International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34637-34646

Design and implementation of layered security protocol using Customized Chaotic Code Transformation for Military Applications

B.Amutha, Karthick Nanmaran, Revathy.Nair
Department of Computer Science and Engineering
SRM University, Chennai Tamil Nadu, India- 603203
*Email id: amutha.b@ktr.srmuniv.ac.in

Abstract- Military systems are densely in need of physical layer security. The need for static secure and insecure pseudorandom binary generators to generate random values are not enough to enforce security in a military scenario. Confidentiality, data integrity and authenticity are realized in high level protocol layers. But the physical layer security is a valuable component to provide high-end system security as it forms the basis for all the layers. We developed a new protocol based on complexity integration in the chaotic code through logistical mapping. In this paper, a new protocol for public key cryptosystem with chaotic key management system through logistic mapping is introduced. As bifurcation is a qualitative behavior of the system, we introduce logistic mapping which has an iterative function, which is able to provide chaotic dynamics in its space has been introduced to increase complexity in the system. In military, people at different cadres can view the data at different levels. The other part of the data packet is consumed with chaotic codes along with the information, which could not be opened as it is more complex. This research aims to impose security in military level data communication through the deterministic chaos with Lorenz equations and bifurcations. The cryptosystem has been used to provide public-key cryptosystem features such as key-exchange, chaotic key management system and encryption/decryption of the intended text. In addition, the proposed cryptosystem protocol solves the man in the middle attack problem since it is based on chaotic management systems, on bifurcating r values using logistic map technique.

Keywords- Encryption, R Value, Bifurcation, Logistic map, chaotic code

1. Introduction

Encryption can protect communications and stored information from unauthorized access and disclosure. Even though we have a secured communication technique, the eavesdropper or attacker can able to detect the data. The research work has been carried out to extend security between the military officials based on the cost and computation.

To make and spread confusion to open the data packet along with the data, the chaotic code was introduced. It will increase the non- linearity using the logistic map in the chaotic code. The plaintext which needs to be sent in secured manner will be encrypted with public key using RSA encryption technique and the pseudorandom numbers are xored with the developed key and then it will be sent to the other end. The attacker cannot be able to extract the information even through the medium, because the data packet itself is filled with confusion. The end users will be provided the private key and pseudorandom numbers, so that, they will extract the original information. This concept is known as public key encryption and this method of encrypting messages makes use of two keys: a public key and a private key. The public key is made publicly available and is used to encrypt messages by anyone who wishes to send a message to the person that the key belongs to. The private key is kept secret and is used to decrypt the received messages. An example of asymmetric key encryption system is RSA.

In the developed algorithm, the plaintext is mixed with Chaos sequence mechanism and then it is applied for encryption and decryption process. It is observed that RSA with chaos take less time to be executed and also highly secure when compared to conventional RSA. The results of the proposed chaos based RSA gives a significant improvement for the accepted sequences of probability over a wide range of chaos with initial conditions. Chaos based RSA makes the system more complex and is fast as compared to the Conventional RSA. In any communication system, including satellite, Internet, mobile, etc., it is almost impossible to prevent unauthorized people from eavesdropping, which is a well-known fact. When information is broadcasted from a satellite or transmitted through Internet, there is a risk of information interception, as the data travels long distance.

Chaos owns certain critical properties such as sensitive to initial condition variations, statistical pseudo randomness, random behavior, and uniform distribution. The nature of chaos has initiated lot of interests in different engineering disciplines. Unlike the classical cryptographic algorithms which are primarily based on discrete mathematics, chaos-based cryptography is based on the complex dynamics of nonlinear systems or maps which are deterministic. Therefore, it can provide fast and secure mechanisms for data protection as the sender alone is able to retrieve the mechanism unless he/she shares it with the receiver.

In a non-linear system, a small change in the initial state can lead to a big different action in the final state. The cryptographic system of the present invention may be employed to encrypt and decrypt sensitive information, to authenticate data and video links, or similar applications. The result is an encrypted message that cannot be modified. replaced, or understood by anyone other than the intended party.

Chaotic encryption mainly uses the random sequence -generated by the chaotic system's iteration - as an imput sequence of the encryption transform. This sequence inherits the pseudo randomness of the chaotic system. Moreover, it can make and spread confusion and it does not identify the characteristics of the obtained cipher text after the use of this sequence, to treat the plaintext. This is a great challenge for cryptanalysts. Therefore, the chaos code has been used in some of the encryption systems recently.

- A chaotic system has three key advantages: The sensitive dependence on initial conditions;
- The critical level. This is the point of nonlinear events;
- The fractal dimension, which shows the unity of order and disorder.

Based on strengths and weaknesses of already existing algorithms, Kelber and Schwarz formulated ten general rules to design a good chaos-based cryptosystem which importantly specifies either to use a suitable chaotic map which preserves important properties during discretization for block cipher or to use a balanced combining function and a suitable key stream generator for a stream cipher.

Use a large key space.
Do not use initial conditions of an inverse system as part of the key. Avoid simple permutations of identical system parameters. Use the same precision for sub key values and their corresponding system parameters. Use a complex input key transformation. Use a dynamical system. Use complex nonlinearities.

Modifying nonlinearities in terms of key and signal values and using several rounds of operation for block ciphers increases complexity in accessing data by unauthorized users.

2. Literature Survey

Public-key encryption with chaos was presented by Ljupco Kocarev and Marjan Sterjev. [1] Chaotic systems are characterized by sensitive dependence on initial conditions, similarity to random behavior, and continuous broad-band power spectrum. The possibility for self-synchronization of chaotic oscillations has sparked an avalanche of works on application of chaos in cryptography. The public-key encryption algorithms based on chaotic maps, which are generalization of well-known and commercially used algorithms were proposed such as Rivest– Shamir–Adleman (RSA), El Gamal, and Rabin. The proof of the encryption algorithms is based on the semi-group property of Chebyshev maps and detailed analysis of the periodic structure of torus auto morphisms and also the software implementation was also discussed.

Implementation of AES and RSA using Chaos System was presented by Bhavana Agrawal, Himani Agrawal.[2] In their paper two Cryptographic algorithms using chaos were discussed. They are RSA and AES. Chaos has attracted much attention in the field of cryptography. It describes a system which is sensitive to initial condition. It generates apparently random behavior but at the same time is completely deterministic. Chaos function is used to increase the complexity and security of the system. AES and RSA are the two cryptographic algorithms. In AES we apply the Chaos on S-box. In RSA, the plaintext was mixed with Chaos sequence initially and then encryption and decryption were formally followed. After Implementing AES and RSA, both the techniques were compared on the basis of speed. A Chaos Based Public Key Cryptosystem was presented by M.R.K. Ariffin and N.A. Abu. [3]A new public key cryptosystem that is built by utilizing the classical one-way chaotic beta-transformation mapping. The AAβ -cryptosystem represents its private keys as a vector and uses the parallelogram law to prove that encryption and decryption does indeed occur. The mathematical hard problem for this system is likely to be harder than the classical Discrete Log Problem and to some extent probably equal or slightly better than the Elliptic Curve Discrete Log Problem (ECDLP). Because of this fact, the AAβ -Cryptosystem maybe more secure than the Elliptic Curve Cryptosystem (ECC).

Survey Report on Chaos Based Public- key Cryptosystem was presented by Adel A. El-Zoghabi, Amr H. Yassin, Hany H. Hussien [4]. Now a days, the encryption technology has been used with chaos based cryptographic algorithms. Chaos owns certain critical properties such as sensitive dependence on initial conditions, random behaviour, and continuous broadband power spectrum, which match the confusion, diffusion, and key sensitivity pertaining to the requirements of cryptography. Chaos based cryptographic offer sundry features over the traditional encryption algorithms such as high security, speed, and sensible computational overheads and power. This paper presents a survey of public key encryption methods based on chaos system.

Chaotic Map Cryptography and security was presented by Alexander N. Pisarchik & Massimiliano Zanin.[5] Chaos has emerged as a new promising candidate for cryptography because many chaos fundamental characteristics such as a broadband spectrum, ergodicity, and high sensitivity to initial conditions are directly connected with two basic properties of good ciphers: confusion and diffusion. The main achievements in the field of chaotic cryptography, starting with the definition of chaotic systems and their properties and the difficulties it has to outwit were reviewed. According to the intrinsic dynamics, chaotic cryptosystems are classified depending on whether the system is discrete or continuous. Due to the simplicity and rapidity, the discrete chaotic systems based on iterative maps have received a lot of attention. In spite of the significant achievements accomplished in this field, there are still many problems, basically speed, that restrict the application of existing encoding/decoding algorithms to real systems. The major advantages and drawbacks of the most popular chaotic map ciphers in terms of security and computational cost are analyzed. The most significant cryptanalytic techniques are considered and applied for testing the security of some chaotic algorithms.

3. Methodology

3.1. Bifurcation

A bifurcation is an abrupt change in the qualitative behavior of a system. The iterative, discrete-time view of chaos is powerful because it allows us to see how a system evolves,

step-by-step. Most nonlinear systems are chaotic only under certain circumstances. A discrete-time analysis can help pin down these circumstances. An example of this is, the flow of water, or any fluid. As long as it is allowed to flow at a reasonable speed along a course free of obstacles, fluid flow is nice and predictable. However, as the speed of flow increases, or as obstacles are added in the path of the flow, the flow starts to get somewhat unpredictable. Eventually, under certain conditions, the fluid no longer behaves in a predictable way at all; this condition is called turbulence. [6]

Turbulence is a good deal as it is more complicated and less understood than classic chaos, but the system changes its qualitative behavior, depending on the specific parameters we assign to it. We expect that using different starting values will give us different results, but we also naturally tend to expect that those results will differ quantitatively, will be somewhat similar qualitatively. [7]We might expect that doubling the weight of a moving particle would halve its velocity, given the same amount of force. We would probably also expect that the particle would still get to where it was headed initially; although it might take longer time. In a chaotic system, however, doubling the weight might cause the particle to reverse direction, stop, oscillate between two or more values, or exhibit any number of qualitatively different behaviors.

The point at which a system changes from one fundamental type of behavior to another is called as bifurcation.[8] An important question is "for what values of our system's parameters, does bifurcation occur?" Applied to our system of moving water, the question is "at what speed does the water flow become turbulent?" Answering this question and others like, it is of great importance if we are designing boats, testing aircraft, trying to understand the fluctuations of the stock market, or trying to predict how populations of wild animals rise and fall.[9]

3.1.1 The Chaos

The logistic map is a model of population growth that exhibits many different types of behavior, depending on the value of a few constants.[9].•Above a certain parameter value, the logistic map becomes chaotic.

Let's take a look at one specific iterative function, or map, to see bifurcation and chaos in action. The function we will investigate, often are called the logistic map, represents a highly simplified model of population fluctuations. It takes an initial population level and tells you what the population will be after some fixed interval of time, or time step. The time step can be as long or as short as you care to make it, depending on what species you are studying. For our purposes, we made an arbitrary quantity representing a generation. The equation then, for some population of pn+1 after an arbitrary time step, starting with population xn is:

$x_{n+1} = rx_n(1-x_n)$ ----------(1)

In equation (1), the parameters that we can modify are the growth rate, r, and the initial population, x0. In particular, we would like to know how the growth rate affects the overall behavior of the system.

For example, if r is less than 1, xn goes to zero as n goes to infinity. This means that the population diminishes to the point of extinction.

$f(x)= rx(1-x)$, $x \in (0,1)$, $r>0$ ----------(2)

As $x_{n+1}= rx_n(1-x_n)$

FOR r=1

$x_{n+1}= rx_n-rx_n^2$ ----------(3)

$f(x) = rx_n-rx_n^2$, $f(x)= -rx_n^2+rx_n$ -------(4)

Taking the differential equation,

$f'(x)= -2rx+r$, $r(-2x+1)=0$ ----------(5)

$r=0$, $-2x+1=0$, $1=2x$, $x=1/2 = 0.5$ $f(1/2)=-r(1/2)2+r(1/2)$

$f(1/2)=-r/4+r/2$ $f(1/2)=r/4$ ----------(6)

The maximum point is (1/2, 1/4) or (0.5, 0.25)

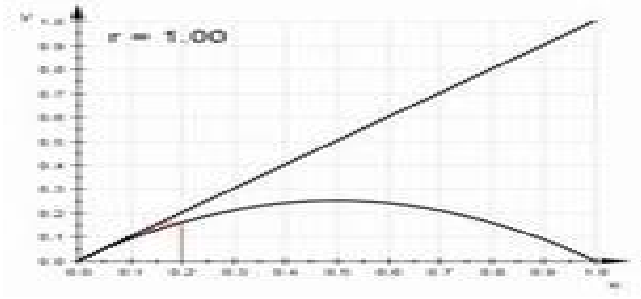

Fig 3.1 logistic map for r=1

For r=1.90

$f(x)=1.90x(1-x)$ ----------(7)

$f(x)= -rx^2+ rx$ ----------(8)

Taking the differential equation

$f'(x)= -2rx+r$, $f'(x)= -2rx+r \Rightarrow -2(1.90)x+1.90$

$-3.8x +1.90=0$, $3.5x=1.9 \Rightarrow x=0.5$ ----(9)

$f(1/2)=-r(1/2)2+r(1/2)$, $f(1/2)=-r/4+r/2$ $f(1/2)=r/4 \Rightarrow$ $1.9/4, x=0.475$ ----------(10)

The maximum point is (0.5, 0.475)

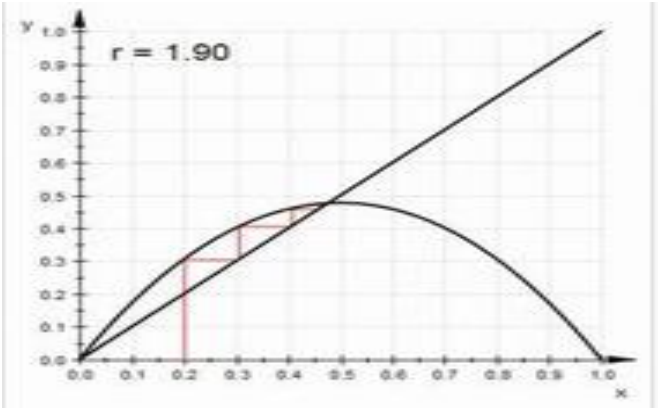

Fig 3.2 logistic map for r=1.90

For r=2.27

$f(x)=2.27x(1-x)$ ----------(11)

$f(x)= -rx^2+ rx$ ----------(12)

$f'(x)= -2rx+r \Rightarrow -2(2.27)x+2.27$ --(13)

$-4.54x +2.27=0$ $4.54x=2.27 \Rightarrow x=0.5$ $f(1/2)=-r(1/2)2+r(1/2)$

$f(1/2)=-r/4+r/2$ $f(1/2)=r/4 \Rightarrow 2.27/4$ $x=0.5675$

The maximum point is (0.5, 0.567)

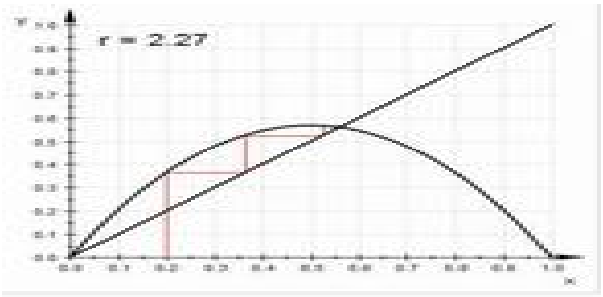

Fig 3.3 logistic map for r=2.27

For r=2.5
f(x)=2.5x(1-x) ----------(14)
f(x)= -rxn2+ rxn ----------(15)
f'(x)= -2rx+r => -2(2.5)x+2.5 (16)
-5x +2.5=0 5x=2.5 => x=0.5
f(1/2)=-r(1/2)2+r(1/2), f(1/2)=-r/4+r/2 f(1/2)=r/4 => 2.5/4,x=0.625 ----------(17)
The maximum point is (0.5, 0.625)
For r=2.8
f(x)=2.8x(1-x) ----------(18)
f(x)= -rxn2+ rxn ---------(19)
f'(x)= -2rx+r => -2(2.8)x+2.8
-5.6x +2.8=0 ----------(20)
5.6x=2.8 => x=0.5 f(1/2)=-r(1/2)2+r(1/2),f(1/2)=-r/4+r/2
f(1/2)=r/4 => 2.8/4,x=0.7
The maximum point is (0.5, 0.7)

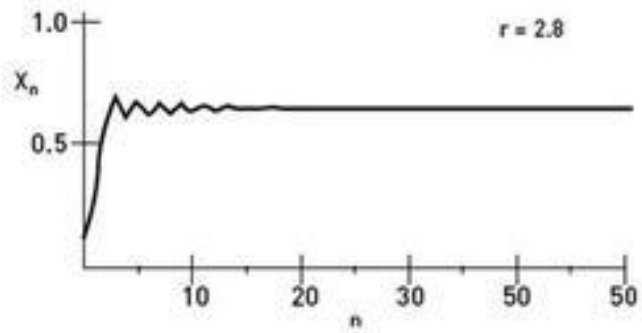

Fig 3.4 Graph for r=2.8

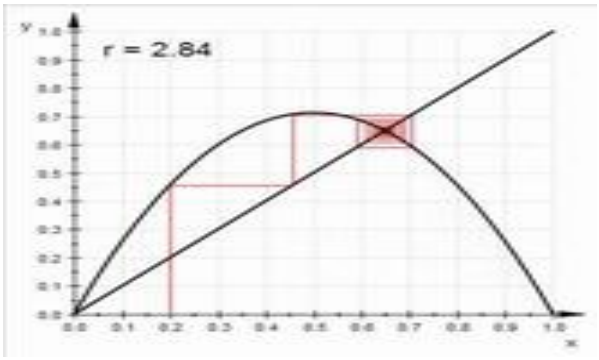

Fig 3.5 logistic map for r=2.84

If r is between 1 and 3, the population eventually settles at some steady-state value. Although the population may wobble a bit over short time spans, the long-term behavior after much iteration for the system is to settle on one population size.
For r=3
f(x)=3x(1-x) f(x)= -rxn2+ rxn --------(21)
f'(x)= -2rx+r => -2(3)x+3-6x +3=0 6x=3 => x=0.5
(22)
f(1/2)=-r(1/2)2+r(1/2), f(1/2)=-r/4+r/2 f(1/2)=r/4 => ¾,x=0.75 ----------(23)
The maximum point is (0.5, 0.75)
For r=3.25
f(x)=3.25x(1-x) ----------(24)
f(x)= -rxn2+ rxn ----------(25)
f'(x)= -2rx+r => -2(3.25)x+3.25-6.5x +3.25=0 6.5x=3.25 => x=0.5
f (1/2)=-r(1/2)2+r(1/2), f(1/2)=-r/4+r/2 f(1/2)=r/4 => 3.25/4,x=0.8125 ----------(26)
The maximum point is (0.5, 0.8125)
For r=3.3
f(x)=3.3x(1-x) ----------(27)
f(x)= -rxn2+ rxn ----------(28)
f'(x)= -2rx+r => -2(3.3)x+3.3-6.6x +3.3=0 6.6x=3.3 => x=0.5
f(1/2)=-r(1/2)2+r(1/2),f(1/2)=-r/4+r/2
f(1/2)=r/4 => 3.3/4,x=0.825 -----(29)
The maximum point is (0.5, 0.825)

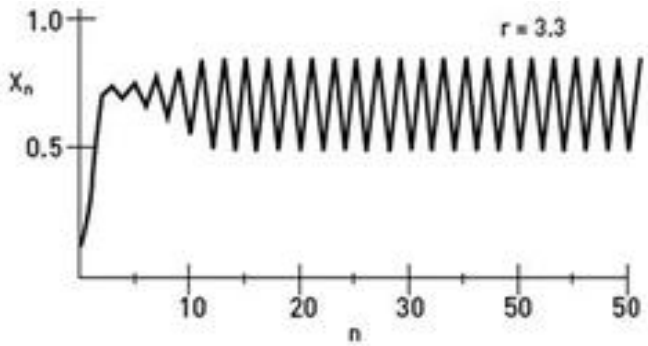

Fig 3.6 Graph for r=3.3

If we let r = 3, we see a surprising change in the system's behavior. Instead of settling on one value, the population oscillates between two different values forever. For our population this would mean, that boom years are followed directly by bust years and vice versa. This change in behavior is a bifurcation from steady-state values to oscillations of time period 2. pEriod 2 means, it takes two iterations to return to the original value.
For r=3.45
f(x)=3.45x(1-x) ----------(30)
f(x)= -rxn2+ rxn --------(31)
f'(x)= -2rx+r => -2(3.45)x+3.45 (32)
-6.9x +3.45=0 6.9x=3.45 => x=0.5
f(1/2)=-r(1/2)2+r(1/2),f(1/2)=-/4+r/2
f(1/2)=r/4 => 3.45/4, x=0.8625
The maximum point is (0.5, 0.8625)

For r=3.5
f(x)=3.5x(1-x) ---------(32)
f(x)= -rxn2+ rxn -------(33)
f'(x)= -2rx+r => -2(3.5)x+3.5 (34)
-7x +3.5=0 7x=3.5 => x=0.5
f(1/2)=-r(1/2)2+r(1/2),
f(1/2)=r/4+r/2
f(1/2)=r/4 => 3.5/4, x=0.875
The maximum point is (0.5, 0.875)

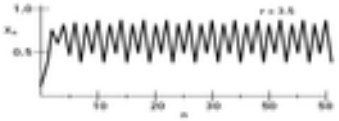

Fig 3.7 Graph for r=3.5

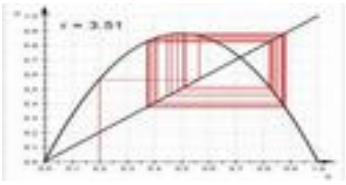

Fig 3.8 logistic map for r=3.5

For r=3.56
f(x)=3.56x(1-x) -----(35)
f(x)= -rxn2+ rxn -----(36)
f'(x)= -2rx+r => -2(3.56)x+3.56
-7.12x +3.56=0 7.12x=3.56 => x=0.5
f(1/2)=-r(1/2)2+r(1/2),
f(1/2)=-/4+r/2
f(1/2)=r/4 => 3.56/4,x=0.89
The maximum point is (0.5, 0.89)
For r=3.58
f(x)=3.58x(1-x) ---------(37)
f(x)= -rxn2+ rxn --------(38)
f'(x)= -2rx+r => -2(3.58)x+3.58 (39)
-7.16x +3.58=0 7.16x=3.58 => x=0.5
f(1/2)=-r(1/2)2+r(1/2),f(1/2)=-/4+r/2
f(1/2)=r/4 => 3.58/4,x=0.895
The maximum point is (0.5, 0.895)
For r=3.66
f(x)=3.66x(1-x) --------(40)
f(x)= -rxn2+ rxn -------(41)
f'(x)= -2rx+r => -2(3.66)x+3.66
-7.32x +3.66=0 7.32x=3.66 => x=0.5
f(1/2)=-r(1/2)2+r(1/2),f(1/2)=-/4+r/2
f(1/2)=r/4 => 3.66/4, x=0.915
The maximum point is (0.5, 0.915)

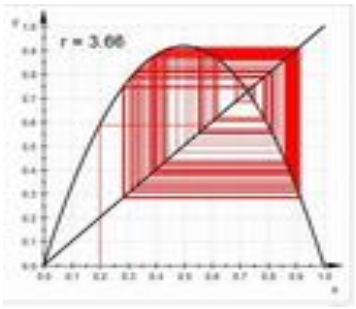

Fig 3.9 logistic map for r=3.66

For r=3.8
f(x)=3.8x(1-x) -------(42)
f(x)= -rxn2+ rxn -----(43)
f'(x)= -2rx+r => -2(3.8)x+3.8 (44)
-7.6x +3.8=0 7.6x=3.8 => x=0.5
f(1/2)=-r(1/2)2+r(1/2),
f(1/2)=-r/4+r/2 f(1/2)=r/4=> 3.8/4,x=0.95
The maximum point is (0.5, 0.95)

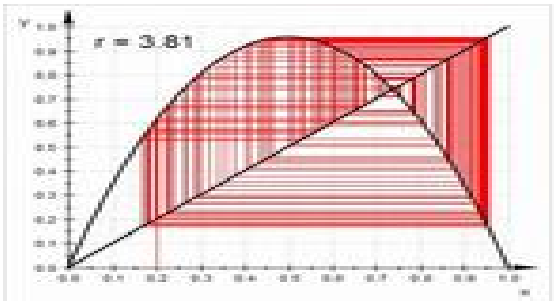

Fig 3.10 Graph for r=3.81

For r=3.9
f(x)=3.9x(1-x) ---------(45)
f(x)= -rxn2+ rxn -----(46)
f'(x)= -2rx+r => -2(3.9)x+3.9 (47)
-7.8x +3.9=0 7.8x=3.9 => x=0.5
f(1/2)=-r(1/2)2+r(1/2),
f(1/2)=-r/4+r/2 f(1/2)=r/4=> 3.9/4,x=0.975
The maximum point is (0.5, 0.975)

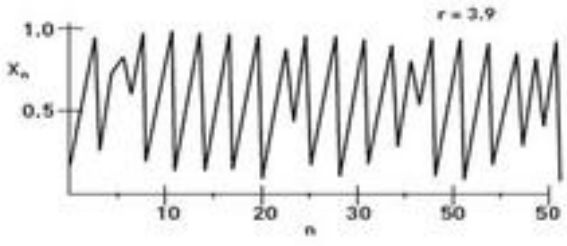

Fig 3.11 Graph for r=3.9

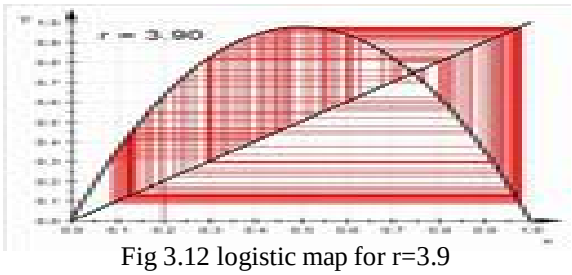

Fig 3.12 logistic map for r=3.9

For r=4
f(x)=4x(1 -x) -----(48)
f(x)= -rxn2+ rxn ---(49)
f'(x)= -2rx+r => -2(4)x+4 -8x +4=0 8x=4 =>
x=0.5 f(1/2)=r(1/2)2+r(1/2),f(1/2)=-r/4+r/2
f(1/2)=r/4 => 4/4,x=1
The maximum point is (0.5, 1)

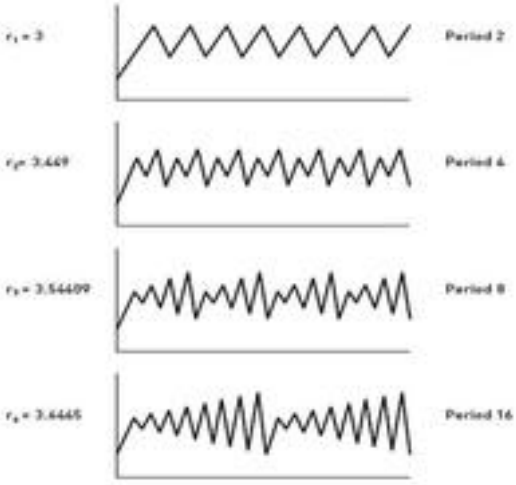

Figure 3.13 period doubling

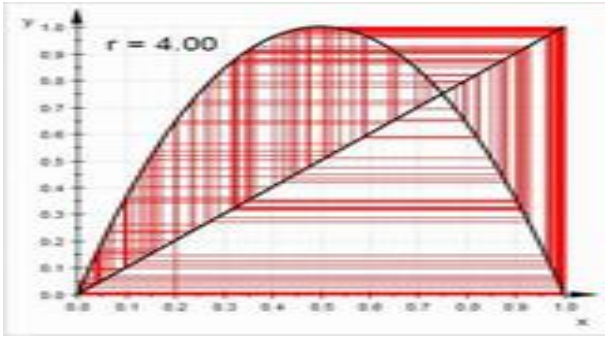

Figure 3.14 logistic map for r=4

As r increases beyond 3, more interesting behavior emerges. More bifurcations can be found and they become more frequent. Each time, the period of oscillation doubles.

The population oscillates first with period 2 when r = 3. When r = 3.449, the period doubles to period 4, indicating that it now takes four iterations for the population to return to a value that it has had before. The period continues to double from 4 to 8 to 16, each time at a successively smaller increment of increase in r. eventually, when r = 3.569946, the period becomes infinite. This means that the population fluctuates wildly, never regularly returning to any previous value.

These period-doubling bifurcations are quite fascinating. [10-12]. Why does a population that is stable at 2.999999 starts swinging between two different values at 3? And why does this oscillation occur more and more rapidly as the r- value approaches the magic number of 3.569946? Furthermore, what happens if we let r get bigger than 3.569946.

Values of r versus their oscillation period paired up with graphs that show the successive period doublings. It is tempting to think that as r increases, the more chaotic the population becomes, but the actual behavior is much more varied than this. The logistic map shows a range of behaviors. Above the magic number, the population becomes chaotic, never settling onto a fixed value and never falling into any periodicity. There are certain "windows" of r- values, above the magic number, that give oscillating populations. It seems that the system bifurcates both into and out of chaos, depending on what r- values one chooses.

We can see the global behavior of the logistic map by looking at what is known as an orbit diagram. This type of diagram is different than the already existing diagrams. The previous diagrams showed how population evolved in time, step by step. An orbit diagram shows how the behavior of a system changes, depending on the r- value. It's a way to see the long-range global behavior of the entire system at a glance.

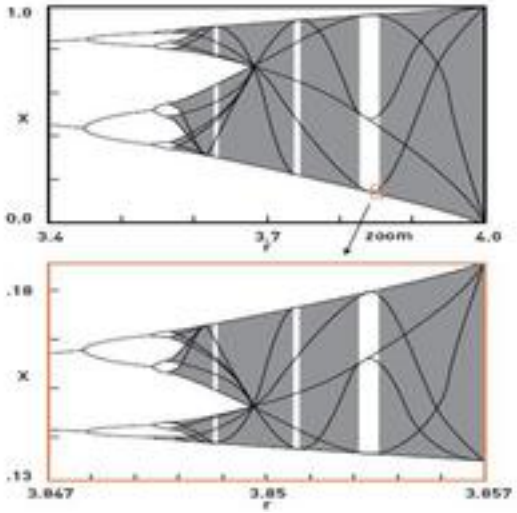

Fig 3.15 Bifurcation

Looking at this diagram, we see r represented along the horizontal and a general p-value along the vertical. This tells us which values of p are accessible for a given value of r. From this point of view, we can easily say that prediction is possible so inrusion is also possible to detect the information.A little further along, we can see the system double, double again, and then double yet again. Eventually, around r = 3.6, it gets really messy. This is chaos, but notice that it does not last forever. As r continues to increase, we see the messiness clear up, at least for small windows of clean oscillations.[14]

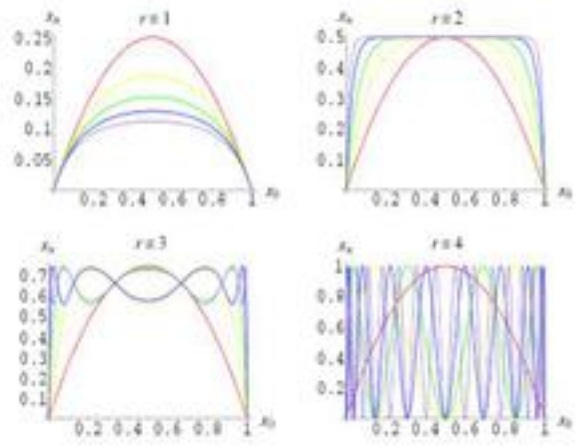

Fig 3.16 variations in r value

4 Asymmetric Key Encryption

The Software Modules in the research works are as follows: Logistic Map, Lorenz System and Encryption and Description. The following steps are involved in designing the system.

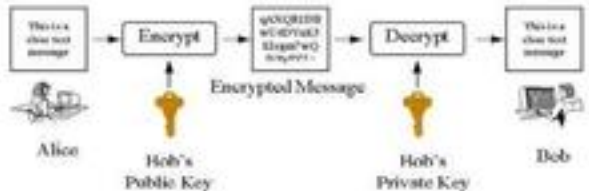

Fig 4.1 Asymmetric key encryption

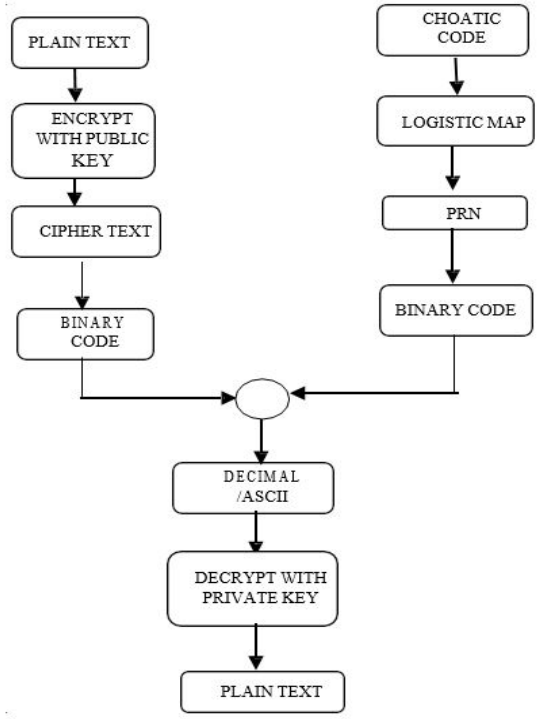

Fig 4.2 Architecture diagram Module Description:

STEP 1: Generate the pseudo random numbers using the logistics map in chaotic code. The list of pseudo random numbers is from the range 0 to 1. The number of random numbers we need isused to fix the size by mentioning N value. Then converting the floating point number into binary and the binary number is assigned to a variable.

STEP 2: Get the plain text from the user which needs to **be** transmitted. Convert the plaintext into ASCII.

STEP 3: Convert the decimal number to binary number. XOR the plaintext with pseudorandom numbers in the form of binary numbers.

STEP 4: Encrypt the binary sequence using RSA algorithm. The cipher text is transmitted through the wireless medium. Decrypt the cipher text to get plain text and reverse the process.

4.1 Logistic Map

The logistic map is an iterative function which is able to give chaotic dynamics in some of its parameter space. [15] The parameter r is the responsible to cause the bifurcation scenario characterized by one of the most well-known route to chaos: the period doubling. This one-dimensional model can be represented as, xn+1=rxn(1- xn),

Where r is the growth rate and (1 - xt) is an intraspecific growth function. These kinds of functions find applications in a wide range of fields, from biology to economics. The logistic map is used to form a chaotic sequence of random numbers. The logistic iterative map with parameter r is: xn+1=rxn(1-xn)

When the value of r lies between 0 to 1, the iterative values ultimately die, which are sovereign of initial condition. When the value of r lies between 2 to 3, the iterative values first oscillate around some value and then finally stabilize on the same value. When the value of r lies between 3 and 3.45 (approximately), the iterative values oscillate between two values forever, which are dependent on r. When the value of r lies between 3.45 and 3.56 (approximately), the iterative values oscillate between four values. As the value of becomes greater than or equal to 3.57, this logistic map is converted into chaotic map, because a slight variations in the initial condition produces dramatically different iterative values over time, exhibit chaotic behavior and trajectory of these iterative values is called chaotic attractor. [16]

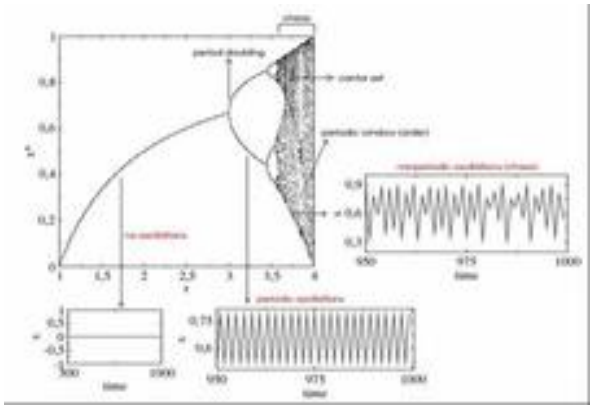

Fig 4.1 The logistic bifurcation diagram

Actually, the chaotic domain leaves a cloud of points in parameter space with a fractional dimensionality.[17] It is relatively easy to show that the logistic map is chaotic on an invariant. The logistic map actually made scientific to think that chaos was not possible to find in population dynamics because it's intrinsic unstability. The initial debate because of May's papers was if the apparent random fluctuations and the unpredictability in natural ecosystems may actually be due to deterministic chaos. Berryman and Millstein argued that in the bifurcation map of the logistic equation , the population spends more time at extremely low densities, where there is a higher probability for deterministic extinction given for example because of external noise. In populations with small size the probability of extinction once the chaotic domain reached is extremely high. They also said that living systems are anti-chaotic and that populations could enter in the chaotic domain because of the human action i.e. perturbations. The role of chaos as a stabilizing factor has been pointed out by Kaneko and Ikegami, who stranded out a high dimen-sional, weak chaotic flow responsible to give stability in host-parasite population dynamics.

4.2 Lorenz Equations

Lorenz equations were very important in the science of chaos because the first strange attractor of a deterministic system was found, described and plotted. By solving numerically Lorenz equations (taking sigma = 10, r = 28 and b = 8 / 3) we can obtain time series and the state variables that can be represented in phase space.

In Equations set 1 we show the Lorenz system and in figure 1 the time series for its variables x, y and z. Equations in Eq. set 1 are the convection equations which were obtained by projecting the infinite-dimensional space of solutions on a three-dimensional subspace.

Specifically, x is proportional to the circulatory fluid velocity, y characterizes the temperature difference between ascending and descending fluid elements, and z is proportional to the distortion of the vertical temperature profile from its equilibrium (which is linear with height).

Sigma, r and b are the physical parameters of the system given by positive values.

$$\frac{dx}{dt} = \sigma(y - x)$$
$$\frac{dy}{dt} = rx - y - xz$$
$$\frac{dz}{dt} = xy - bz$$

Roughly, the Lorenz system is a model of thermal convection which includes a description of the motion of some viscous fluid or atmosphere and the information about heat distribution which actually represents the driving force of thermal convection. The simplicity of this model hidden a wide range of dynamical behaviours for various values of one control parameter.[18]The Lorenz system has either stable or unstable fixed points, a globally attracting periodic or non-periodic solutions, a homo clinic orbit embedded in a two-dimensional stable manifold, bi stability and hysteresis, as variety of cascading bifurcations.

4.3. Encryption and Decryption

1. Construct the Message as per the data packet.
2. Plaintext needs to be converted into Binary code
3. Generate pseudo random numbers from logistics map
4. XOR the plaintext in the form of binary code with random numbers
5. The mapped value is encrypted using RSA encryption algorithm to get a cipher text.

5. Results and Performance Analysis

Using the chaotic code and RSA algorithm technique, the research work was developed, to improve the security and performance in wireless network and is applied for military applications. Using the UDP packet, this message will be sent through the wireless communication system. In the data packet itself the code will be fixed, which in turn will intimate the person who will visualize the message. The higher authority persons can be able to view the message fully and depending upon the cadre and authority level the lower authority person cannot be able to view the higher priority person's message.The level of confusion was increased as the r value increases. The logistic map conceals the amount of data clarification within the chaotic code which is not clear for the people who opens the data packet and conclude the information in a wrong way.

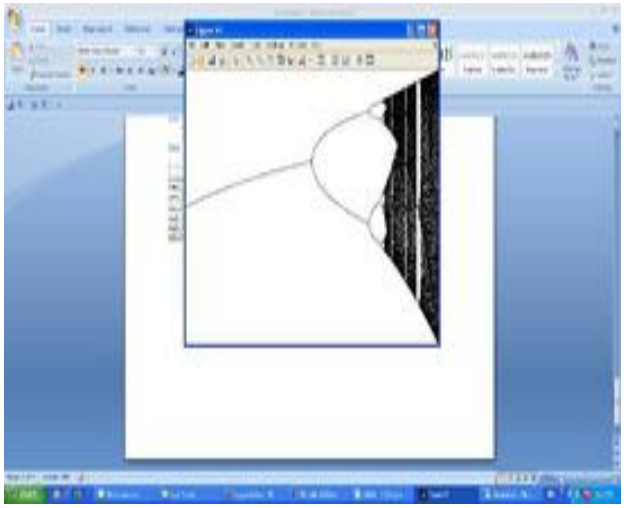

Fig 5.1 logistic map

Table 5.1.Priority and Security level key words in Military service [19]

Clearance level	Term/Keywords
Topsecret Level	Missile, Launch, Uranium, Fusion, Torpedoes, Attack chemical, Weapon, Coded-name, Activate, Reactor, Bio-gas, Ballistic, Designator, Guid-ed, Warheads, Sidewinder, Affect, Electromagnetic, Plutonium
Secret Level	Arm, Buckshot, Rifle, Supply, Power, Explosive, Calibre, Range, Rounds Speed, Operations, Defence, Man-ufacture, Design, Versions, Launcher, Maintenance, Produce, Aircraft, Tanker, Submarine
Confidential level	Generals, Soldiers, Register, Number, Grade, Navy, Designation, Batch, Address, Responsibilities, Age, Date, Contact, Service, Commander, Air-force, Details, Conscripts, Group, Field, Battalion, Records

6. Conclusion and Future Works

The above said information was collected from the Indian army reference word list. [19]. In Military applications the level of clearance control information can be transferred safely to the destination by using chaotic code technique by increasing the complexity and security through different levels of confusions using r values. The basis for selecting the confusion matrix and the base station control was referred from AMNI'09 protocol which has a centralized control of the security code monitoring system. [20]

References

[1] M.R.K.Ariffin and N.A.Abu, "A Chaos Based Public Key cryptosystem", International Journal of Cryptology Research, PP.149-163, 2009.

[2] Bhavana Agrawal, Himani Agrawal "Implementation of AES and RSA Using Chaos System", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

[3] Adel A.El-Zoghabi, Amr H.Yassin, Hany H.Hussien, "Survey Report on Chaos Based Public –Key Cryptosystem", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 12, December 2013.

[4] E.Biham, "Cryptanalysis of the chaotic – map cryptosystem", Proc. Eurocrypt'91, PP. 532- 534, 1991

[5] Alexander N.Pisarchik, Massimiliano Zanin, "Chaotic map Cryptography and security", 2010 Nova Science Publishers, Inc, PP.1-28.

[6] Carmen Pellicer-Lostao, Ricardo Lopez- Ruix, "Notions of Chaotic Cryptography: Sketch of a Chaos based Cryptosystem", Applied Cryptosystem and network Security(Intech Books), 1st Edition, PP.267- 294, 2012.

[7] F.Dachselt, K.Kelber and W.Schwarz, "Chaotic Coding and Cryptanalysis", 1997, http://citeseer.nj.nec.com/ 355232.html

[8] Jaydip Sen, "Theory and Practice of Cryptography and Network security Protocols and Technologies", InTech, 2013.

[9] Kocarev , L.Halle, K.S. Eckert, K.Chua, L.O.Parlitz, U.Int.J, " Bifurcation and chaos" 1992, 2, PP.709-713.

[10] Kocarev, S.Lian (Eds.), "Chaos-Based Cryptography – Theory, Algorithms and Applications", Studies in computational Intelligence vol.354, Springer, 2011.

[11] Ljupco Kocarev, Marjan Sterjev, Attila Fekete and Gabor Vattay, "Public-Key encryption with Chaos", American Institute of physics (AIP), vol. 14, pp-1078-1082.

[12] Mazen Tawfik Mohammed, Alaa Eldin Rohiem, Ali El-moghazy, A.Z.Ghalwash, "Chaotic Based Key Management and Public- Key Cryptosystem", International Journal of Computer Science and Telecommunications, Volume 3, Issue 11, PP.35-42, 2012.

[13] Rodrigo Abarzua, Ivan Jiron, Miguel Alfaro, Ismael Soto, "A New Public Key Cryptography Algorithm Using Chaotic Systems and Hyper elliptic Curves", 10th WSEAS International Conference on systems, Vouliagmeni, Athens, Greece, PP. 771-774, 2006

[14] Robert P.Murphy, "Chaos Theory", Second edition, Ludwig von Mises Institute, Creative commons attribution License 3.0, 2010.

[15] Santo Banerjee, M.R.K.Ariffin, "Chaos Synchronization based Data Transmission with Asymmetric Encryption", International Journal of Computer Applications, Vol.37, Issue.12, PP.6-9, 2012.

[16] Shuichi Aono, Yoshifumi Nishio, "A Cryptosystem Based on Iterations of Chaotic Map", IEICE Technical Report, Vol.107, No.87, 2007.

[17] K.Wang, W.Pei and L.Zhou, "Security of Public Key encryption technique based on multiple chaotic systems", Physical letters. Lett.A, Vol. 360, PP.259-262, 2006.

[18] Yun-Peng Zhang, Xia Lin and Qiang Wang, Richard O.Sinnott, "A Rapid Cryptography Algorithm Based on Chaos and Public key", Journal of Software, Vol.7, No.4, PP. 856- 860, 2012.

[19] A..Madhumitha,, Dr.B.Amutha," Multi-Level Security and Detection against Clone Attack in Military Scenario" IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 1, Feb-Mar, 2014,ISSN: 2320-8791 www.ijreat.org

[20] Amutha.B, V.Nivedha Devi," AMNI'09 PROTOCOL," *International Journal of Information Technology and Knowledge Management*", Volume 2, Number 2, Publisher page 297-303, July-December 2009.