TEST Engineering & Management

March - April 2020
ISSN: 0193-4120 Page No. 01 - 05

Lock to a Locker Method on Fuzzy Cryptography for Double Security

R. Buvaneswari[1], J. Pavana[2], P. Sowmiya[3], V. Abisha[4]

[1,2,3,4]Sri Krishna Arts and Science College, Kuniyamuthur, Coimbatore

Article Info
Volume 83
Page Number: 01 - 05
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 12 March 2020*

Abstract

The sender sends the lock of an encrypted binary number of a locker crisp number from a fuzzy membership table which is defined on an ASCII values of an uppercase alphabets and membership function. The receiver then converts the binary number into a fuzzy number and then it is defuzzified using a suitable formula.

Keywords – *Fuzzy set, Fuzzy subsets, Membership function, Crisp number, Binary number, ASCII values, Cryptography, Encryption, Decryption.*

I. INTRODUCTION

In this fast moving world, security has become one of the major issue. In this situation fuzzy cryptography fills the space. Cryptography is the science of secretwriting.On encryption and deception cryptography plays a vital role .Many cryptography algorithms exists for safer transmissions with tight security. Even though there are lot of cyber-crime issues arisen with the development of advanced technology, the communication started to face some failures. The fuzzy logic is a powerful tool to maintain uncertain inputs.

In 2012 RavinduMadanayake et.al. [6]found that the existing algorithms concerns only about security which fails in Processing duration which was equally important thus at their algorithm they concentrate down on both processing duration and security using encryption and decryption algorithms inby fuzzy graph theory the main aim of them was to establish a strong algorithm which concern s about low processing duration with high security level and thus their algorithm was compared with the previous algorithm s and found with positive results.

In 2016 K.Ganeshkumar et.al.[3] established a new algorithm based on crytography using fuzzy logic for safer communication.. At first the understood the mistakes that causes for hacking by the proposer during the data transmission over the network. Then it was rectified without losing data. Their idea was based on text data encryption using fuzzy on cryptography which provides high accuracy data Tansfering. The previous algorithm had been noded in many ways for secrect communication rather than complexity. Hence the observation was compared with existing algorithm finally reserchers Concluded that its take minimum time and high security for execution.

In 2017 Kamilah Abdullah et.al. [4] gave key Importantance on communication henforth they failed at security this was replaced by the introduction of RSA Cryptosystem which focuses on both the communication as well as security. Rsa algorithm was established by fuzzy set theory. They used triangular fuzzy numbers for encryption and decryption algorithm. By the invention of RSA

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 01 - 05

Crytosystem hackers faced difficulty at the time of hacking on Ecrytption and decryption thus RSA Cryptosystem placed a good time on safer communication.

In 2017 M. Muthumeenakshi et.al. [5] said that The art of Science encompasses the principles and methods of Transforming an intelligible message into unintelligible, and then, retransforms that message back to its original form for more security. The objective was to develop simple, real and secure system, which could be achieved through the software implementation. In their article , fuzzy logic approach had been introduced to embed the encrypted message.

In 2018 P. Amudha et.al. [1] said that Ciphers could be converted into graphs for secrete communication. The field of Graph theory was widely used as a tool of encryption , due to its various properties and its easy representation in computers as a matrix. they explored the usage of Graph theory in cryptography

In this article,an algorithm is is introduced for the process of double encryption and decryption for creating new Algorithm (lock to a locker method). Without the security formula it is impossible to hack the dataThis is a powerful algorithm which cannot take the safer transmission and it is impossible to hack the data unless the security formula is known .the main aim of this article is to eradicated the security accuracy in Data communication.

II.PRELIMINARIES

In this section , the notation of fuzzy subsets and uppercase ASCII values for alphabets are provided for encryption.

Definition 2.1

A *Graph* is an ordered pair G=(V,E) consists of a non-empty finite set V of elements called vertices and a finite set E of ordered pairs of distinct vertices called edges.

Definition 2.2

A *fuzzy set* A on a set X is characterized by a mapping $m: X \rightarrow [0,1]$, which is called the membership function. A *fuzzy set* is denoted by A=(X, m).

Definition 2.3

A *fuzzy subset* of a universe X (a fuzzy set)is a mathematical object A described by its (generalized)characteristic function(membership function $\mu A: X \rightarrow [0,1]$.

Definition 2.4

Crisp is used in Contrast with fuzzy.

A fuzzy variable has a possible range of values, it is imprecise.

A Crisp variable, we may assume, has a precise value.

Definition2.5

Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text.

Definition2.6

Encryption is the process of converting the data into a code, especially to prevent unauthorized access.

Definition 2.7

Decryption is the conversion of encrypted data into its original form. It is generally a reverse process of encryption.

Definition 2.8

Binary number is a number expressed in the base-2 numeral system or binary numeralsystem, which uses only two symbols: typically "0" (zero) and "1" (one). The base-2 numeral system is a positional notation with a radix of 2.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 01 - 05

Definition2.9

ASCII (American Standard Code for Information Interchange) is the most common form for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is

represented with a 7-bit binary number (a string of seven 0s or 1s). 128 possible characters are defined.

The ASCII values for lowercase ranges from 97 to 122, and for the uppercase it ranges from 65 to 90.

III. LOCK FOR LOCKER METHOD

A. Double Encryption Algorithm

Step 1: Let (a, b) denotes any uppercase alphabet letters (COMPUT) and upper case ASCII values are assigned for those alphabets , where a and b should contain same digit of numbers (using 2 digts). The outcome of (a, b) had been assigned from A to Z and 0 to 9.

(a,b)	C(67)	O(79)	M(77)	P(80)	U(85)	T(84)
C(67)	A	B	C	D	E	F
O(79)	G	H	I	J	K	L
M(77)	M	N	O	P	Q	R
P(80)	S	T	U	V	W	X
U(85)	Y	Z	0	1	2	3
T(84)	4	5	6	7	8	9

Step 2: Preparing Fuzzy Membership Table

The outcomes are changed into Fuzzy membership value by using the fuzzy membershi Function $\mu: (a,b) \rightarrow [0,1]$such that$\mu(a,b) = \frac{100a+b}{88000}$. The converted outcomes are listed below in fuzzy membership table.

(a,b)	C(67)	O(79)	M(77)	P(80)	U(85)	T(84)
C(67)	0.07690	0.09053	0.08826	0.09167	0.09735	0.09622
O(79)	0.07703	0.09067	0.08840	0.09181	0.09749	0.09635
M(77)	0.07701	0.09065	0.08838	0.09178	0.09747	0.09633
P(80)	0.07705	0.09068	0.08841	0.09182	0.09750	0.09636
U(85)	0.07710	0.09074	0.08847	0.09188	0.09756	0.09642
T(84)	0.07709	0.09073	0.08845	0.09186	0.09755	0.09641

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 01 - 05

The Fuzzy membership value 0.00000 is assumed for an empty space.

Step 3: An arbitrary number 100000 is multiplied with fuzzy membership number to get the crisp number which strengthern the secrecy.

Step 4: Again the crisp number is converted into binary number for double security.

B. Decryption Algorithm

Step 1: The received binary number is converted into crisp number.

Step 2: Each crisp number is divided by 100000 to get the value of 'r'. where r belongs to [0,1].

Step 3: Using the decryption formula 880r (round of to two decimal places), the value is defuzzified.

IV. NUMERICAL EXAMPLE

In this section the lock to a locker method algorithm is shown by an example for Encryption and Decryption.

4.1 Encryption

Assume the phrase "YOU CAN WIN"

Using the lock to locker method algorithm. This is encrypted as below,

Step 1: The corresponding membership values of the phrase is, 0.07710 0.08838 0.08841 0.0000 0.08826 0.07690 0.09065 0.0000 0.09750 0.08840 0.09065.

Step 2: Converted to crisp number to strengthen the secrecy, 7710 8838 8841 0000 8826 7690 9065 0000 9750 8840 9065.

Step 3: For double security the binary number of each corresponding crisp number are as follows

1111000011110 10001010000110 10001010001001 000000000000 10001001111010 1111000001010 10000001001001 000000000000 10011000010110 10001010001000 10001101101001.

4.2 Decryption

Step 1: Converting the above binary number to crisp number and then dividing each crisp number by 100000 we get,

0.07710 0.08838 0.08841 0.0000 0.08826 0.07690 0.09065 0.0000 0.09750 0.08840 0.09065.

Step 2: Using the decryption formula 880r (round of to two decimal places) we get,

67.85 77.77 77.80 00.00 77.67 67.67 79.77 00.00 85.80 77.79 79.77.

The corresponding decrypted alphabet from the fuzzy membership table is "YOU CAN WIN".

V. CONCLUSION

In this article, the double encryption made for a Membership values by using a suitable Fuzzy membership function. The Sender double encrypts the data from membership table using binary concept and the receiver decrypts the message by converting the given codes into crisp number and defuzzified using the suitable formula. The Proposed Method Strengthen the Security. In future work, the author are motivated to analyse any other method instead of binary numbers.

REFERENCES

[1] P. Amudha, A.C. Charles Sagayaraj A, C.ShanthaSheela ,"An application of Graph theory in Cryptography", International Journal of Pure and Applied Mathematics , 119(13), 375-383, 2018.

[2] Anita Pal , National Institute of Technology Durgapur West Bengal-713209,India.

[3] K.Ganeshkumar, D.arivazhagan, et.al ,'new Cryptography Algorithm with Fuzzy logic for Effective Data Communication'. International journal of Science and tech. vol 9(48), DOI: 10.17485 /ijst/2016/v9i48/108970, Dec 2016.

[4] Kamilahabdullah. Sumarni Abu Baskar, Nor Hanimakamis, and Harialimais , 'RSA cryptosystem with Fuzzy set Theory for encrption

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 01 - 05

and decryption', AIP conference Proceeding 190,030001(2017), volume 950, Issue 10.063/1.5012147.

[5] M. Muthumeenakshi, T. Archana, P. Muralikrishna,"Fuzzy Application In Secured Data Transmission", International Journal of Pure and Applied Mathematics , 116(3), 711-715, 2017.

[6] Ravindumadanayake, et.al ,'Advanced Encryption Algorithm Using Fuzzy Logic", International Journal of Computer networks ((ICICN 2012) IPCSIT vol 27(2012) IACSIT Press),Singapore.

[7] S.Shara et .al on "RSA algorithm using modified subset sum Cryptosystem," in computer and commTech .(India, 2011) pp. 457-461.

[8] L.A.Zadehand R.RYager et al. (John Wiley, New York, 1987). "Fuzzy Sets and Applications :"

[9] L.A Zadeh, information And control, vol. 8, 338-353(1965).