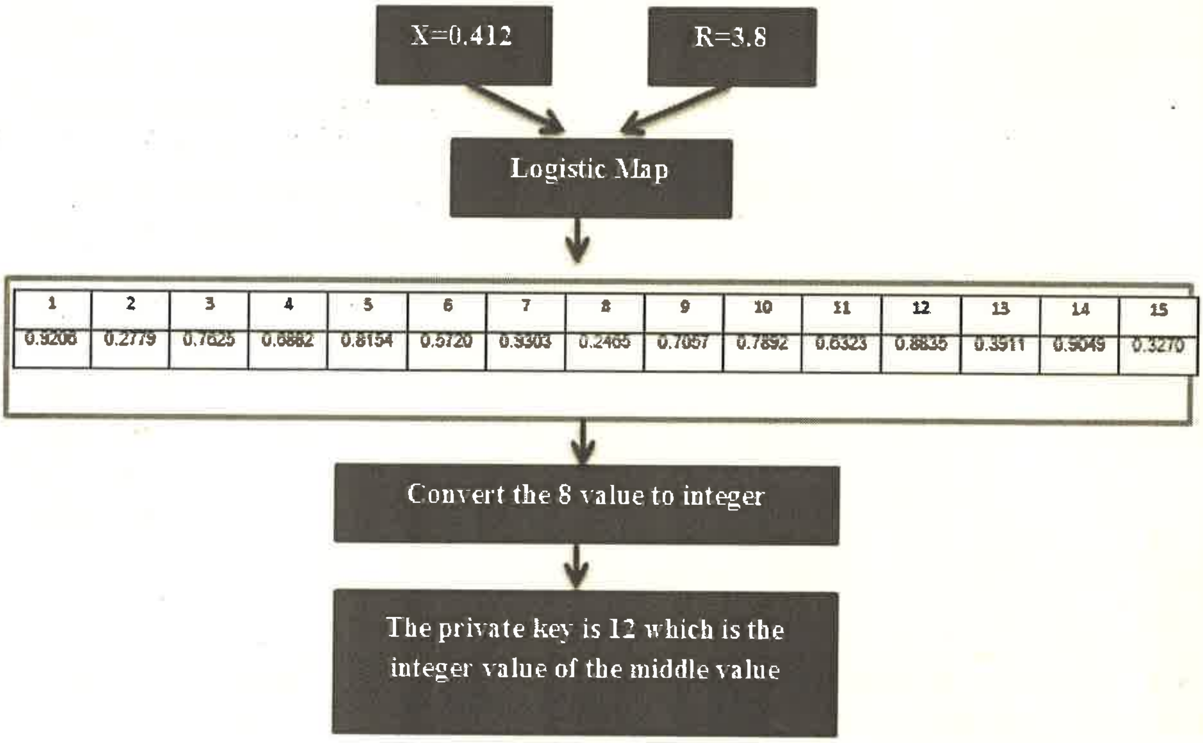
```
Algorithm (1): The proposed method (encryption stage)
Input: The secret message
Output: the ciphertext
Begin
    Step1: Read the secret message characters.
    Step2: Convert the secret message characters to ASCII.
    Step3: Convert these ASCII values to 8bits binary coding.
    Step4: Divide these 8 bits to two parts each part is 4 bits.
    Step5: Convert these 4 bits to decimal values.
    Step6: Determine the x and r values (which are the private keys).
    Step7: Using the logistic map to generate the sequence of values (15 values).
    Step8: Choose the middle value.
    Step9: Add this value to step5 result.
    Step10:Take the absolute value.
    Step11: Convert the absolute value to binary coding.
    Step12: Send the result.
End
```

```
Algorithm (2): The proposed method (decryption stage)
Input: The cipher text
Output: The secret message
```

```
Begin
Step1: Read the received binary ciphertext.
Step2: Convert the received ciphertext to binary.
Step3: Convert the binary to decimal values.
Step4: Determine the x and r values (which are the private keys).
Step5: Using the logistic map to generate the sequence of values (15 values).
Step6: Choose the middle value.
Step7: Subtract this value to step3 result.
Step8: take the absolute value.
Step9: Convert the absolute value to binary coding.
Step10: Convert the binary coding to ASCII values.
Step11: Convert the ASCII values to the corresponding characters.
End
```

4. Case Study of the proposed method

In this section the proposed method two phases will be illustrated in example. The first phase is the generation of the encryption key which is illustrated in figure (7). At the beginning the x0 and r values will be initialized (in the example the values of x is 0.412 and r=3.8). Then the logistic map will be applied to generate sequence of float values which. The middle value of the generated values will be selected in order to converted to integer value and using it as encryption key.


X=0.412
R=3.8
Logistic Map
Convert the 8 value to integer
The private key is 12 which is the integer value of the middle value

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0.9206	0.2779	0.7625	0.6882	0.8154	0.5720	0.9303	0.2465	0.7057	0.7892	0.6323	0.8835	0.3911	0.9049	0.3270

Figure (7): The proposed generation of private key stage

After the encryption key generation the encryption steps will be applied as illustrated in figure (8). First the message characters will be converted to the corresponding ASCII values. After that these values will be converted to 8 bits coding which then will be divided into two parts each part is 4 bits. These 4 bits will be converted to decimal values. These decimal values will be added to the encryption key and taking the absolute value of this adding in order to convert it to binary coding which is considered the ciphertext.

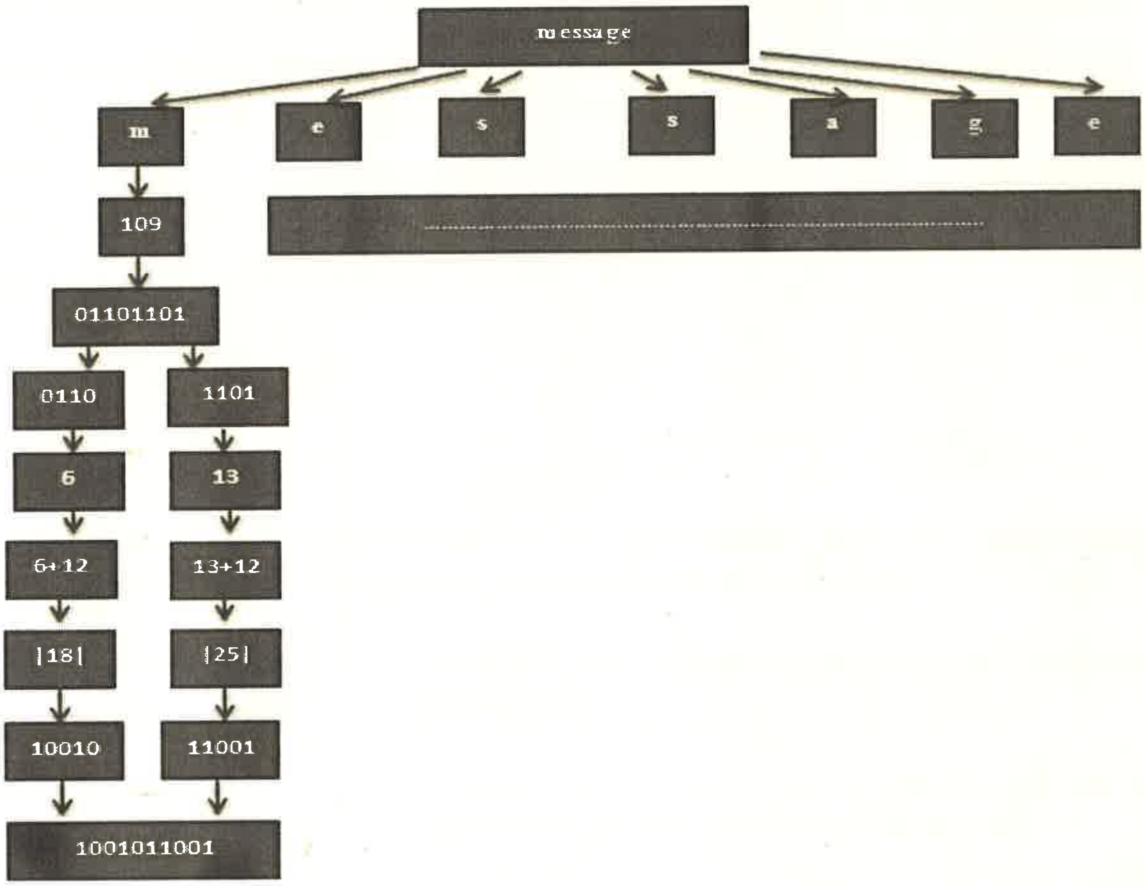


Figure (8): The proposed method (Encryption Steps).

5. Discussion and analysis of the proposed method

The proposed method can be analyzed into two parts which are the key generation part and the encryption part. The encryption key generation part has the following properties:

- The randomness of the initialized values.
- The randomness of the generated values using the logistic map.

In addition to the encryption part has the encryption key generation proprieties, it has high sensitivity to any changes in bits or any data which provide the propriety to discover any changes applied by the attacker, so this feature make the proposed method to be applied to the e-government security systems.

6. Conclusions

E-government plays an important role in these days. E-government transmission needs security in all the fields which is applied in it. In this paper proposed encryption method is proposed for the purposes of the e-government system. In the proposed encryption method the chaos theory is used by utilizing one of its maps which is the logistic map. In the proposed method the logistic map is used in order to generate the encryption key. After that this key will be used in the encryption phase.

References

[1]Shailendra C. Jain Palvia, et al, "E-Government and E-Governance: Definitions/DomainFramework and Status around the World", 2015.

[2]Backus, M. (2001) E-Governance and Developing Countries, Introduction and examples, Research Report,No. 3, April 2001.

[3]Omar G. Abood, et al, "A Survey on Cryptography Algorithms",International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018.

[4]Priya R Sankpal, et al, "Image Encryption Using Chaotic Maps: A Survey", 2014 Fifth International Conference on Signals and Image Processing.

[5]EtemadiBorujeni, S. and Ehsani, M.S. (2015) Modified Logistic Maps for Cryptographic Application.Applied Mathematics, 6, 773-782.

[6]Dania Aljeaid, et al, "Biometric Identity-Based Cryptography for eGovernment Environment", ***Science and Information Conference 2014, August 27-29, 2014 | London, UK***

[7]Liu Liuhua, et al, "Research on E-government date encryption model", 2010 International Conference on E-Business and E-Government.

[8]Bassam Al-Shargabi, “Security Engineering for E-Government Web Services:A Trust Model”, 2016 International Conference on Information Systems Engineering

[9] Zhang Bo-Ping, et al,”Research on E-Government System Network Security Based on Immune A”, 2010 International Conference on E-Business and E-Government.