Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2015, 2(1): 86-90

Research Article ISSN: 2394 - 658X

Implementation and Analysis of Symmetric Key Encryption Technique Using Chaos Theory

Kangkana Bora[1] and Md Abdul Wadood[2]

[1]*Central Computational and Numerical Studies, Institute of Advanced Study in Science and Technology, Guwahati, Assam, India*
[2]*Computer Science and Engineering, Regional Institute of Science and Technology, Meghalaya, India*
kangkana.bora89@gmail.com

ABSTRACT

Chaos theory is the study of dynamic systems that evolve in time presenting properties such ergodicity, sensitivity to initial conditions, topological mixing etc. In recent years quite a number of researches on chaos based cryptosystem have been proposed. However, most of them encounter some problems such as: low level of security and small key space. The key stream generator is the key design issue of an encryption system. A remarkable characteristic of chaotic systems is their capability of producing quite complex patterns of behaviour from Simple real systems which makes it suitable to be used in cryptosystems. This paper presents an approach for the application of Chaos Theory in symmetric key cryptography by implementing and analysing an algorithm based on the concepts of Chaos Theory giving special focus on key generation.

Key words: Chaos Theory, cryptography and symmetric key cryptosystem

INTRODUCTION

Ever since the discovery of chaotic behaviour in the mathematical models of weather systems by Edward Lorenz in the early 1960s [1], chaos theory has been a common theory in various fields including physics, biology, economics and even philosophy. In the last couple of decades, chaos theory has been greatly influencing the field of cryptography as the main principle of a perfect cryptosystem is to generate the most complex key to encrypt the plaintext. A Symmetric Key Cryptosystem uses a secret shared key for both encryption and decryption of messages. The main aim of such system is to generate the key that an unauthorized user can't guess it easily.

This paper discusses how the Chaos Theory is used to generate a key and implement an algorithm that satisfies the needs of a Symmetric Key Cryptosystem.
The Chaos Theory has a logistic equation of the form

$$X_{n+1} = r X_n(1-X_n) \qquad (1)$$

Here, r is a term that decides the randomness of the values of the function and X_n is called the initial condition. This equation is used to generate the symmetric key. Our main aim is to find a proper value of r that gives the most randomness.

CHAOS THEORY AS ITS IS APPLIED TO CRYPTOGRAPHY

The effectiveness of a Symmetric Key Cryptosystem lies in the algorithm used to generate the key. Chaos Theory provides the means to generate an effective key which an intruder is made impossible to guess. Chaos systems have certain characteristics that can be related to some of the important properties a cryptosystem which make chaos systems applicable to cryptography.

Ergodicity

Statistical measurements of the variables give similar results no matter if they are performed over time or space [2]. The output of the system seems similar for any input even if they are different. This characteristic is similar to the 'confusion' property of cryptosystem which ensures that the cipher text does not reveal the plaintext.

Sensitivity to Initial Condition

Given an initial state of a deterministic system, it is well known that the future states of the system can be predicted. However, for chaotic systems, long term prediction is impossible. For specific values of parameters, two trajectories, which are initially very close, diverge exponentially in a short time. Initial information about the system is thus completely lost [3], which is the concept of 'diffusion' in cryptography that is used to mean an increased redundancy of plaintext by spreading it across rows and columns.

Topological Mixing

It means that the system will evolve in time so that any given region of states is always transformed or overlaps with any other given region [2]. Self-mapping of functional values over iterations makes it distributed over the whole space. This characteristic is similar to the 'multi-round transformation' concept of cryptography which transforms the bit positions of the plaintext.

PROPOSED APPROACH

Analysis on r Value

The parameter 'r' is a factor that greatly affects the logistic equation. As per our findings the values of 'r' varies from 1 to 4.2. The reason for not taking more than 4.2 is that if we give those values of 'r' in the logistic equation, it gives undefined values to the function for most of the iterations. For example, the values x after each iteration for r =4.3 are as follows:

```
0.3869999999999999
1.0200932999999999
-0.0881372750310264
-0.4123934534079611
-2.5045857994333325
-37.743404052472684
 -6287.924200138941
-1.7004039828484026E8
-1.2432907004130225 6E17
-6.646818592654068E34
-1.8997484883570277E70
-1.551889057176369E141
-1.0355946476870168E283
-Infinity
-Infinity
-Infinity
-Infinity
-Infinity
-Infinity
```

To study the randomness we considered the concept of standard deviation using the formula-

$$S = \sqrt{}\ (X\text{-}X')^{2}/\ (n\text{-}1) \qquad (2)$$

Where X = each score X' = the mean or average n = the number of values ∑ means the sum across the values

It is said that more the Standard deviation more will be randomness. The standard deviation for distribution of x values keeping r value fixed are as shown in the Table I.

Table -1 Standard Deviation for Distribution of X Values Keeping r Value Fixed (Initial Value Taken is 0.9)

r values	Standard deviation
1	0.0166541
2	0.0812905
3	0.0991434
3.1	0.1164614
3.2	0.1357884
3.3	0.1382067
3.4	0.1739956
3.5	0.2053754
3.6	0.2222499
3.7	0.2136420
3.8	0.2599768
3.9	0.2726017
4	2.0877335

From the above observation it can be said that standard deviation is increasing from r=1 to 4. So r value giving highest standard deviation value is preferred.

Analysis of Initial value

Initial value parameter is another factor that determines the chaotic nature of the logistic equation. The values of initial value X_n varies between 0 and 1. The reason for not allowing more than 1 in its values is that if we take more than 1 the logistic equation results in unpredictable values for the iterations. For example if we take X_n = 2 then corresponding X value after each iterations are-

X_1= 7.862920240164593E23
X_2= -2.4730205881276004E48
X_3 -2.446332331721193E97
X_4 -2.39381675088978E195
X_5 -Infinity
X_6 -Infinity
X_7 -Infinity
X_8 –Infinity and so on...

The standard deviation for distribution of x values keeping initial value fixed and r value as 3 are as shown in the Table -2.

Table -2 Standard Deviation for Distribution of X Values Keeping Initial Value Fixed(r Value Taken is 3)

Values of Initial X_n	Standard deviation
0.1	0.099180
0.2	0.0743054
0.3	0.0318138
0.4	0.0472701
0.5	0.0636953
0.6	0.0472700
0.7	0.0318138
0.8	0.0741372
0.9	0.0991434

From the above observation it can be said that standard deviation is increasing from initial value=0.1 to 0.9. So, initial value giving highest standard deviation value is preferred.

PROPOSED ENCRYPTION AND DECRYPTION ALGORITHM

M Roskin , J.B Casper have developed the concept of Simple cipher and Advanced cipher technique to develop a chaos based cryptosystem [7]. In this approach focus is being given to modify those techniques for stream ciphers so that it can provide better results. The proposed approach is as follows-

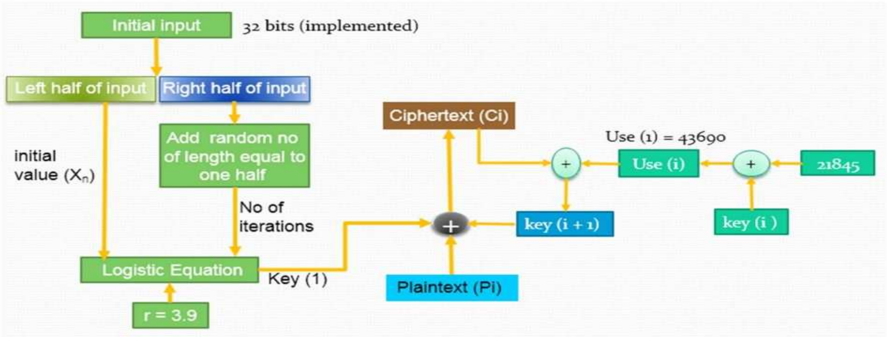

Fig 1 – Block diagram for the encryption technique

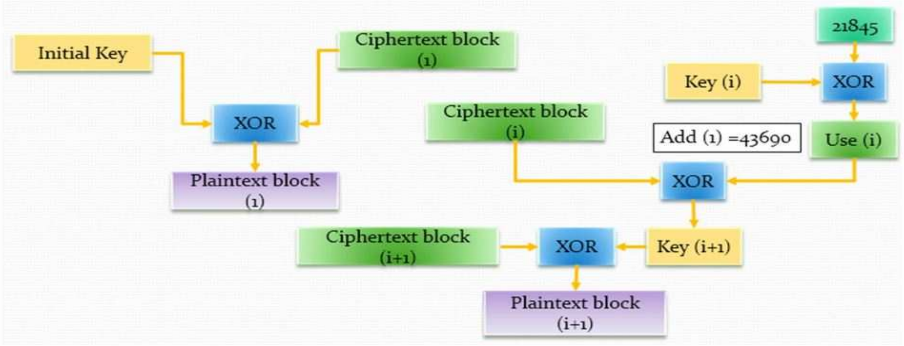

Fig 2-Block diagram for decryption technique

In this approach r value is kept fixed at 3.9. Although the r value 4 gives the highest standard deviation according to the observation s when we take r=4 then some of the keys generated from logistic equation tend to be infinity or exponential which can't be used for implementation. Next r value that gives maximum standard deviation is 3.9. So r value is fixed at 3.9.

ANALYSIS OF THE APPROACH

Ergodicity

Our algorithm satisfies this property as the output ciphertext looks similar even if their plaintext characters are different.

Sensitivity to Initial Condition (Xn)

The followings are observations on the changes in the bit positions of the respective ciphertext when the initial input is changed by one bit at a time, where the number of iterations is fixed to 20 for each of them, and total number of bits in ciphertext is 112 in each case.

Bit positions changed from Xn =0.1 to Xn =0.2:
0,4,6,7,10,12,15,16,20,22,23,26,28,31,32,36,38,39,42,44,47,48,52,54,55,58,60,63,64,68,70,71,74,76,79,80,84,86,87, 90,92,95,96,100,102,103,106,108,111 Total bit Changed=49

Bit positions changed from Xn =0.2 to Xn =0.3:
1,4,6,8,9,10,11,15,17,20,22,24,25,26,27,31,33,36,38,40,41,42,43,47,49,52,54,56,57,58,59,63,65,68,70,72,73,74,75,79,81,84,86,88,89,90,91,95,97,100,102,104,105,106,107,111 Total bit changed=56

Bit positions changed from Xn =0.3 to Xn =0.4:
1,2,6,10,11,12,15,17,18,22,26,27,28,31,33,34,38,42,43,44,47,49,50,54,58,59,60,63,65,66,70,74,75,76,79,81,82,86,90,91,92,95,97,98,102,106,107,108,111 Total bit changed=49

Bit positions changed from Xn =0.4 to Xn =0.5:
2,5,7,8,11,12,13,15,18,21,23,24,27,28,29,31,34,37,39,40,43,44,45,47,50,53,55,56,59,60,61,63,66,69,71,72,75,76,77, 79,82,85,87,88,91,92,93,95,98,101,103,104,107,108,109,111 Total bits changed=56

Bit positions changed from Xn =0.5 to Xn =0.6:
2,6,7,15,18,22,23,31,34,38,39,47,50,54,55,63,66,70,71,79,82,86,87,95,98,102,103,111 Total bits changed=28

From the above results we see that there is a great change in the ciphertext bits for every single bit change in the initial condition in the logistic equation, which is called the Avalanche effect. In most cases there are 4, 5 or 6 bits changes for every 16 bits.

Key Space

Left 16 bits can take value from 1 to 65535, Right 16 bits can take value from 1 to 65535, and Random 16 bits can also take value from 0 to 65535
Note : Right and random bits both can't start from 0 because if both are 0 resultant number of iterations will be 0 which can't be applied, so one of them should be at least 1 and left bits can't be 0.

Table -3 Considering Right and Random Bits

Right bits value	Random bits	No of combinations
1	0 to 65535	65536
2	0 to 65535(excluding (2,1) combination)	65535
3	0 to 65535(excluding (3,1)&(3,2) combinations)	65534
-	-	-
65534	Only (65534,65535) combination	2
65535	Only (65535,65535) combination	1

Total combinations are thus just the sum of 1 to 65536. So total combinations can be found out as below:
Result = n(n+1)/2 [formula for summing up n numbers] = 65536 (65536+1)/2 = 2147516416 combinations

Considering Left and Right (result above) Bits

Left bits value goes from 0 to 65535 and for each value of left (initial condition) we can have 2147516416 combinations.
Therefore,
Overall combinations = 65535 * 2147516416 = 140737488322560 = 2^{47} (approx) [more than 2^{46}]
If we implement for input length of 128 bits then it will be almost 2^{375} combinations which is very large.

RESULTS AND CONCLUSION

Advantages of Proposed Algorithm

The advantages of the proposed approach -

1. Easy to understand and implement
2. Three level security-
    - i) Left 16 bits of the 32 bits input which is almost random
    - ii) Right 16 bits is unknown
    - iii) 16 bits random input which is also unknown
3. The number of bits in the key can be varied as 8,16,32,64 and so on with little modification in the program.
4. Even if the inputs are changed the output ciphertext looks similar and sometimes there are substring with same identity. These makes an intruder confused that he got some clue about the plaintext while it is not the case actually because even if the ciphertext substring are same their plaintext are different as key for each character in the ciphertext is different.
5. For any change in the input the changes in the ciphertext is distributed all over itself which is the diffusion property of cryptography.

Sample output of the approach is as shown below -

Plaintext : how are you?

```
(1)
Initial value of Xn is: 0.7
Number of iterations is: 20
The value of r=3.9
The key is : 0011100010010010
The Cipherext in binary is:
001110001111101000111000100101010011100011100010001110001100001000111000101000110011100011
010001001110001011010000111000100101000011100011101101001110001000001000111000111101110011
100011001000

The Ciphertext in hexadecimal is:
38fa389538e238c238a338d138b4389438ed388238f738c8

(2)
Initial value of Xn is: 0.9
Number of iterations is: 20
The value of r=3.9
The key is : 1111101100011000
The Cipherext in binary is:
111110110111000011111011000111111111101101101000111110110100100011111011001010011111101101
0110111111101100111110111110110001111101111101101100111111110110000100011111011011111011111
101101000010
The Ciphertext in hexadecimal is:
fb70fb1ffb68fb48fb29fb5bfb3efb1efb67fb08fb7dfb42
```

REFERENCES

[1] C A Wood, *Chaos-Based Symmetric Key Cryptosystems*, Department of Computer Science, Rochester Institute of Technology, Rochester, New York, USA, **2007**.

[2] P Carmen and L R Ricardo, *Notions of Chaotic Cryptography: Sketch of a Chaos based Cryptosystem*, Department of Computer Science and BIFI, University of Zaragoza, Spain.

[3] Q V Lawande, B R Ivan and S D Dhodapkar, Chaos Based Cryptography: A New Approach To Secure Communications, *BARC Newsletter, Theoretical Physics Division*, No 258**, 2005**.

[4] N Masuda, Jakimoski, Chaotic Block Cipher: from Theory to Practical Approach, IEEE *Transaction on Circuits and System*, **2006**, vol.53, Issue 6, p.1341-1352.

[5] K Faraoun, Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption, *International Arab Journal of Information Technology*, **2010**, Vol. 7, No. 3**,** p.231-240.

[6] B Bakhache, K Ahmad and S El Assad, A New Chaotic Encryption Algorithm to Enhance the Security of Zig-Bee and Wi-Fi Networks , *International Journal of Intelligence Computing Research, Informatics Society*, **2011**, Vol. 2, Issue 4, p. 220-227.

[7] K M Roskin and J B Casper, *From Chaos to Cryptography http://www.gaianxaos.com/pdf/unsorted/chaos_and_cryptography.pdf.*

[8] K Bora, A Wadood, M Hazarika and Z Ahmed, Analysis of Crypto Components of a Chaotic Function to Study its Random Behaviour, International Journal of Computer Science and Information Technology, **2013**, Vol.5 Issue 2, p. 2566-2568.